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

IPv6 Monitoring in Nederland: De tweede meting

Datum	23 november 2010
Auteur(s)	Maria Boen-Leo, Arjen Holtzer, Martin Tijmes, Rob Smets
Aantal pagina's Aantal bijlagen	48
Projectnaam	IPv6 Monitoring in Nederland
	Deze rapportage maakt onderdeel uit van het monitoringsprogramma van TNO en is tot stand gekomen dankzij een bijdrage van het Ministerie van Economische Zaken
Projectnummer	035.33445

Inhoudsopgave

1 Managementuittreksel

In dit whitepaper, IPv6 Monitoring in Nederland, brengt TNO de status van de uitrol van IPv6 in kaart. Het doel van dit onderzoek is om door middel van het verzamelen van informatie en meetgegevens en door middel van het uitvoeren van interviews en enquêtes een beeld te krijgen hoe ver Nederland is met de uitrol van IPv6 in vergelijking met andere Europese landen.

In juli 2010 is de eerste meting (gepresenteerd als “Nulmeting”) gepubliceerd. Dit whitepaper beschrijft de tweede meting. Ten opzichte van de Nulmeting bevat de tweede meting twee nieuwe onderzoeksonderdelen:

- Interviews onder ISP’s en mobiele operators, en enquêtes bij bedrijven en overheden;
- Voordelen en tekortkomingen van IPv6 n.a.v. security onderzoek.

De positie van Nederland ten opzichte van omliggende landen is sinds de Nulmeting niet gewijzigd. Als gekeken wordt naar de voorbereidingen voor de uitrol van IPv6 loopt Nederland nog steeds mee voorop. Dit blijkt onder meer uit de aanvraag van IPv6 adressen en de plannen van ISP’s voor uitrol. Nederland presteert gemiddeld als het gaat om de daadwerkelijke uitrol van IPv6. Nog maar een klein deel van de IPv6 adressen in Nederland worden geadverteerd, en de hoeveelheid IPv6 verkeer is ook nog heel laag.

Uit de interviews is gebleken dat grote ISP’s en mobiele operators stappen hebben ondernomen om geen last te ondervinden van het opraken van de IPv4 adressen. Ze hebben plannen om IPv6 uit te gaan rollen tussen 2011 en 2013.

De belangrijkste bottleneck voor ISP’s om IPv6 nog niet in te voeren blijft een beperkte ondersteuning door fabrikanten. Dit was in 2009 ook al zo, maar in 2010 geeft een nog groter deel van respondenten aan dat dit belangrijk is. Dit geldt voornamelijk voor partijen die al plannen hebben om IPv6 te gaan invoeren, maar ook voor partijen die nog geen plannen hebben.

Veel bedrijven en overheden zijn zich bewust van de komst van IPv6. Plannen zijn er bij een deel ook, maar echte activiteit is beperkt. Daarnaast is bij organisaties weinig bekend over IPv6-ondersteuning bij applicaties. Meer aandacht voor IPv6 bij deze organisaties is gewenst om beter de risico’s aangaande de IP adresschaarste te managen, omdat de verwachte uitputtingsdatum maart 2011[1] (IANA) is. Het exacte moment van uitputting zal afhangen van het moment waarop RIR’s opnieuw aanvragen voor adresblokken zullen doen. De uitputtingsdatum kan hierdoor nog sterk variëren.

De beschikbaarheid van IPv6 verbindingen voor eindgebruikers is licht gestegen. Er is één grote ISP die IPv6 verbindingen levert aan consumenten en een tiental kleine ISP’s die IPv6 aan zakelijke klanten aanbieden.

Een ander punt van zorg is de beperkte beschikbaarheid van content en diensten over IPv6. Het is onduidelijk wat voor plannen content providers exact hebben op dit gebied.

[1] Bij de voorspelde uitputtingsdatum moet rekening gehouden worden met enkele maande spreiding, http://ipv4.potaroo.net

Indien content daadwerkelijk achterblijft is dit een ontwikkeling die de adoptie van IPv6 kan afremmen.

IPv6 is in mei 2010 aangemeld om opgenomen te worden op de "pas toe of leg uit"-lijst van Open Standaarden[2] voor de overheid. De opname van IPv6 op deze lijst kan een impuls geven aan het gebruik van IPv6 bij de overheid en haar leveranciers. In november 2010 besluit het College Standaardisatie of IPv6 wordt toegevoegd aan deze lijst.

Sinds de Nulmeting is ook het standaardisatiewerk binnen IETF, 3GPP en Broadband Forum gecontinueerd. In de IETF wordt momenteel veel werk verricht aan NAT64 wat tijdens de transitieperiode van IPv4 naar IPv6 perspectief biedt voor translatie tussen deze twee protocollen. 3GPP zal begin 2011 met een nieuwe release komen waarin de migratie naar IPv6 wordt meegenomen in de ontwikkelingen voor mobiele netwerken, en binnen het Broadband Forum zijn twee nieuwe *technical recommendations* tot stand gekomen die bijdragen aan de adoptie van IPv6 door met name fabrikanten.

De frequentie waarmee aan IPv6 gerelateerde kwetsbaarheden gerapporteerd worden blijft laag in vergelijking met IPv4. De ernst van gerapporteerde kwetsbaarheden is in vergelijking met de Nulmeting vrijwel ongewijzigd.

Een lijst van voordelen en tekortkomingen op het gebied van IPv6 beveiligingsmodellen en -implementaties kan als leidraad dienen voor toekomstige maatregelen en richtingen waarin innovatie van meer IPv6 beveiligingsgerelateerde functionaliteiten kan plaatsvinden.

Ten opzichte van de Nulmeting is het gebruik van IPv6 licht gestegen. Er is wel beweging geconstateerd, maar de komende jaren moet nog blijken of alle plannen van ISP’s en andere organisaties ook tot uitvoer komen. Daarom is het belangrijk om de uitrol van IPv6 in Nederland de komende twee jaar te blijven monitoren.

[2] Standaarden in Behandeling, Open Standaarden, Forum Standaardisatie, www.open-standaarden.nl

2 Inleiding

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 IPv6 tijdig wordt opgenomen in het huidige internet, inclusief netwerken van overheden, bedrijven en consumenten. Hierdoor blijft de continuïteit van het gebruik van het Internet zoals het nu is gewaarborgd. IPv4 en IPv6 zullen in de komende decennia naast elkaar blijven bestaan.

Het opraken van de IP adressen is een wereldwijd probleem. Omdat 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 mogelijk 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.

In april 2010 heeft de eerste meting (gepresenteerd als “Nulmeting”) plaatsgevonden en deze werd op 26 juli 2010 gepubliceerd. De tweede meting is rondom oktober 2010 uitgevoerd en wordt in dit white paper gepresenteerd. In deze tweede meting komen dezelfde parameters aan bod als in de Nulmeting. Ten opzichte van de Nulmeting bevat de tweede meting twee nieuwe onderzoeksonderdelen:

- Interviews en enquêtes onder ISP’s, mobiele operators, overige bedrijven en overheden;
- Voordelen en tekortkomingen IPv6 n.a.v. security onderzoek.

In dit white paper komen net als in de Nulmeting vier hoofdonderwerpen aan de orde:

- 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 technologie;
- Veiligheid van IPv6 in relatie tot IPv4.

Dit whitepaper beschrijft de stand van zaken rondom oktober 2010, de tweede meting.
Verschillen met de Nulmeting worden geanalyseerd zodat duidelijk wordt op welke onderdelen de adoptie van IPv6 veranderd is. Met uitzondering van het managementuittreksel, inleiding, conclusies en nieuwe hoofdstukken (3.5 en 5.3) zullen de belangrijkste ontwikkelingen in de tekst worden aangegeven door middel van een dun balkje aan de linker zijde. De grafieken en tabellen in dit whitepaper zijn geupdate met de nieuwe resultaten van het afgelopen half jaar.

3 Introductie IPv6 naast IPv4

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[3]. 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 de inmiddels genomen initiatieven significant bij aan de adoptie?

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

3.2 Achtergrond

In deze paragraaf wordt enige achtergrondinformatie gegeven en is grotendeels overgenomen uit het rapport met de Nulmeting. Allereerst zal ingegaan worden op de achtergrond van het uitgifte proces van IP adressen. Vervolgens zal het belang voor Nederland besproken worden, evenals de stuwende kracht voor de almaar groeiende benodigde hoeveelheid IP adressen. Hierna wordt ingegaan op de opbouw van het IPv6 adres, en het verschil in uitgifte vergeleken met IPv4.

3.2.1 Het uitgifte proces van IP adressen

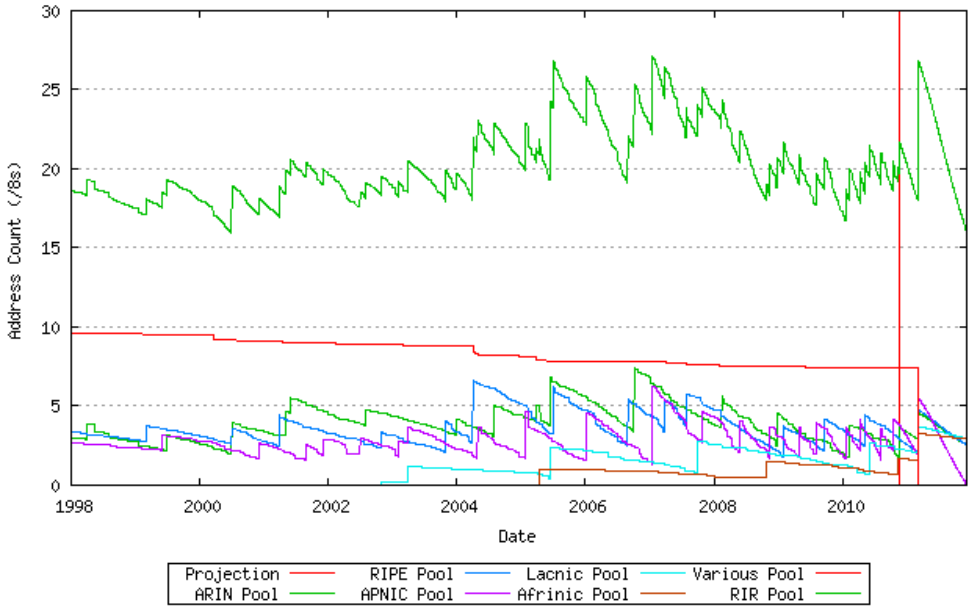
De wereldwijde coördinatie van de uitgifte van IP adressen wordt gedaan door de Internet Assigned Numbers Authority (IANA). IANA gaat zowel over de uitgifte van IPv4 als IPv6 adressen. De locale distributie van IP adressen wordt bewerkstelligd door Regional Internet Registries (RIR's), welke elk een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

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

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.

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[4] 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. De trend in de afgelopen jaren is dat de voorraden bij de RIR's steeds kleiner worden gehouden als het gevolg van het schaarser worden van IPv4 adressen en gewijzigde regelgeving door de IANA.



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

[4] Een /8 representeert een gedeelte van de IPv4 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.

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 27-09-2010 in totaal 23,6 miljoen[5] IPv4 adressen toegewezen gekregen en zal in de toekomst nog vele IP adressen meer gaan gebruiken. In de afgelopen 5 jaar zijn er ruwweg twee miljoen IPv4 adressen per jaar aangevraagd.

Met de invoering van IPv4 had men niet kunnen voorzien dat het Internet in de afgelopen 25 jaar zo'n vlucht zou nemen. Sinds begin jaren negentig speelt het 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.[6]

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[7] 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 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[8] internetaansluitingen	3,09	5,23	5,74
Mobiele telefoonaansluitingen	15,90	17,00	19,80
Totaal aantal aansluitingen	18,99	22,23	25,54

[5] Na de invoering van CIDR

[6] Met de invoering van CIDR (Classless Inter-Domain Routing) in 1993 wordt de totale adresruimte efficiënter 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 adresvoorraad.

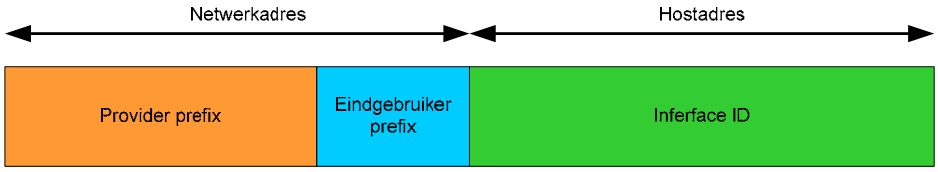
[7] Het totaal aantal huishoudens in Nederland in 2009 is ongeveer 6,6 miljoen.

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

In Tabel 1 is een overzicht gegeven van de internet- en mobiele telefoonaansluitingen in Nederland. Het aantal breedbandige internetaansluitingen nadert het aantal huishoudens[4] 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. Dat het gemiddeld aantal aansluitingen groter is dan 1 komt voornamelijk door apart gebruik van privé en zakelijke telefoontoestellen. 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 Network Address Translation (NAT) zullen de mogelijkheden met IPv4 uiteindelijk niet toereikend zijn. Hierdoor is de transitie naar 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 adresstructuur 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[9] versimpeld. Daarbij zullen door de inherente structuur van grote subnetten en subnet aggregatie het netwerkmanagement en de routering efficiënter 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 een Border Gateway Protocol (BGP) routeringstabel zoveel mogelijk beperkt blijft.

Normaal gesproken zal een ISP aanspraak maken op één of meerdere /32's. De ISP geeft vervolgens bijvoorbeeld een /48 of een /56 uit aan haar klanten met een vaste aansluiting. Dit betekent dat hiermee de eerste 48 of 56 bits van het IPv6 adres vast staan. Deze bits kunnen gezien worden als de provider prefix, zoals aangegeven in Figuur 3. Met de resterende bits in het netwerkadres, de eindgebruiker prefix, kunnen

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

door de klant nog verschillende subnetten gemaakt worden. Voor mobiele telefoons worden in het normale geval /64's uitgegeven.

3.3 ISP's als stakeholder

In 2009 is er voor het project *IPv6 Deployment Monitoring* een enquête uitgezet via de RIR's Ripe NCC en APNIC. Dit project wordt uitgevoerd voor de Europese Commissie[10], door TNO in samenwerking met GNKS Consult

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 nog een groot aantal kwesties waarvan ISP's aangegeven hebben ze als bottleneck voor de uitrol te ervaren[11].
Enkele belangrijke bottlenecks die de invoering van IPv6 belemmeren 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.

In 2010 is nogmaals een enquête gehouden, dit keer onder alle RIR's. De resultaten omtrent de belangrijkste bottlenecks zijn ten tijde van de tweede meting nog niet allemaal bekend. De resultaten die al wel bekend zijn zullen, daar waar toepasbaar, meegenomen worden in de bespreking van de tweede meting in paragraaf 3.4.

Met betrekking tot de belangrijkste bottlenecks om IPv6 nog niet in te voeren, komt uit laatstgenoemde enquête naar voren dat beperkte ondersteuning door fabrikanten vooral nog als grote belemmering wordt gezien voor de invoering van IPv6. Dit was afgelopen jaar ook al zo, maar in 2010 geeft een nog groter deel van de respondenten aan dat dit belangrijk is. Dit geldt voornamelijk voor partijen die al plannen hebben om IPv6 te gaan invoeren, maar ook voor partijen die nog geen plannen hebben.

[10] Meer informatie over het IPv6 Deployment Monitoring project kan gevonden worden op: http://www.ipv6monitoring.eu/
[11] IPv6 Deployment Monitoring Study Report (http://www.ipv6monitoring.eu/project-files?func=startdown&id=9)

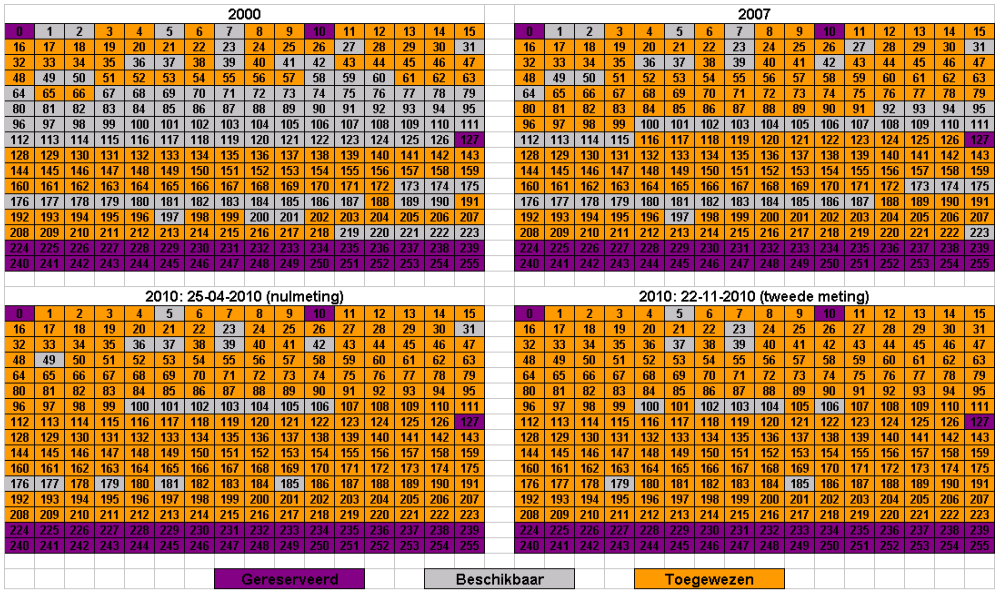
3.4 De tweede meting

Om de ontwikkelingen omtrent IPv6 in kaart te brengen is tweemaal een meting uitgevoerd. In deze sectie zullen de ontwikkelingen in het afgelopen halfjaar weergegeven worden om inzicht te 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 huidige uitrol van IPv6 besproken worden.

3.4.1 Leegloop IANA IPv4 adresvoorraad en uitgifte IPv4 adressen

Wereldwijd

In de afgelopen jaren is het aantal uitgegeven IPv4 adressen gestaag 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.



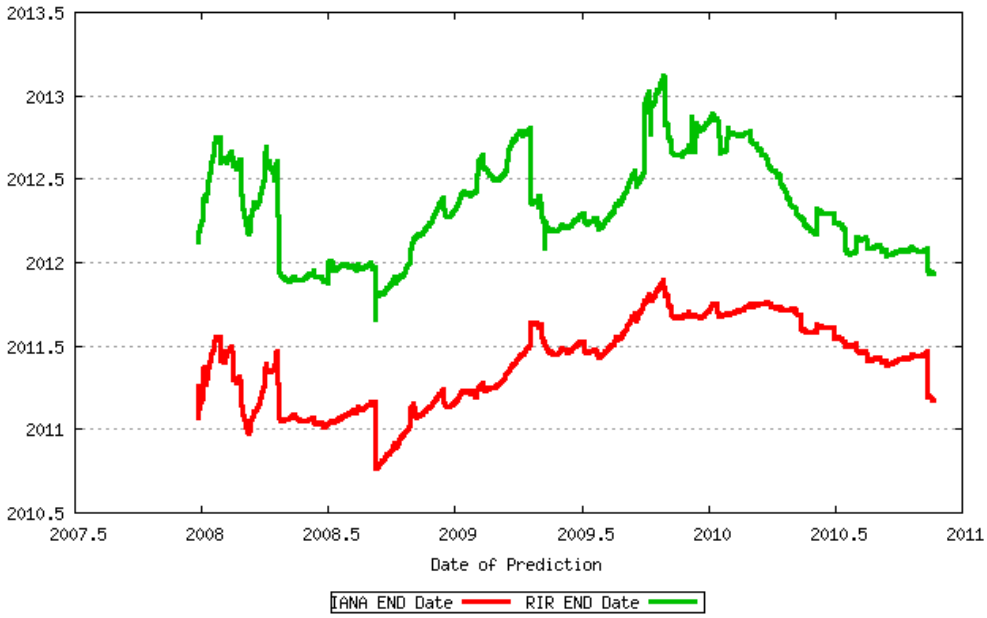
Figuur 4: De leegloop van de IPv4 adresvoorraad bij IANA, in vier verschillende tijdsvakken. De totale adresruimte bestaat uit 256 /8's. In elke tabel zijn de /8's grafisch weergegeven. De tabel rechtsonder geeft de stand van zaken per 22-11-2010 weer. Er is nog 4% (11/256) van de adressen (/8's) beschikbaar voor uitgifte.

Uit Figuur 4 valt op te maken dat nog ongeveer 4% (11/256) van de IPv4 adressen beschikbaar is voor uitgifte. Sinds de Nulmeting op 25 april 2010 zijn er negen /8's toegewezen aan verschillende RIR's. Er zijn verschillende voorspellingen over de consumptiesnelheid van IPv4 adressen en de datum waarop de adressen allemaal uitgegeven zijn. De meest geaccepteerde voorspelling is van Geoff Huston, een 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[12] houdt hij verschillende ontwikkelingen en statistieken bij. Geoff Huston voorspelt dat als de huidige trend van adresconsumptie doorzet, de IPv4 adresvoorraad bij IANA vanaf 4

[12] http://www.potaroo.net/

maart 2011[13] (t.o.v. 30 september 2011, gemeten op 01-04-2010) leeg zal zijn. Naar verwachting zal de eerste RIR in december 2011[13] (t.o.v. november 2012, gemeten op 01-04-2010) al zijn adressen hebben toegewezen. Voor de daadwerkelijke uitputtingsdatum moet rekening worden gehouden met enkele maanden spreiding ten opzichte van de voorspelde datum. Het meest waarschijnlijke scenario is dat APNIC als eerste door haar adressen heen is en dat RIPE NCC snel daarna zal volgen. Het is echter ook mogelijk dat RIPE NCC als eerste door haar adressen heen is.

Wanneer de uitputtingsdatum exact zal zijn is moeilijk te voorspellen. Het is mogelijk te verwachten dat er een 'last-minute' rush op de laatste adressen komt, op het moment dat de laatste adressen door IANA uitgegeven zijn aan de RIR's. Belangrijk is dat in bijna geen enkel model hiermee rekening gehouden is, omdat dit moeilijk te voorspellen is uit de uitgifte data van afgelopen jaren. Daarbij wordt de voorspellingsdatum steeds onbetrouwbaarder naarmate de uitputtingsdatum dichterbij komt. Er moet rekening worden gehouden met het feit dat de uitputtingsdatum van RIPE NCC en andere RIR's snel dichterbij kan komen op het moment dat de IANA adresvoorraad leeg is.



Figuur 5: Voorspelling van de uitputtingsdatum voor IPv4, uitgezet tegen de datum waarop de voorspelling is gedaan. De discontinuïteiten worden veroorzaakt door veranderingen in het uitgiftebeleid van IANA. (bron: potaroo.net)

In Figuur 5 is de voorspelling van de uitputtingsdatum voor IPv4 grafisch weergegeven, ten opzichte van de datum waarop de voorspelling is gedaan. Het afgelopen halfjaar is de uitputtingsdatum steeds verder naar voren gekomen en wijst erop dat in 2011 de IPv4 adresvoorraad van IANA volledig uitgeput zal zijn. Deze trend is te verklaren door het toenemen van de vraag naar IPv4 adressen. Aan de rechter kant van de grafiek is een discontinuïteit te zien die ontstaat door het uitgeven van één of meerdere /8's tegelijk. Doordat de uitgifte van adressen in relatief grote blokken gebeurt, zullen nu de laatste adresblokken uitgegeven worden de komende tijd meer van deze sprongen in deze grafiek te zien zijn.

[13] Gemeten op 22 november 2010

Tabel 2: Het aantal toegewezen IPv4 adressen (in miljoenen /32's)[14]

	2005	2006	2007	2008	2009	27-09-2010
Toegewezen adressen wereldwijd	174,4	168,3	204,1	203,5	189,7	169,3
Relatieve groei wereldwijd	8,6%	7,6%	8,6%	7,9%	6,8%	5,7%
Toegewezen adressen Nederland	2,12	1,72	1,87	0,91	2,08	0,77
Relatieve groei Nederland	14,9%	10,1%	10,3%	4,6%	10,0%	3,4%

Na een groei in uitgifte van IPv4 adressen in 2007, is in 2008 en 2009 het aantal uitgegeven adressen steeds afgenomen, zoals aangegeven in Tabel 2. Deze afname werd voornamelijk veroorzaakt door een lagere toewijzing vanuit RIPE NCC en ARIN. De uitgifte in 2010 lijkt weer te stijgen ten opzichte van voorgaande jaren. Als gevolg van deze ontwikkeling schuift de uitputtingsdatum van IPv4 weer wat naar voren, terwijl deze in 2009 juist naar achteren schoof.

De IPv4 uitgifte wordt op dit moment voornamelijk gedreven door de aanvragen bij de APNIC (55% in 2010) die de afgelopen 5 jaar al een stijgende lijn in uitgifte laat zien, zoals weergegeven in Tabel 3. De consumptie van IPv4 adressen in Zuid-Oost Azië (APNIC) kan voornamelijk toegewezen worden aan China en Japan.

Tabel 3: IPv4 adres uitgifte, verdeling onder de RIR's[14]

	2005	2006	2007	2008	2009	27-09-2010
RipeNCC	35%	33%	30%	22%	23%	20%
ARIN	27%	28%	26%	28%	22%	13%
APNIC	31%	31%	34%	44%	46%	55%
LACNIC	6%	7%	7%	6%	6%	8%
AfriNIC	1%	2%	3%	1%	3%	4%

Nederland
Als het aantal toegewezen IPv4 adressen wereldwijd vergeleken wordt met Nederland, dan is te zien dat in de periode januari tot en met september 2010 de vraag binnen Nederland niet zo sterk groeit als wereldwijd. Uit Tabel 2 blijkt dat Nederland in 2010 ongeveer 0,77 miljoen adressen toegewezen heeft gekregen, ten opzichte van ruim 2 miljoen in 2009. Het totale aantal IPv4 adressen dat Nederland t/m 27-09-2010 heeft aangevraagd komt daarmee op ruim 23,6 miljoen.

3.4.2 De adoptie van IPv6

3.4.2.1 Uitgifte IPv6

Wereldwijd
De uitgifte van IPv6 adresblokken is gaande sinds 1999. Een overzicht van de huidige toewijzingen is te vinden in Tabel 4. In Azië zijn het afgelopen jaar de meeste IPv6 adressen toegewezen. Het valt op dat een relatief groot deel van de IPv6 adressen, die in Europa gealloceerd worden, ook direct geadverteerd wordt (94,93%). Deze

[14] Door geüpdate uitgifte gegevens van verscheidene RIR's kunnen waardes van voorgaande jaren verschillen van de waarden weergegeven in het rapport met de nulmeting.

ontwikkeling is het afgelopen jaar ook waar te nemen in Azië en Oceanië, waar respectievelijk 88,13% en 99,96% wordt geadverteerd.

Tabel 4: Totale aantal toegekende en geadverteerde IPv6 /48's (in miljoenen) op 31-12-2009 en 27-09-2010. Het verschil in aantal tussen 2009 en 2010 is aangegeven met Δ.[15]

	Amerika		Europa		Azië		Afrika		Oceanië	
	2009	*2010*	*2009*	*2010*	*2009*	*2010*	*2009*	*2010*	*2009*	*2010*
Gealloceerd	5316,1	5336,5	2243,1	2263,1	1079,7	1244,7	4,1	5,4	549,5	553,5
Δ	20,4		20,0		65,0		1,3		4,0	
Geadverteerd	33,8	45,0	2132,0	2148,3	773,8	1097,0	1,6	2,0	272,6	553,3
Δ	11,2		16,3		323,2		0,4		280,7	

Tabel 5: Aantal individuele IPv6 toewijzingen (ongeacht adresblokomvang) bij de Regional Internet Registries (RIR's)[15]

	2005	2006	2007	2008	2009	27-09-2010
RipeNCC	96	92	163	437	633	626
ARIN	59	71	215	235	394	433
APNIC	54	43	63	162	191	540
LACNIC	31	16	27	30	35	25
AfriNIC	3	18	20	17	14	32
Totaal	243	240	488	881	1267	1656

Tabel 5 is een overzicht gegeven van het aantal individuele IPv6 toewijzingen (ongeacht adresblokomvang). In het jaar 2010 is er plotseling een enorme stijging te zien in het aantal aanvragen bij APNIC. Australië en China samen hebben met 180 aanvragen in 2010 bijna net zoveel aanvragen als er in totaal in 2009 gedaan zijn. Ook Indonesië lijkt met de adoptie van IPv6 te beginnen door middel van een grote stijging in aanvragen. In de eerste 8 maanden van 2010 heeft Indonesië al 55 aanvragen gedaan, ten opzichte van 32 in de periode van 1999 t/m 2009.

Hoewel het aantal aanvragen voor IPv6 adresblokken in de afgelopen jaren vooral door RIPE NCC en ARIN werden gedomineerd, zijn de landen die bediend worden door APNIC met een flinke opmars bezig. Waar de verklaring voor het grote aantal aanvragen in West-Europa en Noord-Amerika vooral te duiden is aan de meer volwassen internetmarkt en de hoge internetpenetratie, is de stijging van het aantal IPv6 aanvragen in Azië en Oceanië vooral te duiden aan een algehele groei van het gebruik van IP adressen. Zowel voor IPv4 en IPv6 adressen is een duidelijke stijging te zien in het aantal individuele aanvragen en ook het aantal IP adressen.

Nederland

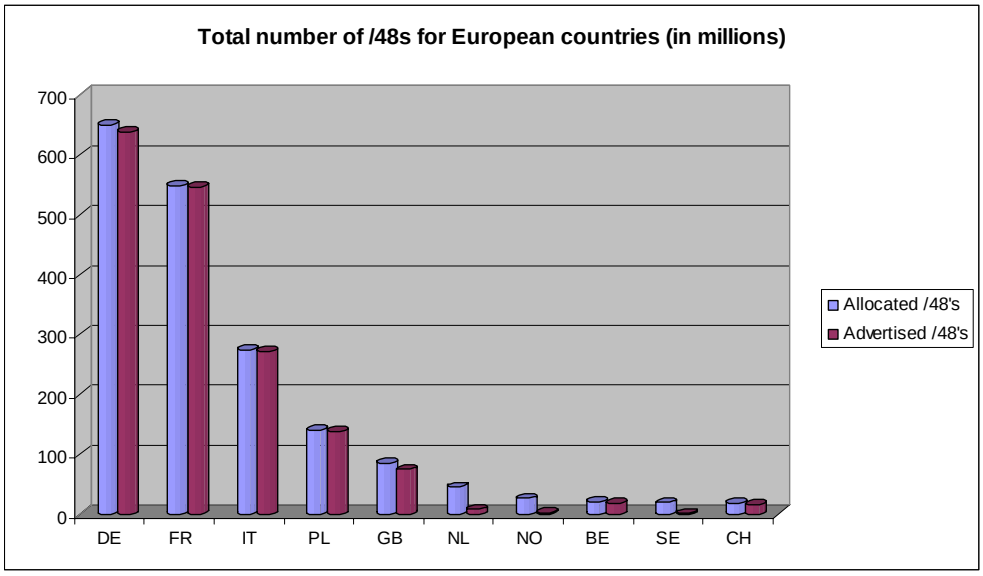
In Tabel 6 is te zien dat in 2009 er door Nederland 3 miljoen IPv6 /48's zijn aangevraagd. In 2010 heeft Nederland 2,56 miljoen /48's aangevraagd en komt hiermee op de 10e plek. Ten opzichte van voorgaande jaren is een constante continuering in de aanvraag van IPv6 adressen waar te nemen, met af en toe een grote uitschieter. Dit jaar zijn in Japan bijvoorbeeld twee /22's aangevraagd.

[15] Door geüpdate uitgifte gegevens van verscheidene RIR's kunnen waardes van voorgaande jaren verschillen van de waarden weergegeven in het rapport met de nulmeting.

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

2007		2008		2009		27-09-2010	
Australië	268,89	Brazilië	4307,55	VS	15,28	Japan	145,29
Engeland	68,75	VS	948,83	Duitsland	9,44	VS	24,12
Japan	67,44	Zweden	9,37	Engeland	4,06	China	22,02
VS	8,19	Frankrijk	5,37	**Nederland**	3,01	België	17,24
Duitsland	5,77	Duitsland	4,52	Australië	2,88	Zweden	5,37
Taiwan	4,26	Engeland	2,36	Rusland	2,88	Australië	5,05
Polen	1,18	**Nederland**	2,23	Japan	2,22	Duitsland	3,93
Uruguay	1,05	Rusland	2,16	Frankrijk	1,64	Engeland	3,87
Canada	0,85	Zwitserland	2,16	Tsjechië	1,44	Rusland	3,15
Rusland	0,72	China	1,70	Zweden	1,44	**Nederland**	2,56

Als er vervolgens gekeken wordt naar het percentage van de adressen dat wordt geadverteerd in de routeringstabellen dan is dit nog maar 13,65%. Ten opzichte van 2009 is hier weinig in veranderd. Zoals weergegeven in Figuur 6, loopt Nederland hierin nog steeds achter op de top 5 Europese landen. Van de nieuw aangevraagde IPv6 adressen in 2010 wordt 63% geadverteerd.



Figuur 6: 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 30-08-2010.

3.4.2.2 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 7 is te zien dat binnen Europa een belangrijk marktaandeel wordt ingenomen door Windows XP, maar dat dit de laatste anderhalf jaar dalende is. In Windows XP

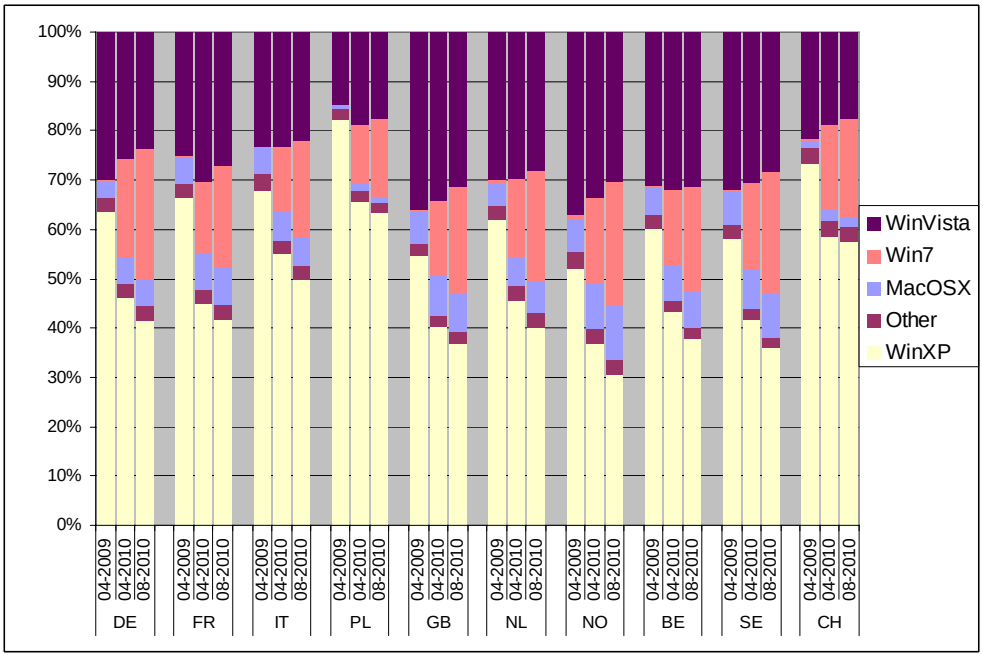
wordt IPv6 niet direct ondersteund, maar kan de IPv6 stack wel geïnstalleerd worden[16]. Daarnaast verlopen DNS requests bij Windows XP altijd over IPv4.

Ten opzichte van de Nulmeting is de stijgende trend in groei van Windows 7 doorgezet. Op 1 september 2010 werd er een persbericht vrijgegeven dat Windows 7 ruim een jaar na de introductie wereldwijd een groter marktaandeel heeft verworven dan Windows Vista[17]. Hiermee is te verwachten dat het marktaandeel van Windows 7 de komende jaren blijft groeien en een steeds groter gedeelte van Windows XP overneemt.

Windows 7, Windows Vista en MacOSX ondersteunen IPv6. In Figuur 7 is te zien dat voor 7 van de 10 weergegeven landen het gezamenlijke percentage van deze drie besturingssystemen al boven de 50% ligt.

Nederland

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



Figuur 7: Marktaandeel besturingssystemen (procentueel) voor de top 10 Europese landen met de meeste IPv6 allocaties

3.4.2.3 Ondersteuning van IPv6 door ISP's

In deze Paragraaf wordt gekeken naar het aantal ISP's dat op dit moment native IPv6 verbindingen kan leveren aan gebruikers. Een overzicht van de plannen en voorbereidingen van ISP's die nog geen IPv6 aanbieden wordt gegeven in Paragraaf 3.5.1.

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

[16] 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.

[17] http://gs.statcounter.com/press/windows-7-jumps-ahead-of-vista-globally-for-first-time

deze website is een overzicht te vinden met de belangrijkste ISP's, onderverdeeld per land.

In Figuur 8 zijn deze resultaten weergegeven in een staafdiagram. Sinds de Nulmeting is het aantal ISP's in Duitsland gegroeid van 10 naar 12, in de VS van 9 naar 10, en het aantal ISP's in Zwitserland van 6 naar 8. Het valt op dat de absolute aantallen die weergegeven zijn in de figuur vrij laag zijn en dat er ten opzichte van de Nulmeting weinig nieuwkomers zijn.

Uit de genoemde enquête in paragraaf 3.3 komt naar voren dat inmiddels 42% van de ondervraagde ISP's (waaronder access providers en hosting providers) in Europa enkele klanten hebben die IPv6 gebruiken, tegenover 34% in 2009. Verder geeft ruim 85% van de ondervraagde ISP's aan dat ze inmiddels plannen hebben gemaakt of IPv6 al uitgerold hebben. Daarbij zegt nog maar 9% dat ze IPv6 niet zullen promoten naar hun klanten, ten opzichte van 43% in 2009.

Nederland

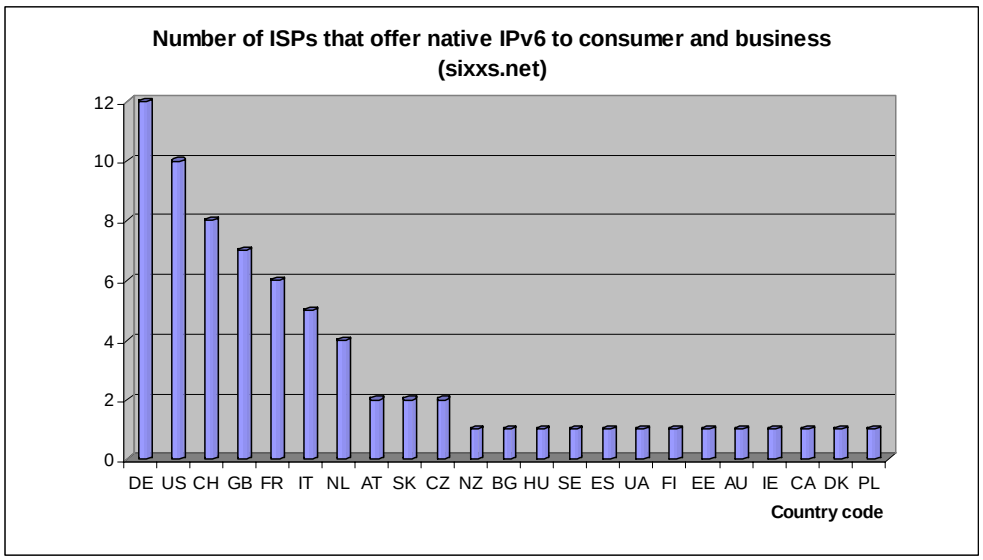
In vergelijking tot andere landen presteert Nederland gemiddeld als gekeken wordt naar het aantal ISP's dat native IPv6 verbindingen aanbiedt. Buiten de gegevens van sixxs.net zijn er in Nederland nog enkele ISP's te vinden die IPv6 verbindingen aanbieden aan een beperkte klantgroep.

In totaal zijn er elf 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. Sinds de Nulmeting zijn hier Intermax, Luna, Tele2, KPN International en Global Crossing bijgekomen. Ten tijde van de Nulmeting bood XS4ALL al als enige IPv6 aan voor een beperkte groep consumenten, maar vanaf 26 augustus 2010 is het mogelijk IPv6 aan te zetten voor alle klanten met een een XS4all-only abonnement[18,19].

XS4ALL was reeds opgenomen in het overzicht in Figuur 8, dus levert hierin geen extra stijging op. Het grotere aanbod op de zakelijke markt wordt deels veroorzaakt door een groter aanbod aan ISP's, alsmede de vraag vanuit bedrijven om met IPv6 te kunnen experimenteren.

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

[19] http://www.computable.nl/artikel/ict_topics/internet/3487453/1282763/xs4all-maakt-ipv6-voor-mkb-beschikbaar.html



Figuur 8: Aantal ISP's per land dat commercieel IPv6 verbindingen aanbiedt aan consumenten en/of zakelijke gebruikers per 15-10-2010 (bron: sixxs.net)

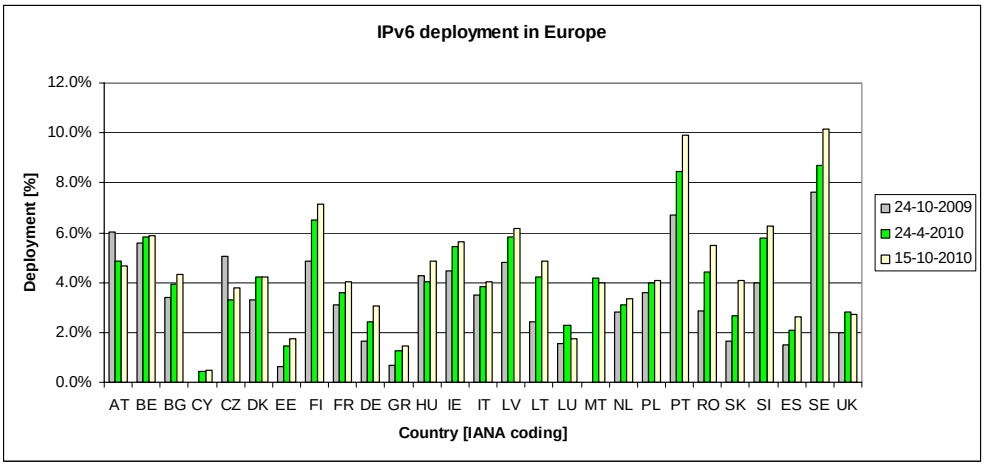
3.4.2.4 Daadwerkelijk IPv6 gebruik

Binnen het project *IPv6 Deployment Monitoring*[20], uitgevoerd door TNO en GNKS Consult, 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 elke Europese lidstaat de top 500 van de meest populaire websites genomen (bron: http://www.alexa.com).

Europa

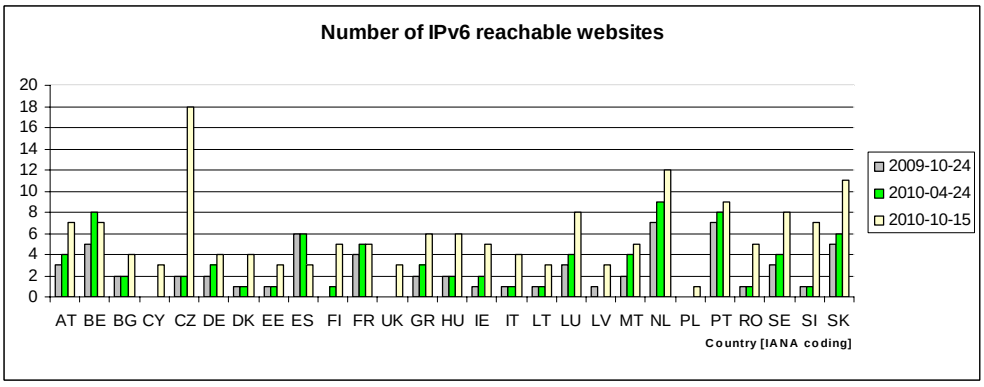
In Figuur 9 staat een overzicht van het percentage IPv6 gebruikers per EU lidstaat. Gemiddeld gezien is er een kleine stijging te constateren in het aantal gebruikers, ten opzichte van de vorige twee meetpunten. De landen Zweden, Portugal en Finland lopen voorop met het aantal IPv6 gebruikers, waarbij voor Portugal rekening gehouden moet worden met een kleine bias richting meer IPv6 gebruikers als gevolg van de gebruikte meetwebsite in het IPv6 domein. Voor de landen waarbij het percentage onder de 3% uitkomt, zijn de aantallen te laag om iets representatiefs te kunnen zeggen over de stijging of afname van het percentage IPv6 gebruikers. Ook uit de genoemde enquête in paragraaf 3.3 blijkt dat het IPv6 gebruik slechts licht stijgt onder de klanten van responderende ISP's.

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



Figuur 9: Percentage van internet gebruikers dat IPv6 gebruikt (bron: ipv6monitoring.eu) per 24 oktober 2009, 24 april 2010 en 15 oktober 2010.

De resultaten gepresenteerd in Figuur 10 zijn niet direct vergelijkbaar als gevolg van de wijziging in de meetmethode sinds de Nulmeting[21]. Als gevolg van deze wijziging is het aantal sites voor de meeste lidstaten toegenomen, waarbij een enorme toename is te constateren voor Tsjechië.



Figuur 10: 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 24 oktober 2009, 24 april 2010 en 15 oktober 2010. Als gevolg van een wijziging in de meetmethode zijn de cijfers niet direct te vergelijken[21].

Nederland

In vergelijking met andere landen laat Nederland een gemiddelde adoptie zien van IPv6. In Figuur 9 laat zien dat ruim 3% van de gemeten 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 nog steeds voorop in Europa, ook al is het absolute aantal laag met 12 uit 500 gemeten websites.

[21] Sinds de nulmeting is de meetmethode aangepast. In plaats van alleen na te gaan of het volledige internetadres (bijv. www.google.com) over IPv6 bereikbaar is, wordt nu ook naar subdomeinen gekeken zonder www en met ipv6 (bijv. google.com en ipv6.google.com)

3.5 Voorbereidingen en plannen bij ISP´s, andere bedrijven en overheden

Uit paragraaf 3.4.2.3 blijkt dat er nog weinig ISP´s zijn, waarbij klanten een IPv6 verbinding kunnen afnemen. De belangrijkste vraag is of de ISP´s die nu nog geen IPv6 internetverbindingen aanbieden ver genoeg zijn met hun voorbereidingen om IPv6 verbindingen aan te bieden wanneer er straks geen nieuwe IPv4 adressen meer beschikbaar zijn. Om een beeld te krijgen van de status van uitrol bij Nederlandse ISP´s zijn interviews gehouden met de grootste ISP´s en netwerk operators in Nederland.

Als ISP´s straks IPv6 internetverbindingen gaan leveren aan hun klanten, dan zal dit in verschillende mate impact hebben op het netwerk van de eindgebruiker. Om inzicht te krijgen in de mate waarin IPv6 leeft bij dergelijke organisaties en welke voorbereidingen zij treffen is een digitale enquête uitgezet onder overheden en bedrijven.

3.5.1 ISP's en netwerk operators

IPv6 kan worden gezien als een noodzakelijke technische aanpassing, die moet voorkomen dat het internet niet meer kan groeien als vanaf 2011/2012 op steeds meer plaatsen geen nieuwe IPv4 adressen meer beschikbaar zijn. Het leveren van internetconnectiviteit behoort tot de kernactiviteiten van ISP's en zij spelen daarmee een centrale rol als het gaat om de introductie van IPv6. Om een beeld te krijgen van de plannen en activiteiten die deze partijen hebben zijn verschillende ISP's hierover geïnterviewd.

De geïnterviewde partijen zijn ISP's die hun internetdiensten leveren over een eigen infrastructuur. Zij zijn dus naast ISP ook netwerk operator en in sommige gevallen kunnen ook andere ISP's gebruik maken van hun netwerk om diensten te leveren.

Van de aanbieders van vaste internetaansluitingen zijn zeven partijen geïnterviewd die gezamenlijk bijna 90%[22] van het marktaandeel hebben als het gaat om consumenteninternet. Deze partijen beschikken bovendien over een eigen netwerkinfrastructuur.

Van de mobiele operators zijn de drie partijen geïnterviewd die gezamenlijk 100%[22] van de Nederlandse infrastructuur in handen hebben, als het gaat om mobiele telefoonaansluitingen. 84,4% van de mobiele aansluitingen wordt ook onder een merknaam van deze partijen verkocht, terwijl 14,6% van de aansluitingen door MVNO's (Mobiele Virtuele Netwerk Operators) wordt aangeboden.

Waar in Figuur 8 alleen ISP's worden meegerekend die IPv6 op dit moment aan klanten aanbieden, is bij de interviews ook gekeken naar de planning, de getroffen voorbereidingen en de afwegingen die voor ISP's een rol spelen bij de introductie van IPv6 en het naderende einde van de IPv4 adresvoorraad. Deze interviews geven dus een vollediger beeld over de mate waarin Nederland voorbereid is op IPv6, in plaats van enkel te kijken naar IPv6 aanbieders.

[22] Bron: Marktrapportage Elektronische Communicatie, TNO, mei 2010

Omdat een deel van de geïnterviewde partijen hun activiteiten op het gebied van IPv6 niet publiek heeft gepresenteerd, is er voor gekozen de bevindingen in deze monitor te aggregeren. De interviews zijn gehouden in de periode april tot en met september 2010.

Opraken IPv4 adressen op LIR niveau
Het uitgifteproces van IP adressen is beschreven in Paragraaf 3.2.1 en kent drie hiërarchische niveaus. Op het mondiale niveau, IANA, is de voorspelde datum waarop alle IPv4 adressen zijn uitgedeeld 4 maart 2011. Op regionaal niveau zal bij RIPE naar verwachting eind 2011 het laatste IPv4-adresblok wordt uitgegeven. Op het derde niveau, het LIR-niveau, is geen eenduidige datum aan te geven, omdat dit afhankelijk is van de voorraden die individuele ISP's hebben en dit maken zij over het algemeen niet openbaar.

De geïnterviewde ISP's is gevraagd naar het moment waarop zij verwachten door hun IPv4 adresvoorraad heen te zijn. Drie partijen geven aan dat deze datum hooguit enkele maanden later ligt dan het moment waarop bij RIPE NCC de adressen op zijn. De overige partijen geven aan nog jaren vooruit te kunnen met hun huidige adresvoorraad tot 2014 of zelfs later. Hierbij speelt een belangrijke rol dat de Nederlandse markt van vast consumenteninternet vrijwel verzadigd is. Dit betekent dat het klantenbestand van ISP's niet snel sterk zal groeien en dat vertaalt zich dan in een beperkte adresconsumptie. De ISP's geven aan dat adresconsumptie met name gedreven zal worden door mobiele aansluitingen en eventuele nieuwe diensten, die onverwacht snel zullen groeien.

Redenen en belemmeringen voor de invoering van IPv6
In overeenstemming met het stuk over adresvoorraden geven de meeste geïnterviewde partijen aan dat het waarborgen van de continuïteit van hun bedrijfsvoering de belangrijkste reden is voor het invoeren van IPv6 en niet het IPv4 adrestekort van de organisatie op zichzelf. Dit tekort is wel de achtergrond hiervan, maar of het de reden is om nu al met IPv6 te beginnen hangt af van het moment waarop partijen verwachten door hun IPv4 adresvoorraad te zijn. Ongeacht deze adresvoorraad willen vrijwel alle partijen rond 2012 klaar zijn om consumenten aan te kunnen sluiten op internet met IPv6. Tabel 7 geeft de redenen om met IPv6 aan de slag te gaan, waar vaste en mobiele operators zich het meest in herkennen.

Tabel 7: Meest gegeven antwoorden door ISP's op de vraag wat de belangrijkste reden is om plannen te hebben op het gebied van IPv6, op volgorde van aantal.

1.	We zien het als een noodzakelijke investering voor de continuïteit van onze bedrijfsvoering
2.	Past in het innovatieve karakter van onze organisatie
3.	Spreiden van investeringen door nu al te beginnen
4.	We willen niet achterop raken op onze concurrenten
5.	Gebrek aan IPv4 adresruimte
6.	We willen bereikbaar zijn op IPv6 voor potentiële klanten en services

Tijdens de interviews is de partijen ook gevraagd naar vertragende factoren om met IPv6 aan de slag te gaan en naar de verwachte knelpunten bij de introductie van IPv6. Hierbij worden hoofdzakelijk de vier redenen in Tabel 8 genoemd. De eerste drie factoren zijn gerelateerd aan de business: IPv6 op zich levert ISP's geen extra omzet op, maar vraagt wel investeringen. De vierde factor wordt vaak genoemd als het gaat om

bepaalde functionaliteiten in producten, die voor IPv4 wel zijn geïmplementeerd, maar voor IPv6 (nog) niet. Daarnaast zijn veel apparaten die IPv6 wel zeggen te ondersteunen vaak nog niet in een omvangrijke productieomgeving gebruikt, waardoor mogelijke problemen nog niet zijn ontdekt. De algemene verwachting is dat dit geen onoverkomelijke problemen zijn, maar dat het wel tijd kost tijd om ze te ontdekken en met de leverancier op te lossen.

Tabel 8: Vertragende factoren bij de introductie van IPv6.

1.	De introductie kost tijd en geld
2.	Er zijn onvoldoende businessvoordelen in relatie tot IPv6
3.	Er is geen vraag in de markt
4.	Producten en diensten ondersteunen IPv6 nog onvoldoende

IPv6 introductiestrategie
De geïnterviewde ISP's zien het aanbieden van IPv6 niet als doel op zich. ISP's leveren aan klanten internetverbindingen en hiervoor zal bij het merendeel alleen IPv6 worden gebruikt als dat noodzakelijk is. Deze noodzaak wordt in de consumentenmarkt naar verwachting bepaald door een gebrek aan IPv4 adressen aan de ISP-zijde. In dat geval kan een ISP er voor kiezen om volledig zelf te bepalen welke klanten op welk moment een IPv6 aansluiting krijgen, omdat zij weinig tot geen rekening hoeft te houden met de vraag uit de markt. Het voordeel hiervan is dat de ISP op deze manier zelf de regie houdt over de tijdslijnen voor de introductie van IPv6 in haar netwerk. De consequentie van deze aanpak is dat IPv6 bij een ISP niet in één keer voor alle consumenten beschikbaar komt, maar met de tijd langzaam zal groeien. Een deel van de ISP's geeft overigens aan dat consumenten op een bepaald moment wel op aanvraag een IPv6 verbinding kunnen krijgen.

In de zakelijke markt zal het veel gangbaarder zijn dat IPv6 verbindingen worden geleverd als klanten hier zelf om vragen. In deze markt is meestal sprake van een intensievere afstemming tussen klant en ISP, waardoor dit mogelijk is. De geïnterviewde partijen geven aan dat het over het algemeen eenvoudiger is om bedrijven te voorzien van een IPv6 internetaansluitingen dan consumenten.

Plannen voor de introductie van IPv6
In de interviews is gevraagd naar de concrete plannen van de ISP's. Hierbij is onderscheid gemaakt tussen drie fases:
- voorbereidingen;
- introductie van IPv6 in het netwerk;
- het aanbieden van diensten via IPv6.

Bij *voorbereidingen* is gevraagd naar het in kaart brengen van de urgentie van IPv6, het opleiden van personeel, het vragen naar ondersteuning van IPv6 in producten en diensten en het aanvragen van een IPv6 adresblok.

Bij *introductie* is gevraagd naar de plannen om het core-netwerk, het accessnetwerk en de thuisrouter klaar te maken voor IPv6.

Bij het *aanbieden van diensten* is gevraagd wanneer klanten naar verwachting een IPv6 internetverbinding bij de ISP kunnen afnemen.

Alle geïnterviewde patijen hebben de voorbereidingsfase er al op zitten, of zitten momenteel in een vergevorderd stadium hiervan. Als het gaat om de introductie van IPv6 in het netwerk, dan is het core-netwerk bij de meeste partijen in 2010 afgerond. Wat betreft het gereedmaken van het accessnetwerk liggen de antwoorden tussen 2011 en 2013, waarbij het zwaartepunt in 2012 ligt. Het daadwerkelijk aanbieden van IPv6 internetverbindingen naar consumenten wordt momenteel al gedaan door één partij. Op basis van de huidige plannen zal de helft van de overige partijen halverwege 2011 de eerste consumenten kunnen aansluiten op IPv6. De andere partijen zullen vanaf 2012 volgen, afhankelijk van de noodzaak die zij op dat moment zien. De overgang naar IPv6 zal daarna gestaag plaatsvinden. Het moment waarop alle consumenten een IPv6-internetverbinding zullen hebben kunnen partijen moeilijk aangeven, maar dit zal zeker niet voor 2015 zijn.

De deelnemers geven aan dat het via IPv6 aansluiten van zakelijke klanten vaak eenvoudiger is dan consumenten. Enkele partijen kunnen dit momenteel ook al.

Compatibiliteit met het IPv4 internet
Bij verschillende partijen zal IPv6 niet direct de oplossing betekenen voor hun probleem van IPv4 adresschaarste. Zo geldt voor mobiele operators dat veel mobiele telefoons op dit moment nog geen IPv6 ondersteunen. Voor vaste operators geldt dat er nog veel IPv4-only apparatuur bij klanten staat. Maar het belangrijkste in deze context is misschien nog wel de manier waarop content wordt aangeboden. Momenteel wordt het overgrote deel hiervan alleen maar op IPv4 aangeboden. Zolang dit het geval blijft zullen ISP's ook connectiviteit moeten verzorgen naar deze IPv4-websites voor hun nieuwe aansluitingen die straks wel een IPv6 adres hebben, maar geen publiek IPv4 adres meer. Alle partijen geven aan dat hun doel het realiseren van een *dual-stack* netwerk met publieke IP adressen is, maar dat kan niet meer wanneer ze door hun IPv4 adressen heen zijn.

Om de nieuwe IPv6 gebruikers toch toegang te kunnen bieden naar de IPv4 wereld, zullen ISP's genoodzaakt zijn om oplossingen te gebruiken om hun IPv4 adresgebruik te verlengen. Een belangrijk techniek die hierbij gebruikt kan worden is NAT. Dit is een technologie, waarbij meerdere klanten van een ISP één of meerdere (publieke) IP-adressen delen, door in het ISP netwerk een adresvertaling te doen. Een dergelijke oplossing wordt door de meeste geïnterviewde vaste operators als onwenselijk gezien, omdat het naar verwachting extra investeringen, complexiteit en beheerlast met zich meebrengt. Daarnaast is de verwachting dat deze oplossing niet voldoende schaalbaar is. Deze oplossing wordt dan ook alleen overwogen door ISP´s, met een beperkte voorraad IPv4 adressen. Bij mobiele operators is het gebruik van NAT in het operator netwerk nu al gangbaar. Op het gebied van IPv6-IPv4 vertaalservices hebben de meeste partijen momenteel geen serieuze plannen, al kan men zich voorstellen dat het in sommige gevallen een oplossing kan bieden.

Andere diensten
Bij de introductie van IPv6 ligt de nadruk op het leveren van een IPv6 internetverbinding. Aan andere diensten zoals VoIP, IPTV en email wordt geen prioriteit gegeven. Mochten er nieuwe diensten worden geïntroduceerd waarvoor veel IP adressen nodig zijn, dan kan dit een aanjager zijn voor het gebruik van IPv6. Eén en ander hangt ook samen met het feit of een ISP ervoor kiest om voor een dienst private

of publieke IP adressen te gebruiken. Voor bijvoorbeeld VoIP, worden vaak private adressen gebruikt en dit kan voorlopig nog uitstekend werken.

Wat betreft het aanzetten van IPv6 op webservers wordt door ISP´s opgemerkt dat dit eenvoudig te realiseren is, maar dat men geen invloed heeft op webpagina's, die op de server draaien. Deze webpagina's zullen in sommige gevallen met de 128-bit grote IPv6 adressen om moeten kunnen gaan wanneer mensen ze op IPv6 benaderen. Denk hierbij bijvoorbeeld aan gastenboeken die IP adressen weergeven en/of opslaan. Omdat dit buiten de invloed van de hosting provider ligt is men terughoudend met het aanzetten van IPv6 voor alle pagina's.

3.5.2 Bedrijven en overheden

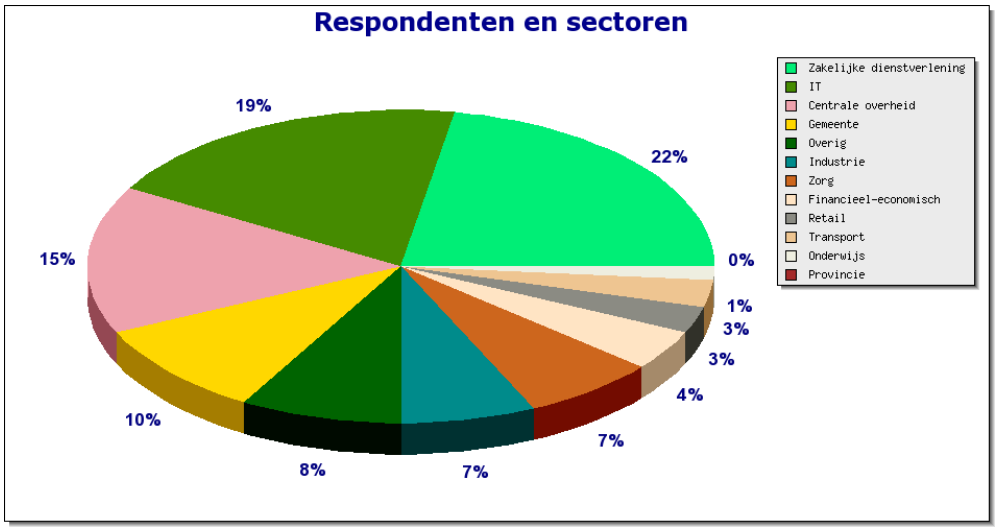
Naast de aanbieders – ISP's – zijn ook de gebruikers een belangrijke partij als het gaat om internet. Consumenten zullen naar verwachting voor het grootste deel hun ISP volgen als het gaat om IPv6 en hier in veel gevallen niet eens van op de hoogte zijn. Voor organisaties is het echter van belang hier beter over na te denken.

Om een beeld te krijgen hoe IPv6 leeft bij bedrijven en overheden is er een enquête uitgezet met vragen aan organisaties over hun bekendheid met en plannen op het gebied van IPv6. De enquête is uitgezet op verschillende plaatsen, waaronder de Vereniging van Nederlandse Gemeenten, de 'fortune 500' bedrijven in Nederland in samenwerking met ICT Media en de Interdepartementale Commissie van CIO's (ICCIO) van de Rijksoverheid. In totaal is op deze manier aan ruim 2000 individuen het verzoek gedaan de IPv6 enquête namens hun organisatie in te vullen. Uiteindelijk hebben 72 organisaties de enquête ingevuld.

Het is belangrijk om te vermelden dat IPv6 in mei 2010 is aangemeld om opgenomen te worden op de "pas toe of leg uit"-lijst van Open Standaarden[23] voor de overheid. Dit betekent dat overheden bij ICT-aanbestedingen om IPv6 moeten vragen en expliciet moeten toelichten als men voor een product of dienst kiest, waarbij IPv6 niet wordt ondersteund. De opname van IPv6 op deze lijst kan een impuls geven aan het gebruik van IPv6 bij de overheid en leveranciers van de overheid. In november 2010 wordt definitief besloten door het College Standaardisatie of IPv6 wordt toegevoegd aan de lijst.

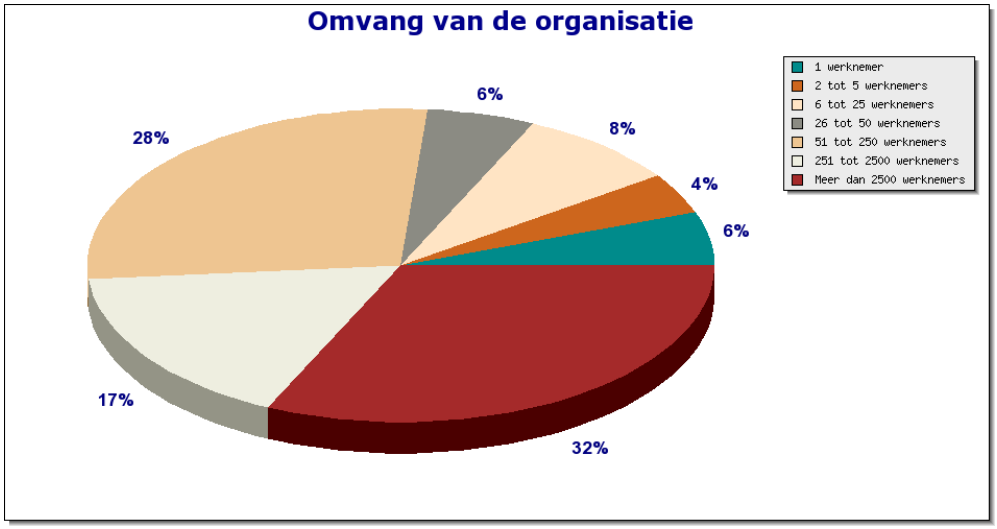
Bevindingen
Bij het uitzetten van de enquête is geprobeerd om organisaties in allerlei sectoren te bereiken en niet alleen organisaties in de IT sector. Figuur 11 geeft de verdeling van de organisaties die de enquête hebben ingevuld over verschillende sectoren.

[23] Standaarden in Behandeling, Open Standaarden, Forum Standaardisatie, www.open-standaarden.nl

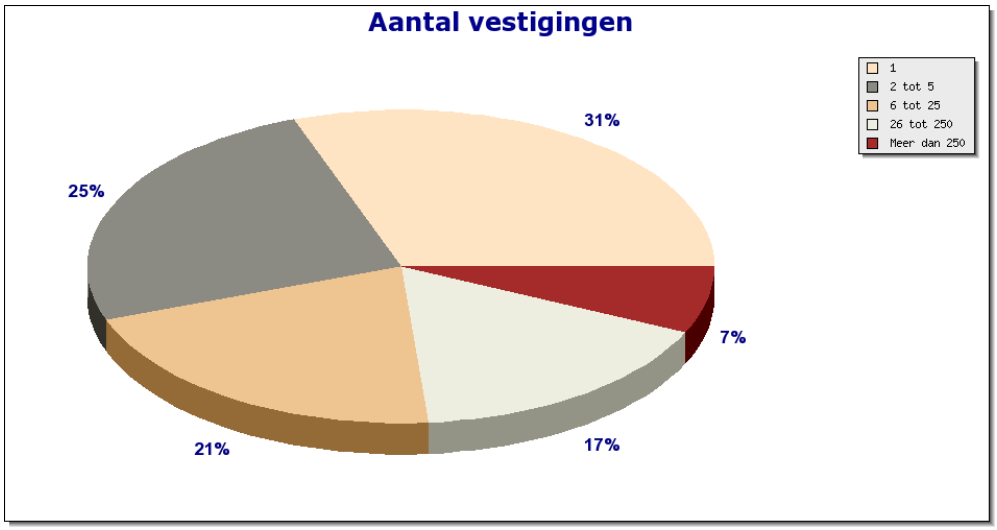


Figuur 11: Aantal respondenten per sector

Ook de omvang van de organisaties is wisselend, zoals is te zien in Figuur 12 . Zowel zeer grote bedrijven als het MKB zijn vertegenwoordigd. Ook als wordt gekeken naar het aantal vestigingen in Figuur 13 is het verschil in omvang van de deelnemende organisaties duidelijk te zien.



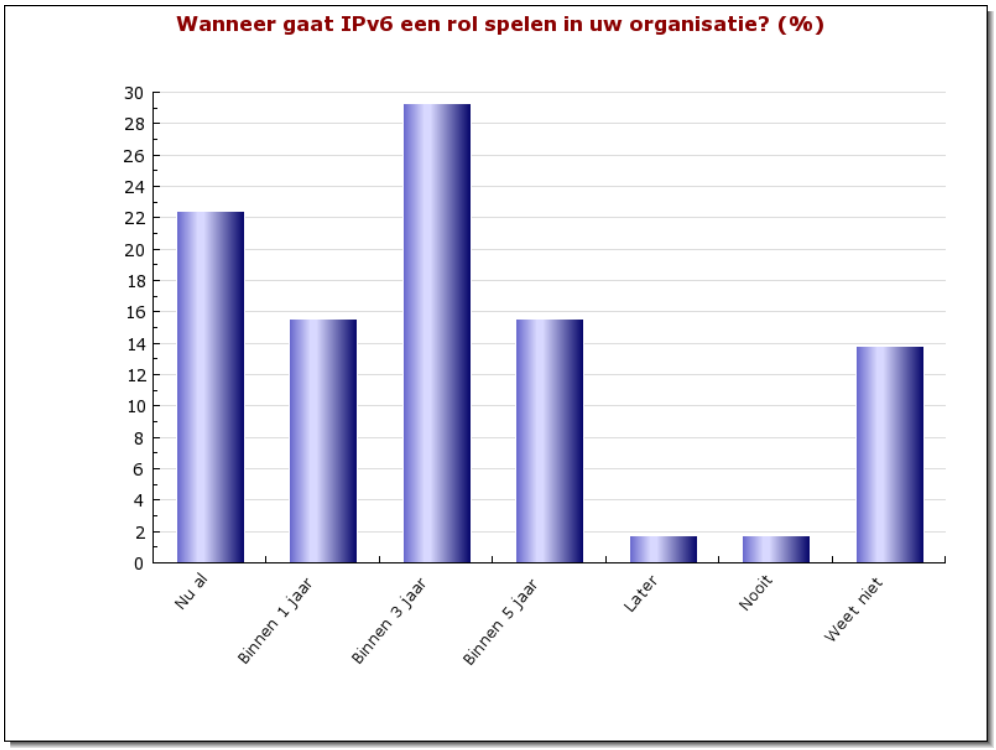
Figuur 12: Verdeling van respondenten naar omvang van de organisatie.



Figuur 13: Het aantal vestigingen van de organisaties die hebben meegedaan aan de enquête

Op de vraag of de deelnemer bekend is met de komst van IPv6 reageert 81% positief en 19% negatief. Dit geeft aan dat de bewustwording hoog is, maar niet compleet. Overigens lijken de antwoorden willekeurig verdeeld over verschillende sectoren. De deelnemers die ‘nee’ hebben geantwoord hebben in de enquête verder geen vragen meer gekregen waarvoor bekendheid met IPv6 nodig is. De weergegeven percentages in het vervolg van deze paragraaf zijn gebaseerd op de 81% die wel op de hoogte is van de komst van IPv6.

Figuur 14 geeft weer wanneer IPv6 voor gebruikersorganisaties een rol gaat spelen. Voor 37% is dat nu of binnen een jaar. Voor de 44% is dat ergens tussen 2012 en 2015. Een groep van ongeveer 14% weet het niet.



Figuur 14: Indicatie wanneer IPv6 een rol gaat spelen voor gebruikersorganisaties

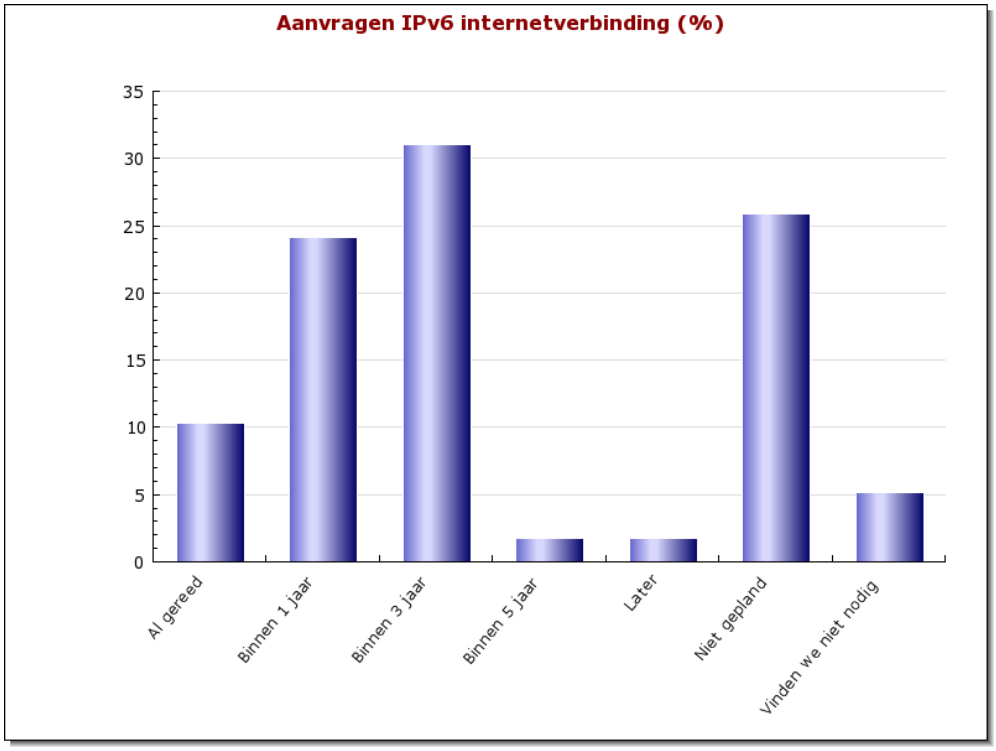
Specifiek is gevraagd naar de plannen die organisaties hebben op het gebied van IPv6. Hierbij konden de respondenten aangeven op welke termijn zij de activiteiten genoemd in Tabel 9 van plan zijn uit te voeren. Zij konden hierbij ook aangeven dat het voor hen niet van toepassing is of dat zij geen noodzaak zien voor plannen.

Tabel 9: Activiteiten omtrent de introductie van IPv6 uit de enquête.

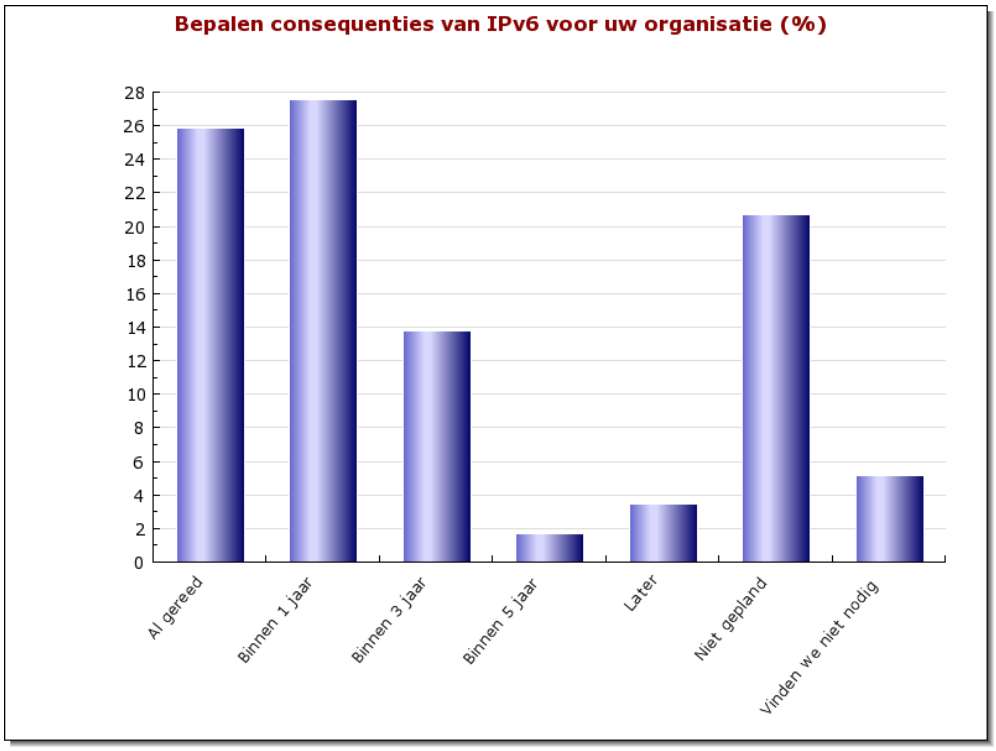
Onderzoeken van de urgentie van IPv6 voor mijn organisatie
Onderzoeken van de consequenties (organisatorisch, financieel, etc.) van de invoering van IPv6 in de eigen organisatie
Opleiden van personeel
Product en dienstleveranciers vragen om IPv6
Het aanvragen van een IPv6 adresblok
Aanvragen van een externe IPv6 verbinding naar het Internet
Netwerkinfrastructuur geschikt maken voor IPv6
Webpagina bereikbaar maken via IPv6
IT diensten (Intranet, ERP, CRM, etc.) geschikt maken voor IPv6
Anders

Bij de antwoorden op deze vragen valt op dat een groep van zo'n 20% van de deelnemers geen plannen heeft op het gebied van IPv6 en zo'n 5% het niet nodig vindt om plannen te hebben. Per activiteit is er een groep van zo'n 65-75% die wel plannen heeft. Er is wel een verschil te zien tussen de activiteiten als het gaat om de termijn waarop men ze heeft gepland. Figuur 15 laat bijvoorbeeld zien wanneer partijen van plan zijn een IPv6 internetverbinding aan te vragen. Iets meer dan 30% wil dit ergens tussen 2011 en 2013 doen. Kijkend naar het bepalen van de urgentie van IPv6 voor de

organisatie en het bepalen van de consequenties van IPv6 voor de organisatie, zie Figuur 16, dan is te zien dat dit een hogere prioriteit heeft.

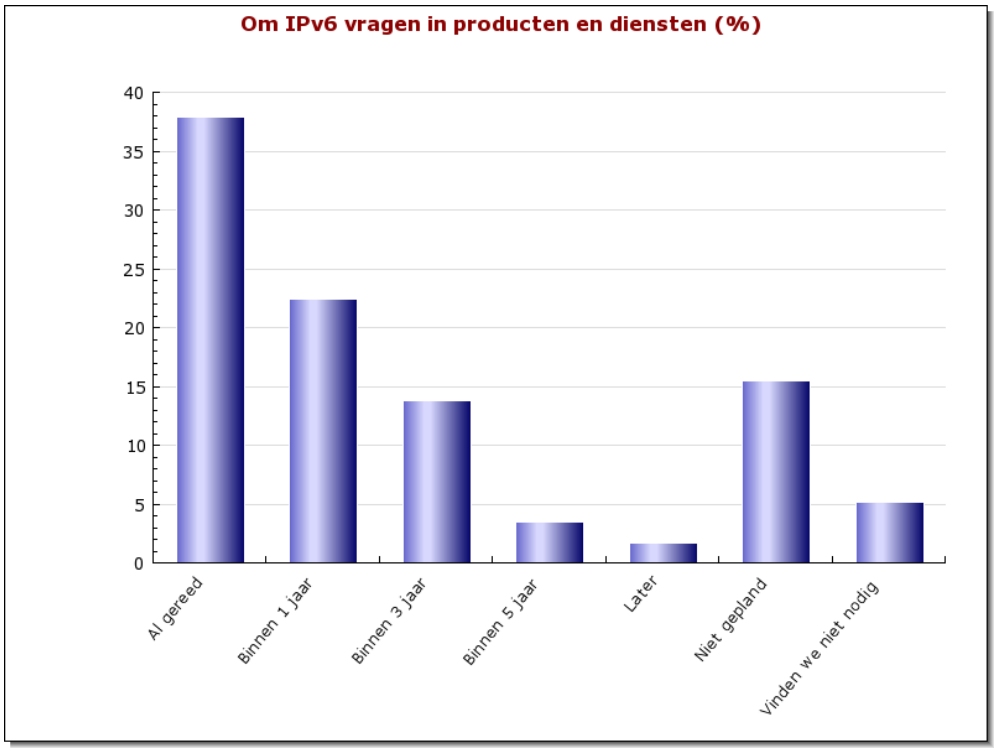


Figuur 15: Wanneer zijn organisaties van plan een IPv6 internetverbinding aan te vragen.



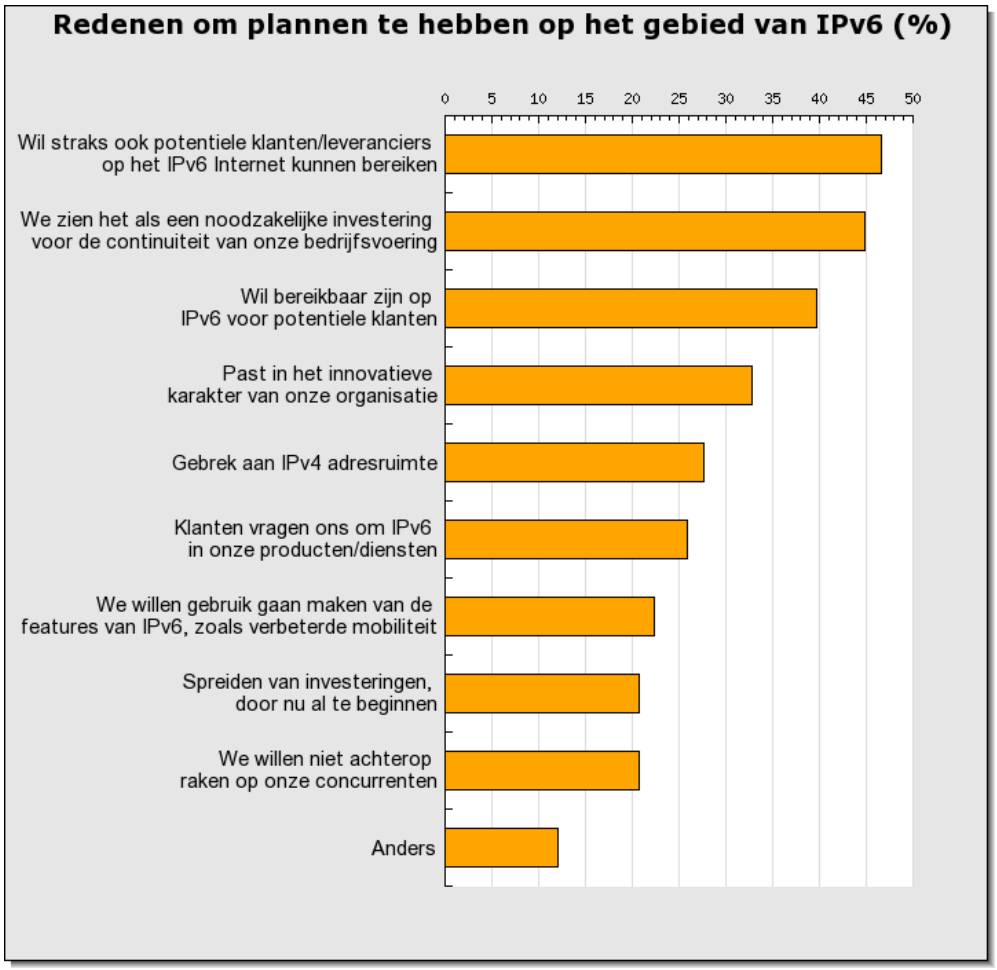
Figuur 16: Wanneer zijn organisaties van plan de consequenties te bepalen voor hun organisatie

Een andere activiteit die bij de respondenten prioriteit heeft is het bij aanschaf van producten of diensten, vragen om IPv6-ondersteuning, zie Figuur 17. 38% zegt hier al mee bezig te zijn.



Figuur 17: Planning van organisaties voor het vragen om IPv6 in producten en diensten

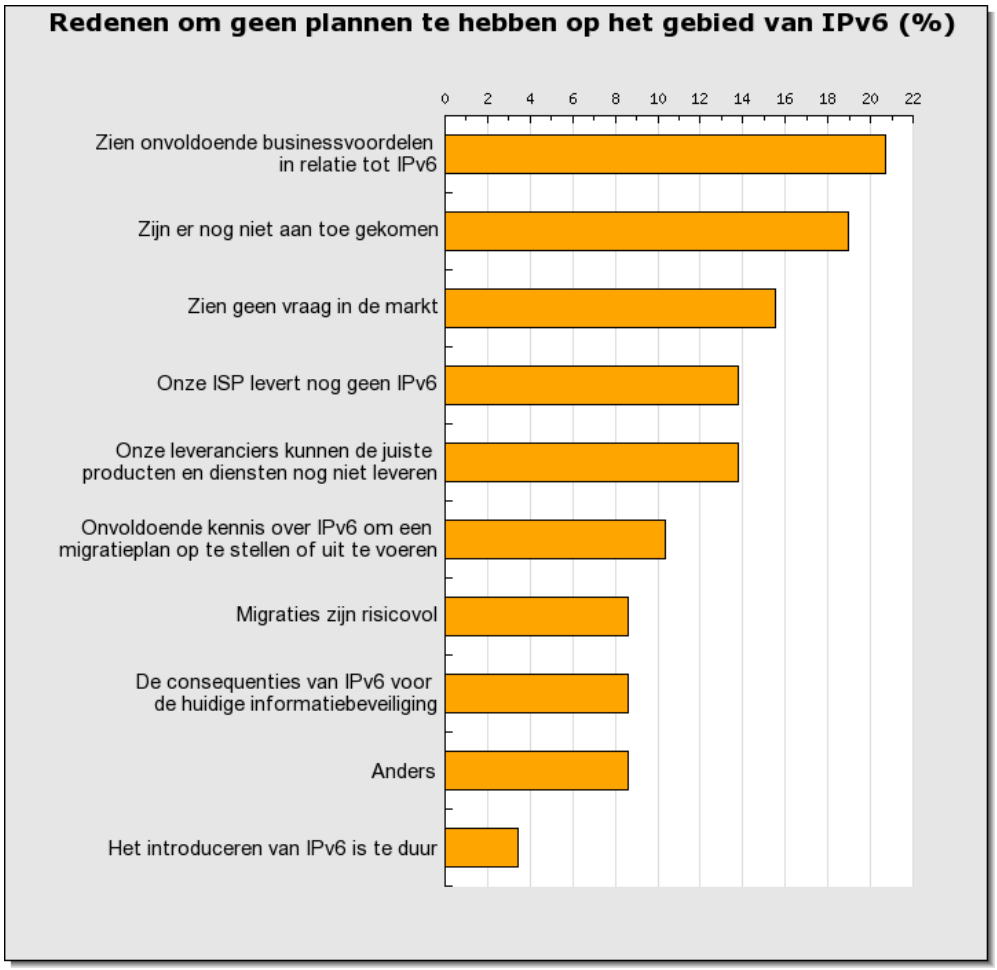
De grootste implementatieactiviteit is het gereed maken van het interne netwerk op IPv6. Activiteiten met mindere urgentie zijn het gereedmaken op IPv6 van de webpagina, de IT diensten en het kantoornetwerk. Deze activiteiten zijn dan ook maar bij zo'n 5 tot 15% van de deelnemers gereed.



Figuur 18: Redenen voor organisaties om met IPv6 aan de slag te kunnen.

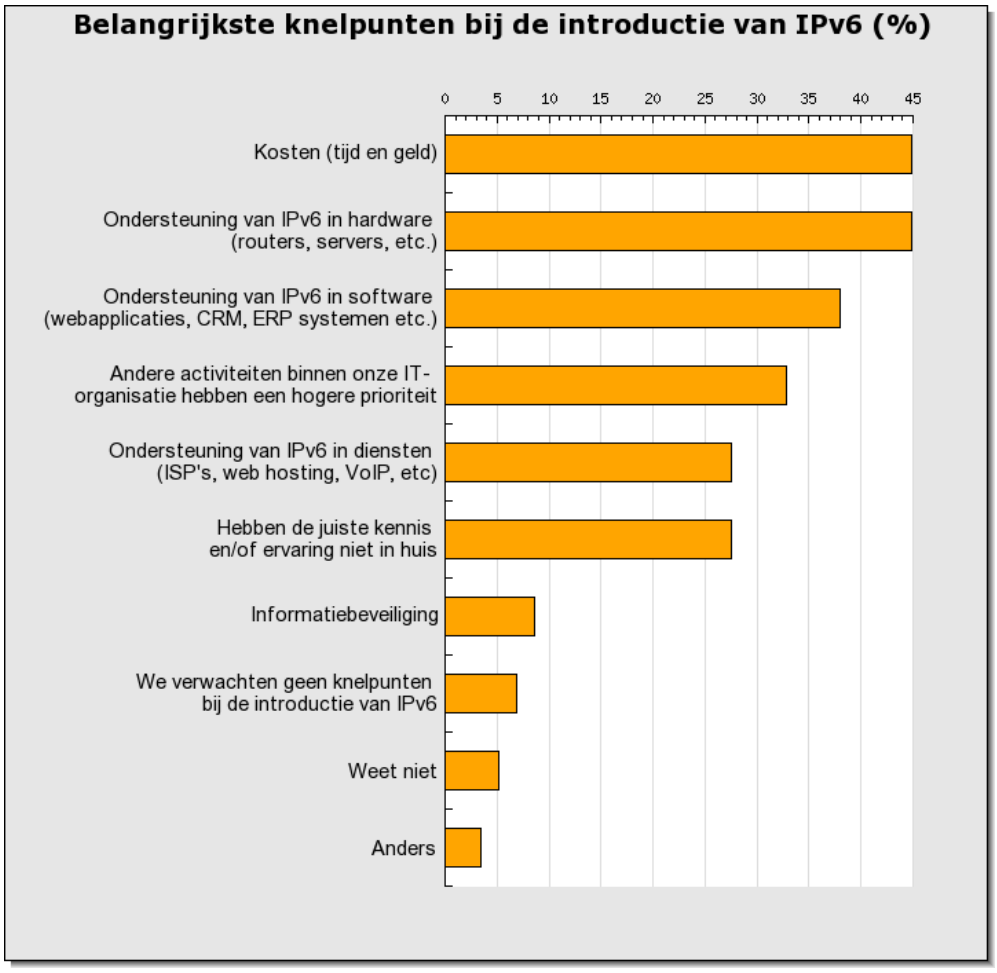
Figuur 18 laat de belangrijkste redenen zien die de deelnemers hebben gegeven om met IPv6 aan de slag te gaan. Het gaat hier toch vooral om iedereen te kunnen blijven bereiken op internet en daarmee ook een stuk continuïteit van de bedrijfsvoering te kunnen realiseren.

Aan de partijen die een bepaalde activiteit niet hebben gepland is gevraagd waarom ze deze plannen niet hebben. Deze redenen zijn weergegeven in Figuur 19 en net als bij de ISP's wordt het ontbreken van businessvoordelen gezien als belangrijkste reden. Opvallend is dat kosten voor de meeste partijen geen belangrijke reden lijken te zijn om niets met IPv6 te doen, maar dit wel als knelpunt wordt aangeven in Figuur 20.



Figuur 19: Redenen voor organisaties om niet met IPv6 aan de slag te gaan

In Figuur 20 is weergegeven wat de deelnemers aan de enquête zien als de belangrijkste knelpunten bij de introductie van IPv6. Tijd, geld, ondersteuning van IPv6 in hardware en software en prioriteitstelling spelen hierbij de belangrijkste rol.

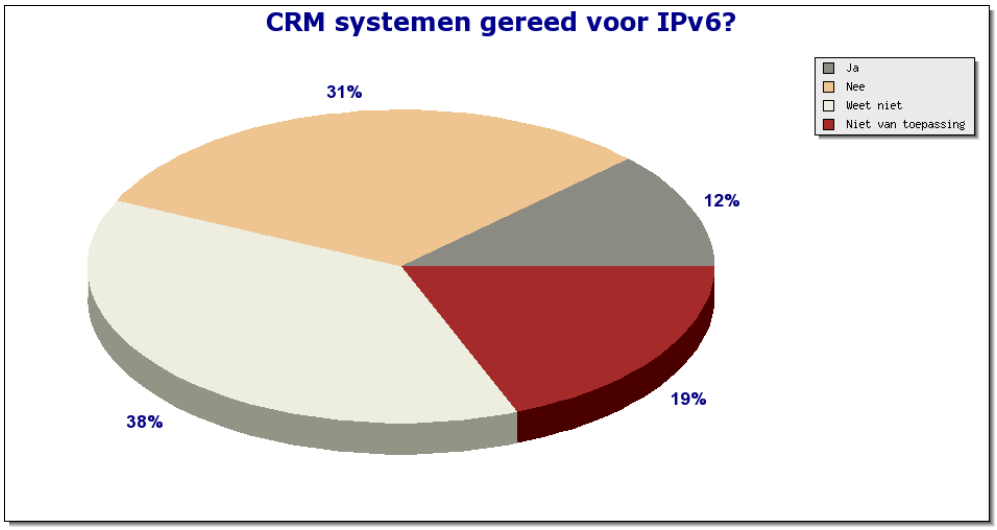


Figuur 20: Knelpunten bij de introductie van IPv6

Corporate IT

Als laatste onderdeel van de enquête is gevraagd naar de IT systemen die organisaties gebruiken en of men weet of deze applicaties klaar zijn voor IPv6 of niet.

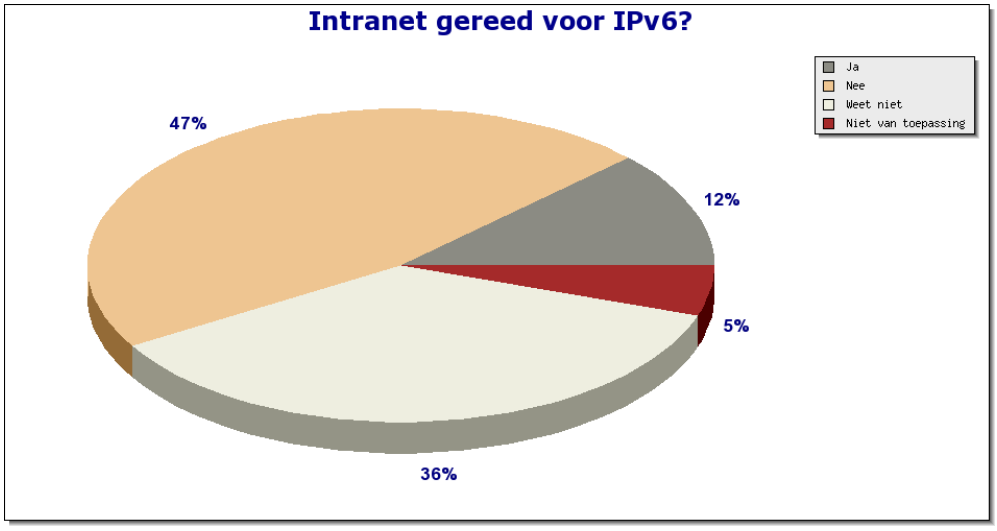
Zo'n 30% tot 40% van de deelnemers weet niet of de verschillende systemen klaar zijn voor IPv6. Figuur 21 laat bijvoorbeeld de antwoorden zien voor Customer Relation Management (CRM) systemen. 38% weet niet of de systemen klaar zijn, 31% zegt dat ze niet klaar zijn en 12% dat ze wel klaar zijn voor IPv6. De rest van de respondenten maakt geen gebruik van een CRM systeem in de organisatie. De antwoorden voor Content Management Systemen (CMS) en Enterprise Resource Planning (ERP) systemen, data opslag en instant messaging geven een vergelijkbaar beeld.



Figuur 21: Zijn uw CRM systemen klaar voor IPv6?

Figuur 22 geeft weer wat partijen hebben geantwoord op de vraag of het intranet van hun organisatie gereed is voor IPv6 en hier zegt bijna de helft dat dit niet het geval is en ruim een derde weet het niet.

Duidelijk is dat in de hoek van applicaties nog veel kan gebeuren als het gaat om IPv6 ondersteuning. Als dit wordt afgezet tegen de plannen van 60-70% van de organisaties om binnen 1-5 jaar IPv6 te introduceren in het kantoornetwerk, dan is er voor de meeste partijen nog wel even tijd om IPv6 ondersteuning in IT systemen te realiseren. Overigens zal het per organisatie verschillen hoe belangrijk het is om IPv6 te gebruiken op het interne netwerk. IPv6 is voor hen in de eerste plaats van belang voor externe koppelingen naar het internet en eventuele (buitenlandse) vestigingen.

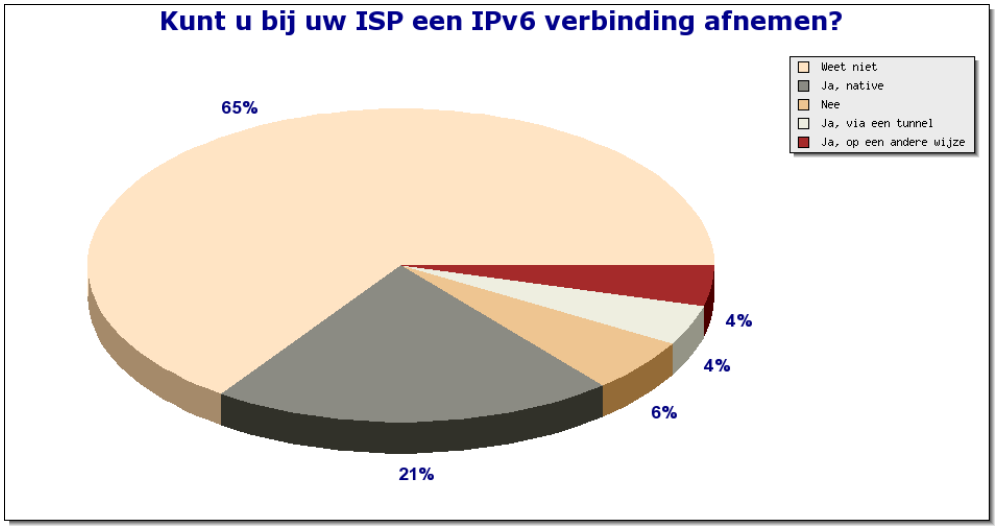


Figuur 22: Is uw intranet klaar voor IPv6?

IPv6 internetverbinding

De respondenten hebben aangegeven bij welke ISP zij hun internetverbinding afnemen en of zij bij deze partij op dit moment een IPv6 internetverbinding kunnen afnemen. Figuur 23 toont de antwoorden op de vraag. Er zijn in totaal meer dan 20 verschillende ISP's genoemd. 65% geeft aan dit niet te weten, hetgeen niet verrassend is aangezien

slechts 10% heeft aangegeven al een IPv6 verbinding te hebben aangevraagd, zoals in Figuur 15 is te zien. 21% geeft aan een IPv6 verbinding te kunnen afnemen bij hun ISP.



Figuur 23: Kunnen organisaties een IPv6 verbinding afnemen bij hun ISP?

3.5.3 Conclusies

ISP's en mobiele operators

Ook al leveren de meeste ISP's nog geen IPv6 internetverbindingen, IPv6 staat bij de grote partijen in Nederland duidelijk op de agenda. Vrijwel alle geïnterviewde ISP's zijn de voorbereidingsfase voorbij en zijn bezig met de uitrol van IPv6 in hun netwerk. De meeste partijen zullen tussen 2011 en 2013 hun eerste consumenten aansluiten op IPv6.

Het aanbieden van IPv6 zal voor veel consumenten 'onder water' gebeuren. Zij zullen veelal op IPv6 worden aangesloten op een moment dat door de ISP is gekozen. In de zakelijke markt zal de introductie van IPv6 veel meer worden gerealiseerd op basis van klantvraag.

Op LIR-niveau is de IPv4 adresvoorraad per organisatie verschillend. Sommige ISP's verwachten begin 2012 door hun adressen heen te zijn, terwijl anderen aangeven nog tot 2014 of later met hun adresvoorraad verder te kunnen.

De voornaamste reden voor ISP's om aan de slag te gaan met IPv6 is het waarborgen van de continuïteit van hun bedrijfsvoering. De belangrijkste remmende factor is dat IPv6 geen financiële voordelen oplevert. Daarnaast wordt maturiteit van IPv6 in hardware en software genoemd als aandachtspunt.

ISP's die door hun IPv4 adresvoorraad heen zijn kunnen niet al hun klanten native dual-stack aansluiten. Als op dat moment het overgrote deel van de websites en -services alleen maar via IPv4 bereikbaar is, zullen zij noodgedwongen gebruik moeten maken van technieken, zoals NAT in het providernetwerk.

Mobiele operators bieden momenteel nog geen IPv6 omdat de meeste mobiele telefoons en mobiele interface kaarten (dongles) dit nog niet ondersteunen. Voorlopig kunnen zij nog vooruit met IPv4 en eventueel NAT. De netwerken zelf worden naar verwachting binnen 1-3 jaar geschikt gemaakt voor IPv6, zodat het mogelijk vanaf 2012 geïntroduceerd wordt voor mobiele gebruikers.

Kijkend naar de snelheid van de uitrol van IPv6 in Nederland in relatie tot het opraken van de IP adressen bij IANA, RIPE NCC en ISP's, leveren de interviewresultaten het volgende beeld:

IPv6 staat bij de grote partijen in Nederland duidelijk op de agenda. Vrijwel alle geïnterviewde ISP's zijn de voorbereidingsfase voorbij en zijn bezig met de uitrol van IPv6 in hun netwerk. De meeste partijen zijn van plan tussen 2011 en 2013 hun eerste consumenten aansluiten op IPv6.

ISP's, die begin 2012 hun eerste klanten niet op IPv6 kunnen aansluiten lopen een risico als consumenten actief om IPv6 gaan vragen of er toch een populaire IPv6-only dienst mocht ontstaan.

Het aanbieden van content en diensten op IPv6 is een voorwaarde voor de continuering van de groei van internet. Als content en diensten onvoldoende op dual-stack worden aangeboden, zal dit leiden tot hogere kosten voor ISP's en een slechtere internetgebruikservaring.

Bedrijven en overheden

Het bewustzijn op het gebied van IPv6 is bij de ondervraagde bedrijven en overheden is ruim aanwezig. Ook heeft het merendeel van de organisaties plannen op het gebied van IPv6. Concrete activiteiten hebben echter bij veel organisaties nog niet plaatsgevonden.

Er zijn nog veel IT systemen en applicaties die niet geschikt zijn voor IPv6. Een significant deel van de organisaties heeft hier helemaal geen beeld van. Ook weet het merendeel van de organisaties niet of hun ISP een IPv6 internetverbinding kan leveren.

Gebruikersorganisaties zien weinig tot geen voordelen in IPv6 en de benodigde investeringen zijn dan ook de belangrijkste remmende factor. Toch wil men niet het risico lopen om potentiële klanten op IPv6 niet te kunnen bereiken.

De tijdslijnen voor de introductie van IPv6 liggen bij de gebruikersorganisaties duidelijk wat verder weg dan bij de ISP's. Dit varieert van 2012 tot 2015. Een deel van de organisaties heeft zelfs helemaal geen plannen.

De bevindingen uit de enquêtes beschouwend betekent dit het volgende:

Veel bedrijven en overheden zijn zich bewust van de komst van IPv6. Plannen zijn er bij een deel ook, maar echte activiteit is beperkt. Daarnaast is bij organisaties weinig bekend over IPv6-ondersteuning bij applicaties. Meer aandacht voor IPv6 bij deze organisaties is gewenst om beter de risico's aangaande de IP adresschaarste te managen.

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 werkgroepen, waarvan een groot aantal 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.

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. 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.

Het afgelopen halfjaar heeft de werkgroep ‘IPv6 Operations’ één RFC uitgebracht met betrekking tot “IPv6 Deployment in Internet Exchange Points (IXPs)”. IXP’s zijn fysieke infrastructuren die ISP’s gebruiken om verkeer met andere ISP’s te kunnen uitwisselen. In deze RFC wordt ingegaan op een IPv6 adresseringsplan, en hoe IPv6 data, control en management verkeer afgehandeld moet worden. Andere onderwerpen waar o.a. aan gewerkt worden zijn:

- (2010-04-15) Emerging Service Provider Scenarios for IPv6 Deployment;
- (2010-06-22) Simple security capabilities in CPE for residential IPv6 services;
- (2010-07-12) Mobile Network Considerations for IPv6 Deployment;
- (2010-08-11) Requirements for IPv6 customer edge routers;
- (2010-08-31) Security concerns with IP tunneling.

Binnen de werkgroep ‘behave’ wordt op dit moment veel werk verricht aan NAT. De doelstelling is om voor april 2011 enkele informerende RFC’s en standaarden met betrekking tot NAT64 en NAT46 te publiceren. NAT64 maakt het mogelijk om IPv6-only clients te laten communiceren met IPv4-only servers. Deze implementatie biedt de

mogelijkheid om IPv6-only te gebruiken in plaats van dual-stack, indien men de dual-stack tussenstap wil overslaan of een limiet ziet aan de eindige schaalbaarheid van NAT44 door een te hoge complexiteit. Afgelopen juni heeft T-Mobile USA aangekondigd stapsgewijs (per telefoonmodel) IPv6-only te gaan introduceren, met behulp van NAT64, DNS64 en een IPv6 PDP context. Als laatste biedt NAT64 ook perspectief om te gaan met IPv4-only applicaties.

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 is Release 10, welke begin 2011 wordt verwacht. Onderdeel van deze release is een migratie studie naar IPv6, waaruit richtlijnen naar voren zullen komen welke erg belangrijk zijn voor mobiele operators.

In de tijd tussen de Nulmeting en de tweede meting zijn er geen officiële (tussen)publicaties geweest over de migratie studie naar IPv6. Voor een groot deel is deze studie afhankelijk van werk verricht door de IETF. De studie is nu voor ongeveer 70% afgerond.
Voor de volledigheid worden de drie migratiescenario's hier nogmaals vermeld:

- 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[24] te gebruiken achter een NAT.
- 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.
- Aansluiting d.m.v. IPv6-only en toepassingen die IPv6 ondersteunen
  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.

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

[24] 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.

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 stemden de aan deze *working texts* deelnemende organisaties in met WT-124 en WT-187. Hierdoor werden deze door de deelnemende organisaties definitief bekrachtigd als technical recommendations TR124 en TR187. WT-177 is op dit moment kandidaat voor stemming. Input en ideeën t.b.v. WT-242 worden aangeleverd. WT-243 moet echter 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 mogelijk zijn.

4.5 Conclusie

In de IETF wordt momenteel veel werk verricht aan NAT64 wat tijdens de transitieperiode van IPv4 naar IPv6 perspectief biedt voor translatie tussen deze twee protocollen, met name voor IPv4-only of IPv6-only clients en diensten.

Sinds de Nulmeting is ook het standaardisatie werk binnen 3GPP en Broadband Forum gecontinueerd. 3GPP zal begin 2011 met een nieuwe release komen en binnen het Broadband Forum zijn reeds twee nieuwe *technical recommendations* geaccepteerd omtrent 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. In paragraaf 5.2 worden de gegevens zoals gepresenteerd in de Nulmeting ververst en vergeleken met de gegevens uit de Nulmeting.

5.2 IPv6 kwetsbaarheden

5.2.1 Methode

In deze monitor wordt gebruik gemaakt van gerapporteerde kwetsbaarheden[25,26]. 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[27]. 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)

[25] 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.

[26] www.osvdb.org

[27] www.first.org/cvss

- 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)

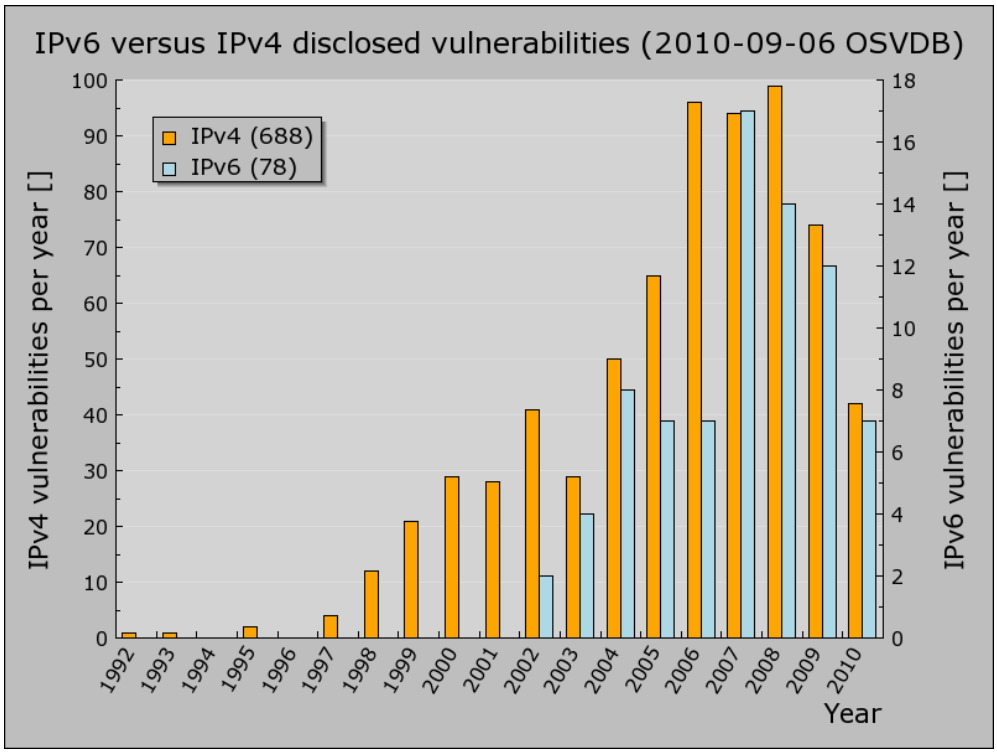
Door middel van een verdeelsleutel wordt het uiteindelijke CVSS cijfer bepaald dat een maat is voor de ernst van de kwetsbaarheid.

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.

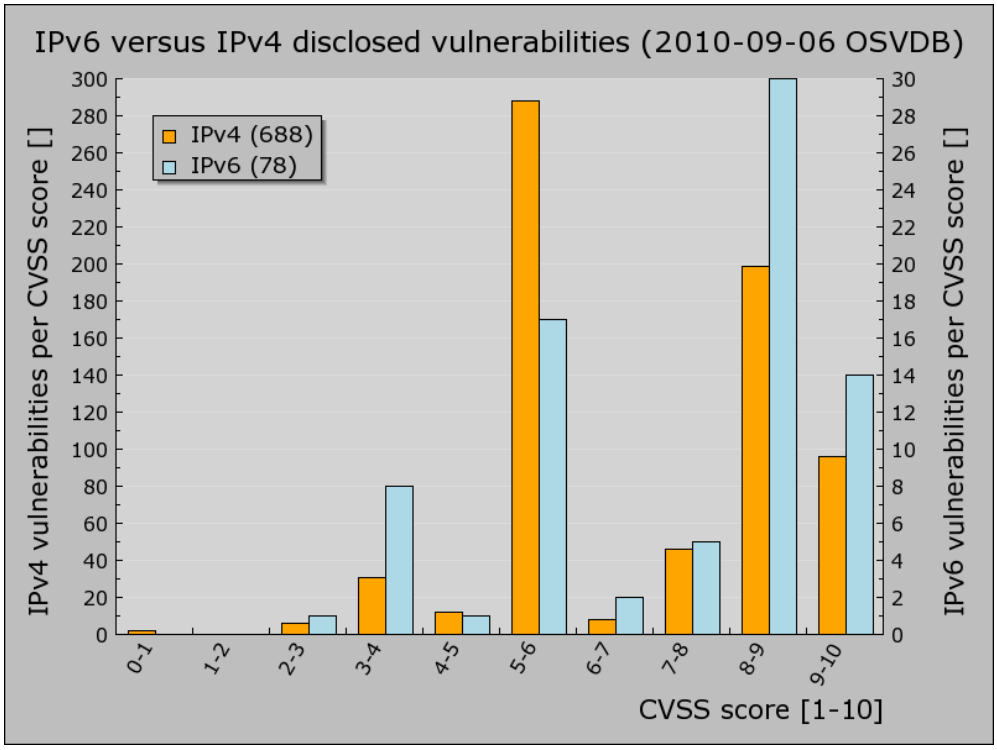
In paragraaf 5.2.2 worden op vergelijkbare manier en onder gelijke condities nieuwe grafieken gepresenteerd als in de Nulmeting[28].

5.2.2 Monitoring van kwetsbaarheden



Figuur 24 Aantallen gerapporteerde[26] IPv4 en IPv6 kwetsbaarheden per jaar, tot 7 september 2010

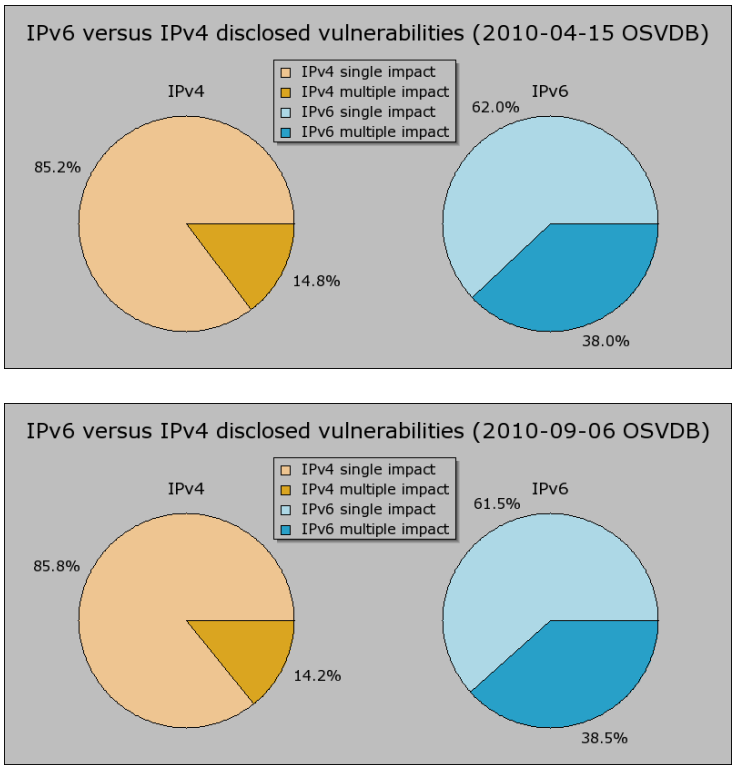
De gerapporteerde IPv6 kwetsbaarheden in 2010 (Figuur 24) zijn over de periode van april 2010 [28] tot september 2010 toegenomen van 2 tot 7. De IPv4 gerelateerde kwetsbaarheden in 2010 laten in deze periode een toename zien van 12 naar 42. Voor 2010 betekent dit dat na extrapolatie naar verwachting het aantal kwetsbaarheden ongeveer gelijk zal zijn aan die gemeten over 2009. Net als in het geval van de Nulmeting is het van belang dat kwetsbaarheden met gelijke inzet gerapporteerd worden. Er is geen aanwijzing dat dit gedurende de tweede meting anders zou zijn geweest.



Figuur 25: Aantallen gerapporteerde[26] IPv4 en IPv6 kwetsbaarheden ingedeeld naar kwetsbaarheidscore, tot 7 september 2010.

De verdeling naar ernst (CVSS cijfer) (Figuur 25) van de kwetsbaarheden tussen april 2010 [28] en september 2010 blijft nagenoeg onveranderd. Er valt geen significante verschuiving in de distributie van de kwetsbaarheden waar te nemen.
Tussen de periode van april 2010 en september 2010 is het aantal kwetsbaarheden dat impact kan hebben op meerdere producten (Het is in zo'n geval niet mogelijk makkelijk uit te wijken naar een alternatief product.) marginaal veranderd.

[28] IPv6 Monitor in Nederland: De Nulmeting, TNO rapport Nr. 35334, TNO-ICT, Brassersplein 2, 2612CT Delft, The Netherlands



Figuur 26: Impact van kwetsbaarheden op producten en software. Boven: situatie tot 15 april 2010, onder: situatie tot 7 september 2010.

5.3 Voordelen en tekortkomingen van IPv6

In een recent onderzoek dat in opdracht van de EU is uitgevoerd[29] wordt een overzicht gegeven van voordelen en tekortkomingen van IPv6.
Binnen de Nederlandse IPv6 TaskForce heeft zich een discussie afgespeeld omtrent privacy en IPv6 adressering waardoor gebruikersgedrag makkelijk gevolgd zou kunnen worden.

5.3.1 IPsec en IPv6

De beveiligingsmechanisme van IPsec (IPv4) en de end-to-end IPv6 beveiliging zijn gelijk (IPsec is onderdeel van IPv6). Verschillen ontstaan door verschillende manieren waarop sleutelinformatie wordt overgedragen en verstuurd. Indien bestaande, voor IPv4 gebruikte mechanismes ook voor IPv6 kunnen worden ingezet is verslechtering van het beveiligingsregime niet te verwachten. Indien een nieuw systeem moet worden geïntroduceerd levert dit wel een punt van aandacht op.

5.3.2 NAT

Network Address Translation (NAT) wordt gebruikt om meerdere interne IP adressen gebruik te laten maken van een publiek IP adres. Hoewel NAT niet als een

[29] IPv6 security models and dual-stack (IPv6/IPv4) implications, Study Report, 05-07-2010, InfoCom, http://ec.europa.eu/information_society/policy/ipv6/docs/studies/Study%20Report%20v4.1.pdf

beveiligingsmechanisme mag worden aangemerkt schermt het in combinatie met een router wel het interne netwerk af. NAT heeft echter ook als nadeel dat het complex is in relatie tot service transparantie. Fouten in de configuratie van NAT kunnen echter wel leiden tot gaten in de beveiliging. IPv6 maakt het mogelijk netwerken makkelijker uit te breiden gebruikmakend van publieke netwerken zonder het gebruik van NAT.

5.3.3 IPv6 firewalls

In IPv4 ICMP verkeer wordt vaak geblokkeerd. IPv4 ping is een voorbeeld van ICMP verkeer dat vaak uitgefilterd wordt, maar het komt ook vaak voor dat het volledige IPv4 ICMP verkeer wordt uitgefilterd. In het geval van IPv6 is ICMPv6 verkeer essentieel en het gedachteloos filteren van deze berichten is vanuit operationeel oogpunt niet aan te raden. Netwerk beheerders moeten getraind worden op de consequenties van het al of niet toestaan van ICMPv6 berichten m.b.t. de beveiliging van netwerken en hoe dit te configureren in firewalls.
Tevens zal door IPv6 niet langer het netwerk centraal staan maar de host (gebruiker). Hierdoor zullen niet alleen de eisen enigszins veranderen, maar de noodzaak van virusscanners, firewalls, access control, en het uitschakelen van onnodige diensten zal hoger worden.
Het is echter een misverstand dat beveiliging van de host afdoende is. Ook netwerk elementen zoals routers en switches zullen voorzien moeten worden van beveiligingssystemen zoals firewalls en filters. Een voorbeeld zijn valse router adverteer berichten die makkelijk tot een man-in-the-middle aanval kunnen leiden. Hierbij moet ook de topologie meegenomen worden: een vaste LAN aansluiting dient anders beveiligd te worden dan een wireless LAN aansluiting.

5.3.4 Mobiele devices

Mobiele devices zoals smartphones en laptops met mobiele interface kaarten (dongles) zullen gedurende lange tijd zowel IPv4 als IPv6 gaan ondersteunen. IPv6 pilots zullen nog moeten plaatsvinden onder druk van een commerciële snelle uitrol. Dit levert een potentieel risico op waarbij een te snelle uitrol leidt de mogelijkheid van misbruik van een ondoordachte of niet-uitgeteste implementatie.

5.3.5 Migratie

Daar waar mogelijk zal een dual-stack transitie scenario moeten worden gebruikt. Tunneling is mogelijk over die netwerken die niet dual-stack gemaakt kunnen worden. Indien het niet mogelijk is in tunnels te kijken kan dit risico’s opleveren. Ook mechanismes die automatisch tunnels kunnen opzetten kunnen ongewenste situaties opleveren. Communicatie tussen IPv4-only en IPv6-only elementen kan alleen via applicatie layer netwerken betrouwbaar gebeuren. Wordt gebruik gemaakt van beveiligde tunnels (IPsec) dan levert dit problemen op. IPv4-only elementen zullen in deze context van een dual-stack moeten worden voorzien of vervangen.

5.3.6 Besturingssystemen

De meeste besturingssystemen ondersteunen IPv6, echter niet altijd volledig. Het MacOSX ondersteund geen DHCPv6 en MSWindows ondersteund nog geen SEND. IPv6 staat vaak standaard aan. Dit is een risico indien netwerken niet voldoende zijn

voorbereid op het kunnen filteren van ICMPv6 en firewalls IPv6 niet (afdoende) ondersteunen. IPv6 zal standaard dan ook uitgezet moeten worden.

5.3.7 IPv6 mobile

IPv6 mobile kent vele voordelen t.o.v. mobile IP (IPv4 mobile).
Er zijn echter nog geen implementaties die als volwassen kunnen worden aangemerkt. Dit kan leiden tot potentiële kwetsbaarheden indien een snelle invoering plaats zal moeten vinden. Het overschakelen tussen netwerken kan echter ook op de applicatie laag uitgevoerd worden. Totdat een veilige IPv6 mobile implementatie voorhanden is het schakelen op applicatie laag de meest veilige manier.
De mobile IP dienst is kwetsbaar (Denial of Service aanvallen) in het geval NAT gebruikt wordt (zowel voor IPv6 als IPv4). Het gebruik van NAT moet voorkomen worden waardoor IPv6-only als enige oplossing in aanmerking komt indien een oplossing op applicatie laag niet wenselijk is.

5.3.8 E2E-diensten

E2E diensten (hieronder vallen ook M2M diensten) kunnen makkelijk via IPv6 worden geïmplementeerd, gebruikmakend van een globale certificering van credentials

5.3.9 Secure Neighbor Discovery

Het Secure Neighbor Discovery protocol dat op netwerkelementen draait verbetert de veiligheid van bedrijfsnetwerken. SEND voorkomt dat valse routeradvertenties het netwerk onveilig maken. Er zijn op dit moment nog geen implementaties voor hosts.

5.3.10 Privacy en IPv6 adressen

De laatste 64 bits van een IPv6 adres, het hostadresdeel, kunnen informatie bevatten die uniek zijn voor een terminal zoals een computer of smartphone. (Dit komt door gebruik van autoconfiguratie van IPv6 adressen.) Hierdoor is het mogelijk verbanden te leggen tussen een terminal en de locaties of websites waar IPv6 pakketten met een gelijk hostadres waargenomen worden. Indien de identiteit van een gebruiker gekoppeld kan worden aan dit hostadres, zou het mogelijk kunnen zijn op basis van het hostadres de gebruiker als individu te identificeren op andere locaties en andere websites.
Deze problematiek speelt niet voor IPv4 omdat specifieke terminalinformatie niet in een IPv4 adres wordt verwerkt.
De IPv6 standaard laat toe het hostadresdeel willekeurig te kiezen. Hierdoor wordt het minder triviaal gebruikers aan IPv6 adressen te koppelen. Gebruikers moeten dit echter wel weten en het besturingssysteem van de computer of smartphone moet dit wel ondersteunen. Hier ligt een verantwoordelijkheid bij de makers van besturingssoftware.
Naast de mogelijkheid om gebruikersgedrag via het hostadresdeel van het IPv6 adres te monitoren en te herleiden tot een terminal zijn er voldoende andere methodes om dit te doen. Deze methodes werken even efficiënt op IPv4 als op IPv6.

5.4 Conclusies

Zowel voor IPv6 als voor IPv4 vindt monitoring en analyse plaats van kwetsbaarheden in implementaties van netwerk elementen en software.

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 wel een grotere impact hebben dan kwetsbaarheden in IPv4. De frequentie waarmee IPv6 gerelateerde kwetsbaarheden gerapporteerd wordt is laag in vergelijking met IPv4 maar is vanaf 2008 wel relatief constant. De ernst van de kwetsbaarheden zijn in vergelijking met de Nulmeting vrijwel ongewijzigd.

De jaarlijkse daling die vanaf 2008 leek te zijn ingezet is in 2010 het kleinst. Door de uitrol van IPv6 zullen de komende jaren meer fabrikanten IPv6 implementaties in hun producten doorvoeren en zal de diversiteit van IPv6 implementaties toenemen. Om deze redenen is het van belang gedurende de resterende tijd in 2010 tot en met 2012 alert te blijven. Indien een vervolg meting verdere verslechtering laat zien kan dit de perceptie omtrent IPv6 uitrol doen veranderen.

In deze monitor is een lijst opgenomen met tekortkomingen, maar ook voordelen van IPv6. Deze lijst vormt een leidraad als het gaat om toekomstige maatregelen en richtingen waarin innovatie van meer IPv6 beveiligingsgerelateerde functionaliteiten kan plaatsvinden.

6 Conclusies

Uit vergelijking met de Nulmeting is gebleken dat dit jaar de mondiale uitgifte van IPv4 adressen gestegen ten opzichte van voorgaande jaren. Hier is vooral een sterke groei te zien in de regio bediend door APNIC (Oost-Azië, Zuidoost-Azië en Oceanië). Als gevolg hiervan komt de verwachte uitputtingsdatum sneller dichterbij. Uit voorspellingen van Geoff Huston blijkt dat de adresvoorraad bij IANA in maart 2011 leeg zal zijn. Voor de daadwerkelijke datum moet rekening gehouden worden met enkele maanden spreiding ten opzichte van de voorspelde uitputtingsdatum. Hetzelfde geldt voor de verwachte uitputtingsdatum van de eerste RIR in december 2011. Ten opzichte van de Nulmeting zijn beide data met respectievelijk zes en elf maanden naar voren geschoven, wat ook aangeeft dat de data in korte tijd snel kunnen variëren.

Op LIR-niveau is de IPv4 adresvoorraad per organisatie verschillend. Sommige ISP's verwachten begin 2012 door hun adressen heen te zijn, terwijl anderen aangeven nog tot 2014 of later met hun adresvoorraad verder te kunnen.

In vergelijking met ons omringende landen loopt Nederland, net als ten tijde van de Nulmeting, 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. Een belangrijke ontwikkeling sinds de Nulmeting is het aanbieden van een IPv6 aansluiting aan alle klanten door XS4ALL in Nederland. Dit is de eerste ISP die IPv6 aansluitingen grootschalig aanbiedt aan consumenten. Voor de zakelijke markt waren IPv6 aansluitingen al verkrijgbaar.

IPv6 staat bij de grote ISP's in Nederland duidelijk op de agenda. Vrijwel alle geïnterviewde ISP's zijn de voorbereidingsfase voorbij en zijn bezig met de uitrol van IPv6 in hun netwerk. De meeste van deze partijen zullen tussen 2011 en 2013 hun eerste consumenten op IPv6 kunnen aansluiten. Het aantal consumenten dat IPv6 zal kunnen gebruiken zal de jaren daarna gestaag groeien.

ISP's, die begin 2012 hun eerste klanten niet op IPv6 kunnen aansluiten lopen een risico als consumenten actief om IPv6 gaan vragen of in het geval een populaire IPv6-only dienst ontstaat.

Het aanbieden van nieuwe aansluitingen op IPv6 is voor ISP's met een IPv4 adrestekort nog geen oplossing voor het realiseren van compatibiliteit tussen de nieuwe IPv6 aansluitingen en het huidige IPv4 Internet. Omdat veel content alleen nog over IPv4 bereikbaar is, zullen ISP's genoodzaakt zijn om gebruik te maken van technieken als NAT in het provider netwerk. Het tijdig aanbieden van dual-stack content en diensten zijn een voorwaarde om het gebruik van dergelijke technologieën te beperken.

Het aanbieden van content en diensten op IPv6 is een voorwaarde voor de continuering van de groei van internet. Als content en diensten onvoldoende dual-stack wordt aangeboden, zal dit leiden tot hogere kosten voor ISP's en een slechtere internetgebruikservaring.

Veel bedrijven en overheden zijn zich bewust van de komst van IPv6. Plannen zijn er bij een deel ook, maar echte activiteit is beperkt. Daarnaast is bij organisaties weinig

bekend over IPv6-ondersteuning in applicaties. Meer aandacht voor IPv6 bij deze organisaties is gewenst om beter de risico's aangaande de IP adresschaarste te managen.

De frequentie waarmee IPv6 gerelateerde kwetsbaarheden gerapporteerd wordt blijft laag in vergelijking met IPv4. De ernst van gerapporteerde kwetsbaarheden is in vergelijking met de Nulmeting vrijwel ongewijzigd.

Een lijst van voordelen en tekortkomingen op het gebied van IPv6 beveiligingsmodellen en implementaties kan als leidraad dienen voor toekomstige maatregelen en richtingen waarin innovatie van meer IPv6 beveiligingsgerelateerde functionaliteiten kan plaatsvinden.