Brassersplein 2
2612 CT Delft
Postbus 5050
2600 GB Delft

www.tno.nl

T +31 88 866 70 00
F +31 88 866 70 57
infodesk@tno.nl

TNO-whitepaper

35518

IPv6 Monitoring in Nederland: De derde meting

Datum	25 mei 2011
Auteur(s)	Maria Boen-Leo, Tim Hartog, Arjen Holtzer, Harm Schotanus, Rob Smets, Martin Tijmes
Aantal pagina's	41
Projectnaam	IPv6 Monitoring in Nederland
Projectnummer	055.01021

Deze rapportage maakt onderdeel uit van het monitoringsprogramma van TNO en is tot stand gekomen dankzij een bijdrage van het Ministerie van Economische Zaken, Landbouw en Innovatie.

Managementuittreksel

Sinds 2010 voert TNO monitoring uit van IPv6 in Nederland. Dit whitepaper beschrijft de derde meting. In deze meting wordt een update gegeven over de uitrol van IPv6, waarbij de stand van zaken rond april 2011 wordt beschreven. Eerder zijn de Nulmeting en Tweede Meting gepubliceerd.[1] In het vierde kwartaal van 2011 zal nog een vierde meting gepubliceerd worden.

Uit de vorige metingen is gebleken dat grote ISP's en mobiele operators bezig zijn met de voorbereidingen voor IPv6, maar dat slechts een enkeling het commercieel aanbiedt. Uit deze metingen bleek ook dat de beschikbaarheid van content en diensten een punt van zorg is. Om hier meer inzicht in te krijgen is een enquête onder hosting providers uitgezet. Daarnaast is er ingezoomd op de beveiligingsaspecten van IPv6 om na te gaan of dit mogelijke belemmeringen opwerpt. Verder is er een inventarisatie gemaakt van consumentenproducten met betrekking tot IPv6.

De voorraad van IPv4-internetadressen op mondiaal niveau is nu op. IANA heeft de laatste adresblokken uitgegeven op 3 februari 2011. Ook in Azië is de voorraad zo goed als op, waarbij ervoor gezorgd wordt dat nieuwe netwerken nog een kleine hoeveelheid IPv4 adressen kunnen bemachtigen. Op Europees niveau is de voorraad IPv4 adressen naar verwachting voor het einde van 2011 op. Verder is te zien dat de aanvraag voor IPv6 adressen toeneemt.

Hoewel het bewustzijn en de urgentie omtrent de noodzaak voor IPv6 zijn toegenomen, heeft dit zich nog steeds niet vertaald in daadwerkelijk gebruik. Er is nauwelijks groei in het aantal websites dat IPv6 ondersteunt en ook nauwelijks toename in het aanbod van IPv6 aansluitingen. In vergelijking tot de rest van Europa doet Nederland het niet slecht, al moet er nog veel gebeuren voordat IPv6 gemeengoed is. Zo blijkt uit een steekproef onder producten voor consumenten dat IPv6 ondersteuning daar zeer beperkt is. Op 8 juni 2011 wordt "World IPv6 Day" georganiseerd en heeft als doel om zoveel mogelijk content providers hun diensten 24 uur lang dual-stack te laten aanbieden.

De ondervraagde hosting providers zijn in meerderheid actief op het gebied van IPv6 en geven aan IPv6 in hun diensten te leveren of dit te kunnen leveren mocht dit noodzakelijk worden. De grootste belemmering die een deel van de hosting providers ervaart voor het daadwerkelijke gebruik is het gebrek aan IPv6 aansluitingen bij consumenten. Zij zijn geneigd te wachten tot ISP's hun klanten op IPv6 aansluiten zodat er ook bezoekers via IPv6 op door hun gehoste websites kunnen komen.

Op dit moment wordt beveiliging van IPv6 nog niet als reëel obstakel ervaren. Door het beperkte gebruik is het nog niet heel interessant om misbruik te maken van IPv6. Bovendien hebben andere obstakels bij de transitie naar IPv6 een hogere prioriteit. Het is te verwachten dat beveiliging van IPv6 in de toekomst een belangrijkere rol zal spelen, wanneer de afhankelijkheid ervan toeneemt.

[1] http://www.rijksoverheid.nl/zoeken?search-keyword=ipv6

Inhoudsopgave

1 Inleiding

Dit whitepaper beschrijft de derde meting in het kader van IPv6 monitoring in Nederland. Eerder zijn de Nulmeting[2] en Tweede Meting[3] gepubliceerd. In de tweede helft van 2011 zal nog een vierde meting gepubliceerd worden.

Uit de vorige metingen is gebleken dat IPv6 bewustzijn toeneemt, maar dat het nog op weinig plekken daadwerkelijk is geïntroduceerd. Vergeleken met de rest van Europa doet Nederland het echter niet slecht, al moet er nog veel gebeuren voordat IPv6 gemeengoed is.

Uit de nulmeting kwamen twee punten van zorg naar voren. Het eerste punt omvat de beschikbaarheid van IPv6 verbindingen voor eindgebruikers. Het tweede punt van zorg is de beschikbaarheid van content op en diensten over IPv6. Ook was het onvoldoende duidelijk of organisaties wel voldoende actie ondernemen.

In de tweede meting bleek dat de grote ISP's en mobiele operators zich aan het voorbereiden zijn om geen last te ondervinden van het opraken van de IPv4 adressen. Ze hebben plannen om IPv6 uit te gaan rollen variërend van 2011 tot 2013. Een belangrijke bottleneck voor ISP's om IPv6 nu al in te voeren zijn de kosten die het met zich meebrengt. Daarnaast is er een beperkte ondersteuning door fabrikanten. Bij de overheid is concreet actie ondernomen door IPv6 in november 2010 op te nemen in de "pas toe of leg uit"-lijst.

Uit onderzoek dat TNO en GNKS Consult hebben uitgevoerd voor de Europese Commissie is gebleken dat de bewustwording onder Europese ISP's in het afgelopen jaar sterk gestegen is. Maar ook hierbij wordt opgemerkt dat het aantal IPv6-enabled websites en het daadwerkelijke gebruik van IPv6 nauwelijks gestegen is in de afgelopen twee jaar.

In deze derde meting zal een update gegeven worden over de uitrol van IPv6, waarbij de stand van zaken rond april 2011 wordt beschreven.

1.1 Leeswijzer

Dit whitepaper is als volgt ingedeeld. Allereerst zal enige achtergrond informatie gegeven worden die speelt bij de introductie van IPv6 naast IPv4, waar specifiek aandacht gegeven wordt aan het veranderende uitgiftebeleid voor de laatste IPv4 adressen. In Hoofdstuk 3 wordt de leegloop van de IPv4 adresvoorraad en de uitgifte van IPv4 adressen door Regional Internet Registries (RIR's) besproken. Vervolgens zal in Hoofdstuk 4 ingegaan worden op de adoptie van IPv6, waarbij onder andere ingegaan wordt op de adresblok uitgifte, de ondersteuning van IPv6 door ISP's en het daadwerkelijke gebruik. In Hoofdstuk 5 wordt ingegaan op de ondersteuning door hosting partijen en productondersteuning bij leveranciers. Hoofdstuk 6 bespreekt beveiligingsissues omtrent IPv6. Tenslotte zullen in Hoofdstuk 7 de conclusies geformuleerd worden.

[2] http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2010/07/26/ipv6-monitoring-in-nederland-de-nulmeting.html
[3] http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/01/12/ipv6-monitoring-in-nederland-de-tweede-meting.html

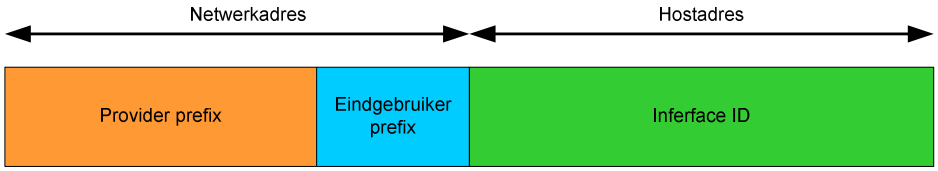
2 Introductie IPv6 naast IPv4

In dit hoofdstuk wordt enige achtergrondinformatie gegeven over de introductie van IPv6 naast IPv4, waarbij deels informatie is overgenomen uit de Nulmeting en de Tweede Meting[4,5]. Allereerst zal kort ingegaan worden op het gebruik van IPv4 en IPv6 adressen door eindgebruikers. Vervolgens wordt het uitgifteproces van IP adressen besproken, waarna er ingegaan wordt op het uitgiftebeleid van de laatste IPv4 adressen. Tenslotte wordt het belang van IP adressen in Nederland aangehaald.

2.1 IPv4 en IPv6 adressen bij eindgebruikers

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. Met 32 bits kunnen ongeveer 4,3 miljard unieke adressen gevormd worden. De adresruimte die IPv6 biedt met 128 bits wordt vaak duidelijk gemaakt aan de hand van vergelijkingen. Zoals het aantal IPv4 adressen dat gelijk is aan het aantal liters water in het IJsselmeer, terwijl het aantal IPv6 adressen vergelijkbaar is met het aantal liters water van alle wereldoceanen samen.

De IPv6 adresstructuur is weergegeven in Figuur 1. De eerste 64 bits worden gebruikt voor het netwerkadres en de laatste 64 bits voor het hostadres. Voor IPv6 zal een eindgebruiker een compleet netwerkadres aangeboden krijgen, waarbij de eindgebruiker het hostadres bepaalt op basis van het MAC adres of een ander mechanisme. Doordat per netwerkadres nog 2^{64} hostadressen beschikbaar zijn zal de daadwerkelijke utilisatie van de totale adresruimte van IPv6 uiteindelijk laag zijn.



Figuur 1: 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.

Met IPv4 krijgen typische eindgebruikers één publiek IP adres toegewezen (hoewel het ook voorkomt dat publieke IP adressen gedeeld worden onder meerdere eindgebruikers). Het verkrijgen van meer dan één adres is vaak moeizaam. Door middel van NAT kan de eindgebruiker meer dan één apparaat gebruiken achter hetzelfde IP adres, maar dit brengt moeilijkheden met zich mee wat betreft de bereikbaarheid van buitenaf voor individuele apparaten.

Met IPv6 zal de eindgebruiker over het algemeen minimaal een /64 aangeboden krijgen door de ISP. In 2002 is door de IETF RFC 3177 gepubliceerd met de aanbeveling om /48's aan eindgebruikers toe te wijzen. Dit betekent dat hiermee de

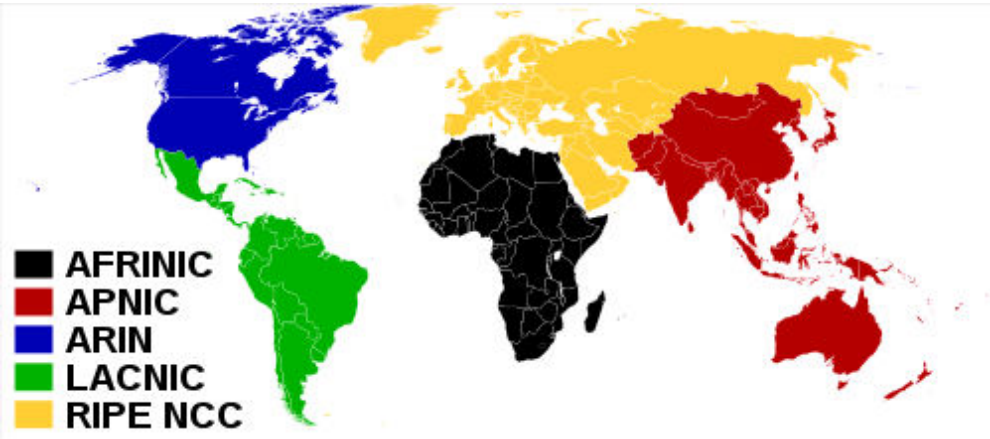
[4] http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2010/07/26/ipv6-monitoring-in-nederland-de-nulmeting.html
[5] http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/01/12/ipv6-monitoring-in-nederland-de-tweede-meting.html

eerste 48 bits van het IPv6 adres vast staan. Deze bits kunnen gezien worden als de provider prefix, zoals aangegeven in Figuur 1. Met de resterende bits in het netwerkadres, de eindgebruiker prefix, kunnen door de klant nog verschillende subnetten gemaakt worden. De in 2002 opgestelde RFC 3177 is in maart 2011 vervangen door RFC 6177 met het advies dat de exacte grootte van de provider en eindgebruiker prefix door de operationele partijen bepaald dient te worden. Er valt te beargumenteren dat een /48 in een aantal gevallen duidelijk overbodig is, en dat eindgebruikers met kleinere prefixen toe kunnen.

2.2 Het uitgifteproces 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), die 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 2.

Elke RIR kan een aanvraag doen bij de IANA 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.
Op 3 februari 2011 heeft IANA de laatste adresblokken uitgegeven waarmee de IPv4 adresvoorraad op mondiaal niveau leeg is.[6,7] De laatste toewijzing is een gehonoreerde aanvraag van APNIC. Tegelijkertijd zijn de laatste vijf gereserveerde adresblokken (allen ter grootte van één /8) verdeeld onder de vijf RIR's.



Figuur 2: De Regional Internet Registries (RIR's), en hun bedieninggebied.

2.3 Beleid uitgifte laatste IPv4 adresblokken door RIR's

Met de naderende schaarste van de IPv4 adressen passen de RIR's hun beleid aan betreffende het aanvragen en toewijzen van nieuwe IPv4 adressen. Het beleid is erop gericht om zeker te stellen dat nieuwe en opkomende netwerken ook in de toekomst kleine blokken IPv4 adressen kunnen krijgen, zodat deze met zowel

[6] http://www.icann.org/en/news/releases/release-03feb11-en.pdf
[7] http://www.nu.nl/internet/2436586/laatste-ipv4-adressen-uitgedeeld.html

gevestigde IPv4 als IPv6 netwerken kunnen communiceren, tijdens de transitie naar IPv6.

Elke RIR heeft zijn eigen beleid betreffende de laatste IPv4 adressen. Een samenvatting hiervan is gegeven in Tabel 1. Een aantal RIR's houdt een deel van de laatste /8 gereserveerd voor toekomstig gebruik. Op het moment dat de resterende adressen zijn uitgegeven, is de verwachting dat de gereserveerde adressen terug gaan naar de adresvoorraad voor uitgifte.

Tabel 1 Overzicht van het beleid van RIR's betreffende de uitgifte van de laatste IPv4 adressen.

	RIPE	**APNIC**	**ARIN**	**LACNIC**	**AfriNIC**[1]
Bij welke grootte van de RIR adresvoorraad gaat het beleid in?	/8	/8	/8	/12	/11[2]
Grootte van de IPv4 adresblok allocaties?	/22	/22	equiv. 3 mnd[6]	/24 - /22	/27 - /22
Uitsluitend allocaties aan nieuwe LIR's?	nee	nee	nee	ja[3]	nee
Kan LIR slechts eenmalig uit de resterende voorraad putten?	ja	ja	nee[4]	ja	nee
Moet LIR een IPv6 allocatie hebben voordat nieuwe IPv4 adressen worden aangevraagd?	ja	nee	nee	nee	ja[5]
Heeft RIR een adresblok gereserveerd voor toekomstig gebruik?	-	/16	/10	-	/12

[1] Het weergegeven beleid ligt nog ter goedkeuring en is nog niet definitief geïmplementeerd. (d.d. 25-11-2010)

[2] Op het moment dat de grootte van de IPv4 adresvoorraad gelijk is aan één /8, wordt de maximale allocatie grootte al aangepast naar een /13.

[3] Tenzij beargumenteerd kan worden dat de adressen benodigd zijn voor kritieke infrastructuren.

[4] De minimale tijd tussen nieuwe aanvragen is 3 maanden.

[5] Als de aanvrager nog geen IPv6 allocatie heeft, zal tegelijkertijd met de IPv4 allocatie een IPv6 allocatie gedaan worden.

[6] Er kan tot maximaal voor 3 maanden aan adressen worden aangevraagd per keer.

APNIC heeft op 15 april 2011 het moment bereikt waarbij hun voorraad IPv4 adressen nog één /8 bevat[8]. Hiermee gaat het uitgiftebeleid in zoals weergegeven in Tabel 1. Door de ongekende groei van vaste en mobiele netwerken in de Asia-Pacific regio is dit moment snel dichterbij gekomen, sinds de uitputting van de IANA IPv4 adresvoorraad. Voor veel operatoren zal het ingaan van dit beleid effectief betekenen dat de voorraad IPv4 adressen leeg is.[9]

[8] http://www.apnic.net/publications/news/2011/final-8

[9] http://www.zdnet.com/blog/networking/it-8217s-official-asia-8217s-just-run-out-of-ipv4-addresses/948

2.4 Het gebruik en belang van IP adressen in Nederland

Een IP adres is van belang om toegang tot het Internet te hebben. Wereldwijd groeit het aantal mensen dat toegang heeft tot het Internet steeds verder. Nederland is koploper in de Europese Unie op het gebied van computerbezit en internettoegang. In 2010 beschikte 92% van de Nederlandse huishoudens over een computer en beschikte 91% over internettoegang. Ook in Luxemburg, Zweden, Noorwegen en Denemarken heeft meer dan 80% van de huishoudens toegang tot het Internet. Het gemiddelde in de EU27 ligt op 65,2%. Tabel 2 geeft een overzicht hoe de toegang tot pc's en het Internet over de afgelopen 6 jaar is veranderd.

Tabel 2: Overzicht van het aantal huishoudens in Nederland en de toegang tot een pc en het Internet, 2005-2010

	2005	**2006**	**2007**	**2008**	**2009**	**2010**
Aantal huishoudens (in miljoenen)	7,190	7,146	7,190	7,242	7,313	7,386
Toegang tot pc (% huishoudens)	83	84	86	88	91	92
Toegang tot internet (% huishoudens)	78	80	83	86	90	91

Enkele jaren geleden was de desktop nog het middel bij uitstek om het Internet te gaan. In de afgelopen jaren is gebruik van de laptop en de mobiele telefoon voor internettoegang echter sterk gestegen. In de afgelopen 6 jaar is het gebruik van een laptop onder de internetgebruikers gestegen van 27% naar 73%. Ook de mobiele telefoon laat een stijging zien van meer dan 25%, zoals als weergegeven in Tabel 3. Naast de laptop en de mobiele telefoon is de televisie een apparaat dat steeds meer gebruikt wordt voor internettoegang.

Tabel 3: Overzicht van het gebruik van apparatuur om toegang te hebben tot het Internet. Percentage van alle internetgebruikers in Nederland dat een bepaald apparaat gebruikt.

	Desktop	**Laptop**	**Mobiele telefoon**
2005	95%	27%	13%
2006	93%	33%	14%
2007	91%	44%	21%
2008	87%	56%	24%
2009	86%	65%	30%
2010	83%	73%	39%

In Tabel 4 is een overzicht gegeven met het aantal breedband- en mobiele telefoonaansluitingen. Ook in de afgelopen twee jaar is het aantal aansluitingen nog flink gestegen, waarbij het aantal breedband internetaansluitingen steeds dichter bij het aantal huishoudens komt.

Tabel 4: Overzicht met het aantal breedband internet- en mobiele telefoonaansluitingen (in miljoenen) in Nederland.

	2004	**2006**	**2008**	**2010**
Breedband internetaansluitingen	3,09	5,23	5,74	6,31
Mobiele telefoonaansluitingen	15,90	17,00	19,80	20,73
Totaal aantal aansluitingen	18,99	22,23	25,54	27,04

Zowel de groeiende internettoegang onder huishoudens als het meer gevarieerd gebruik van apparaten voor toegang tot het Internet, zorgt ervoor dat het gebruik van IP adressen steeds verder groeit. Nederland heeft tot 2011 in totaal ruim 24 miljoen IPv4 toegewezen gekregen. 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.

3 Leegloop IPv4 adresvoorraad en uitgifte IPv4 adressen

In dit hoofdstuk zal een overzicht van de stand van zaken gegeven worden met betrekking tot de IPv4 adresvoorraden bij de RIR's en de uitgifte van IPv4 adressen.

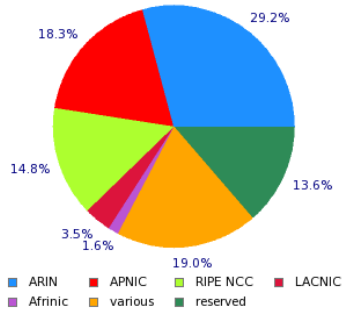
3.1 IPv4 adresvoorraad

Mondiale adresvoorraad

Op 3 februari 2011 is de laatste IPv4 aanvraag gehonoreerd en zijn de resterende /8 blokken verdeeld onder de RIR's[10]. Hiermee is de mondiale IPv4 adresvoorraad leeg. In Tabel 5 is een overzicht gegeven van distributie van /8 blokken onder de RIR's. In Figuur 3 is deze verdeling grafisch weergegeven. Een deel van de adressen is gereserveerd en bestemd voor o.a. multicast, interne netwerken en toekomstig gebruik. De adressen in de categorie 'various' zijn veelal allocaties uit de periode voor het bestaan van de RIR's.

Tabel 5: Verdeling /8's onder RIR's

	/8's	**%**
ARIN	75.00	29.2
APNIC	47.00	18.3
RIPE NCC	37.00	14.8
LACNIC	9.00	3.5
AfriNIC	4.00	1.6
various	48.92	19.0
reserved	35.08	13.6
total	*256.00*	*100.0*

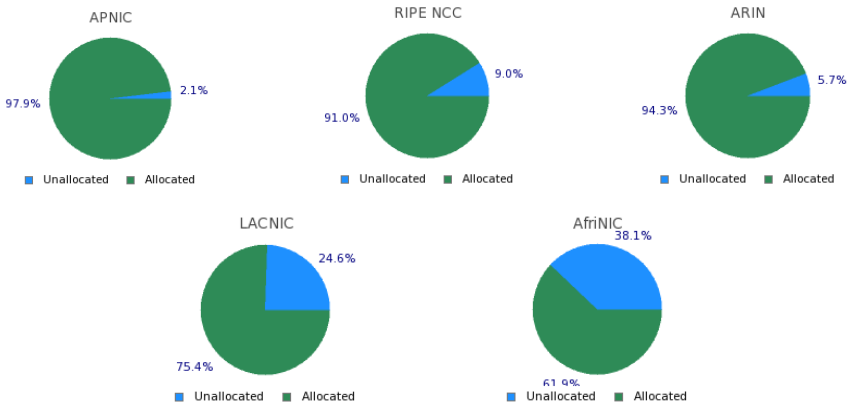


Figuur 3: Grafische verdeling /8's onder RIR's

Adresvoorraad per RIR

Nu de mondiale adresvoorraad bij IANA leeg is kunnen de RIR's hun voorraden niet meer aanvullen. In Figuur 4 wordt per RIR getoond hoe groot de resterende adresvoorraad nog is per 07-04-2011. Bij de APNIC, RIPE NCC en ARIN is de resterende hoeveelheden IPv4 adressen nog beperkt en zal naar verwachting het eerste het beleid omtrent de laatste IPv4 adressen in werking treden, zoals besproken in paragraaf 2.3.

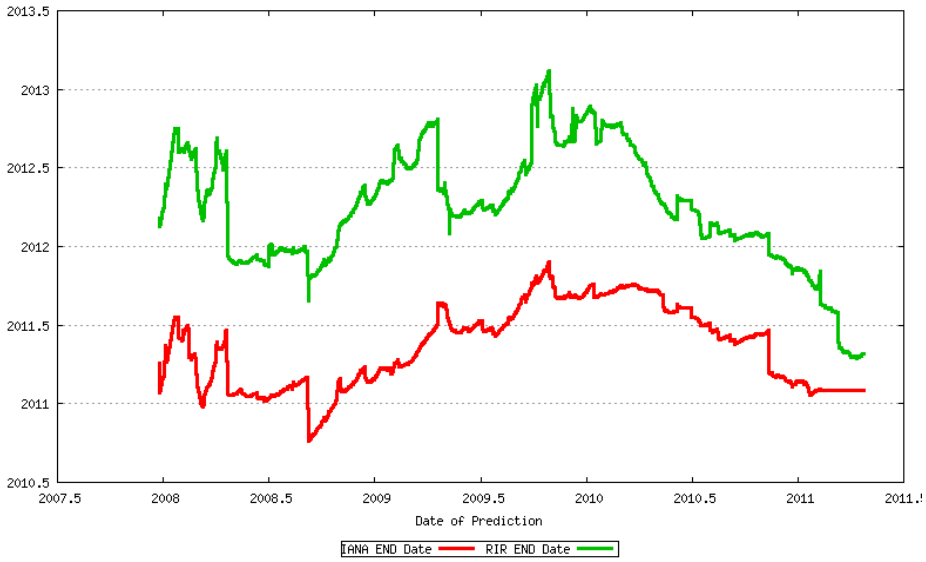
[10] http://www.nro.net/news/ipv4-free-pool-depleted



Figuur 4: Overzicht van de IPv4 adresvoorraad in de RIR pools. Status per 26-04-2011.

Uitputtingsdatum

De uitputtingsdatum van een RIR wordt gezien als die datum waarop het nieuwe uitgiftebeleid ingaat (zoals besproken in paragraaf 2.3). Het moment waarop een RIR dit moment bereikt is moeilijk exact te voorspellen. In Figuur 5 is de voorspelling van de uitputtingsdatum van de IANA en APNIC grafisch weergegeven, ten opzichte van de datum waarop de voorspelling is gedaan. Voor beide voorspellingen geldt dat de uitputtingsdata uiteindelijk veel sneller waren dan in eerste instantie voorspeld werd. De APNIC heeft op 15 april 2011 het moment bereikt waarbij hun voorraad IPv4 adressen nog één /8 bevat[11]. Het wordt verwacht dat de RIPE NCC als tweede door haar adresvoorraad is.



Figuur 5: Voorspelling van de uitputtingsdatum voor IPv4, uitgezet tegen de datum waarop de voorspelling is gedaan. De 'RIR end date' geeft de uitputtingsdatum voor de eerste RIR weer, welke in dit geval APNIC is. (bron: potaroo.net, d.d. 26-04-2011)

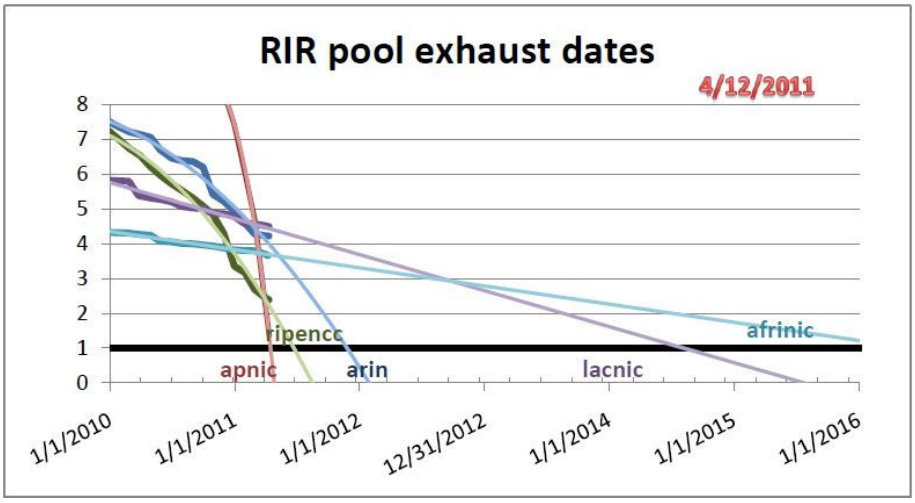
De discontinuïteiten in de grafiek ontstaan door wijzigingen in uitgifte beleid en de uitgave van relatief grote adresblokken. De trend is te verklaren door het toenemen van de vraag naar IPv4 adressen, zoals besproken wordt in de volgende sectie.

[11] http://www.apnic.net/publications/news/2011/final-8

Naast de voorspelling van Geoff Huston, wordt op ipv4depletion.com ook een voorspelling gedaan over de uitputtingsdata. Deze zijn weergegeven in Tabel 6. Op http://penrose.uk6x.com/ stelt BT dat RIPE op 1 februari 2012 de uitputtingsdatum bereikt. Op http://www.tndh.net/~tony/ietf/ipv4-pool.htm wordt door Tony Hain (CISCO) voorspeld dat RIPE eind juni 2011 al de uitputtingsdatum bereikt, zoals weergegeven in Figuur 6.

Tabel 6: Overzicht uitputtingsdata RIR's, zoals voorspeld door ipv4depletion.com, d.d. 08-04-2011

RIR	**Depletion date**
APNIC: Asia/Pacific	2011-04-23
RIPE NCC : Europe and Middle East	2012-05-27
ARIN: North America	2013-02-02
AfriNIC: Africa	2015-04-28
LACNIC: South America	2015-09-14



Figuur 6: Grafische weergave uitputtingsdata voor RIR's [bron: http://www.tndh.net/~tony/ietf/ipv4-pool.htm]

Het is duidelijk dat er veel variatie bestaat in de gedane voorspellingen over de uitputtingsdata van de RIR's. Dit heeft o.a. te maken met de vele factoren waarmee rekening gehouden moet worden. In de afgelopen jaren is het aantal aangevraagde adressen wereldwijd gestegen, is de voorraad IPv4 adressen bij IANA sneller leeg geraakt dan voorspeld en is daarop volgend de voorraad bij APNIC snel afgenomen. Door al deze ontwikkelingen is het moeilijk exact te voorspellen wanneer de andere RIR's door hun IPv4 adresvoorraad heen zullen zijn.

Teruggave IPv4 adressen aan RIPE

In 2010 zijn er zo'n 500.000 IPv4 adressen terug gegaan naar de RIPE adresvoorraad. Dit aantal is niet wezenlijk anders dan in voorgaande jaren. Teruggave van adressen is voornamelijk het gevolg van faillissementen. Op 25 maart 2011 kwam in het nieuws dat Microsoft 667 duizend IPv4 adressen wil kopen van het failliete Nortel.[12] RIPE geeft aan dat er in Europa op dit moment nog geen sprake is van betaalde overdrachten van IPv4 adresblokken tussen LIR's. Een belangrijke motivatie hiervoor is dat LIR's nog steeds aanvragen kunnen doen bij

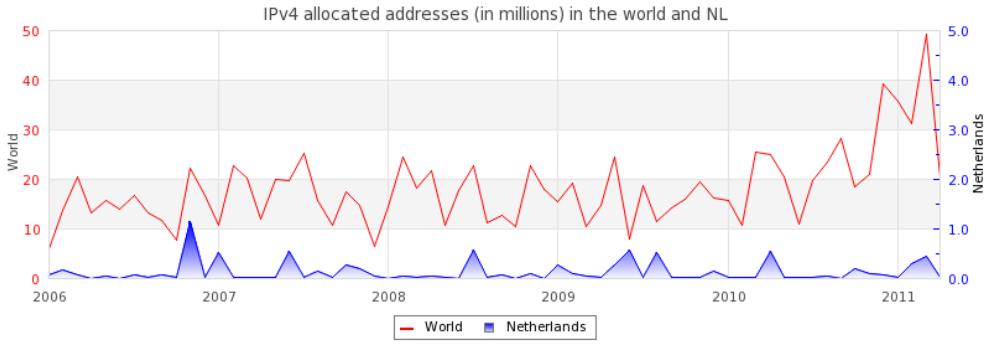
[12] http://www.pcmag.com/article2/0,2817,2382616,00.asp

RIPE zonder dat dit kosten met zich meebrengt. Wel is het zo dat door fusies en overnames van bedrijven adresblok verschuivingen plaatsvinden. Dit speelt echter al jaren en is in de afgelopen jaren niet wezenlijk veranderd.

3.2 IPv4 uitgifte

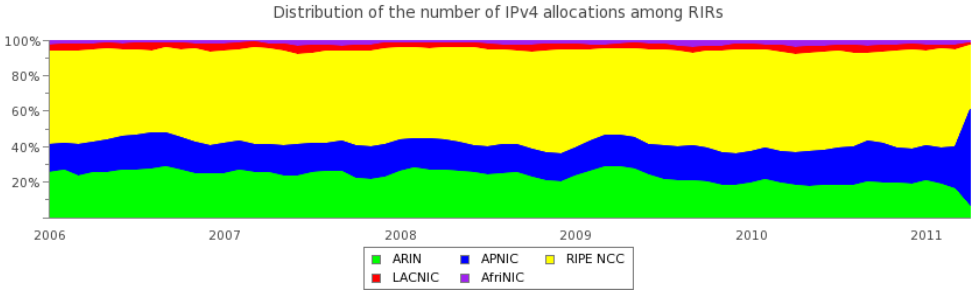
Wereldwijd

In Figuur 7 wordt de uitgifte van IPv4 /8 blokken weergeven, voor zowel de wereld als Nederland specifiek. In het laatste halfjaar is een duidelijke trend te zien, waarbij het aantal toegewezen adressen stijgt. Hierdoor komt de uitputtingsdatum van de RIR's steeds verder naar voren, zoals is weergegeven in Figuur 5.

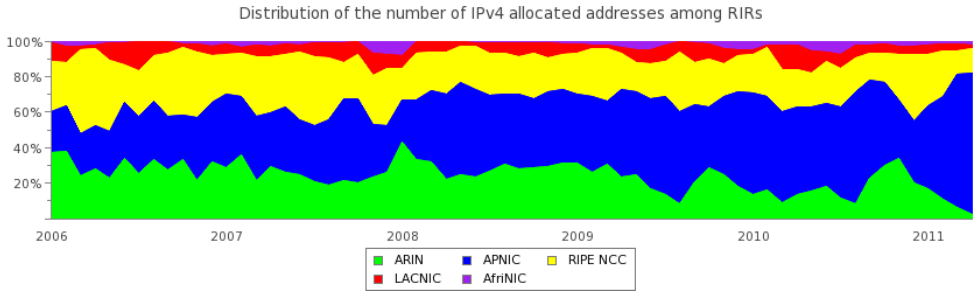


Figuur 7: Uitgegeven IPv4 adressen (in miljoenen) in de wereld en in Nederland

Het grootste deel van de adressen wereldwijd werd tot nu toe uitgegeven door APNIC, tot haar uitputting op 15 april 2011. In Figuur 8 en Figuur 9 wordt respectievelijk een grafische weergave van de verdeling van het aantal allocaties per RIR en het daadwerkelijke aantal toegewezen adressen per RIR gegeven. In april 2011 is er een enorme stijging in het aantal adresaanvragen bij APNIC waar te nemen. Waar het maandelijkse aantal toewijzingen in de afgelopen jaren voor APNIC altijd kleiner was dan 200, is het aantal toewijzingen in maart en april gestegen naar respectievelijk meer dan 300 en meer dan 1600. De consumptie van IPv4 adressen in Zuid-Oost Azië (APNIC) kan voornamelijk toegewezen worden aan China en Japan.



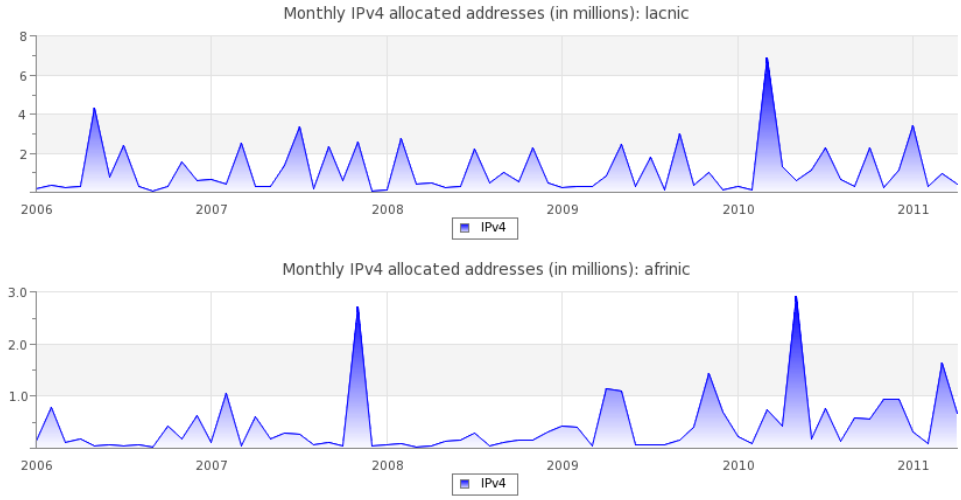
Figuur 8: Procentuele verdeling van het aantal IPv4 allocaties, verdeeld onder de RIR's (update: 26-04-2011)



Figuur 9: Procentuele verdeling van het aantal uitgegeven IPv4 adressen, verdeeld onder de RIR's (update: 26-04-2011)

Het valt op dat vanaf februari 2011 het aantal uitgegeven adressen sterk gegroeid is. Dit is ook goed zichtbaar in Figuur 10. Er is een duidelijke *run* te constateren rondom het moment dat de IANA IPv4 adresvoorraad is leeg geraakt (3 feb 2011). RIPE heeft aangegeven ook een tijdelijke stijging in het aantal IPv4 aanvragen waar te nemen, die ongeveer 1 à 2 weken aan hield, rond de IANA *run-out*. Tijdens de *run-out* van APNIC was geen merkbare stijging waar te nemen. Dit heeft mogelijk drie verschillende redenen. Ten eerste speelt de *run-out* in een ander bedieningsgebied dan dat van RIPE. Ten tweede kan de leegloop bij APNIC als 'oud nieuws' ervaren worden, aangezien slechts twee maanden eerder de IANA voorraad leeg was. En ten derde zijn de LIR's in het bedieningsgebied mogelijk al verzadigd met IPv4 adressen, naar aanleiding van de gedane aanvragen in februari. RIPE geeft op haar website een wekelijkse update van de IPv4 voorraad.[13]

[13] http://www.ripe.net/internet-coordination/ipv4-exhaustion/ipv4-available-pool-graph



Figuur 10: Maandelijkse adresuitgifte in miljoenen IPv4 adressen, weergegeven per RIR (update: 26-04-2011)

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 7 blijkt dat Nederland in 2010 ongeveer 1,13 miljoen adressen toegewezen heeft gekregen, ten opzichte van ruim 2 miljoen in 2009. Het totale aantal IPv4 adressen dat Nederland t/m 2010 heeft aangevraagd komt daarmee op ruim 24 miljoen.

Tabel 7: Het aantal toegewezen IPv4 adressen (in miljoenen /32's)[14]

	2005	**2006**	**2007**	**2008**	**2009**	**2010**
RipeNCC	61.32	55.54	60.86	44.40	44.18	65.07
ARIN	47.43	46.55	53.03	57.18	41.29	45.24
APNIC	53.66	51.44	69.68	88.87	86.98	120.39
LACNIC	10.94	11.42	14.73	11.32	10.93	17.28
AfriNIC	1.88	5.34	11.06	3.16	11.98	17.04
Totaal	175.23	170.29	209.36	204.93	195.36	265.02
Nederland	2,12	1,72	1,86	0,91	2,08	1,13

3.3 Conclusie

De algemene trend van het aantal uitgegeven IPv4 adressen is stijgend. Per 3 februari 2011 is de IANA IPv4 adresvoorraad uitgeput, waardoor RIR's hun voorraad niet meer kunnen aanvullen. Rond deze periode was er een duidelijke stijging te zien in het aantal adresaanvragen. Vooral bij APNIC zijn zeer veel aanvragen gedaan, omdat men zich waarschijnlijk realiseerde dat het om de laatste IPv4 adressen ging. Op 15 april 2011 is bij APNIC de uitputtingsdatum bereikt, omdat de voorraadgrens van één /8 is bereikt. Hierdoor is het uitgiftebeleid veranderd. In deze maand zijn bij APNIC een recordaantal aanvragen gedaan van meer dan 1600, terwijl in voorgaande jaren het aantal maandelijkse aanvragen nooit meer dan 200 was.

[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.

Ook RIPE heeft een tijdelijke stijging in het aantal aanvragen geconstateerd begin februari van enkele weken. Rond de uitputtingsdatum van APNIC is er echter geen stijging opgemerkt. Het is waarschijnlijk dat RIPE de eerstvolgende RIR zal zijn die door haar adresvoorraad heen is en de grens van één /8 bereikt. Op dat moment zal ook bij RIPE een veranderd uitgiftebeleid van kracht worden.

4 De adoptie van IPv6

4.1 Uitgifte IPv6

Wereldwijd

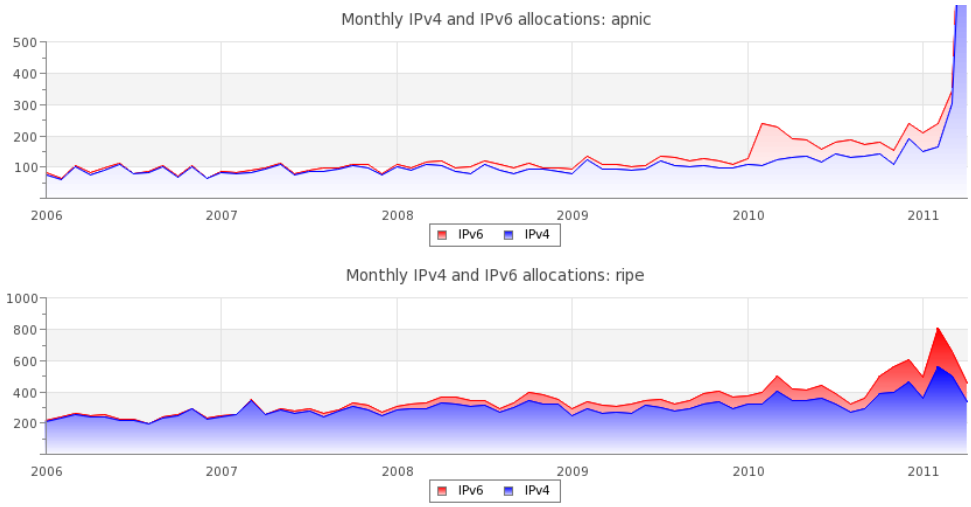
De uitgifte van IPv6 adresblokken is gaande sinds 1999. In Tabel 8 is te zien dat er pas in de afgelopen 4 jaar over substantiële aantallen aanvragen gesproken kan worden. In het jaar 2010 is er plotseling een enorme stijging te zien in het aantal aanvragen bij APNIC. Australië, China, India en Japan samen hebben met 368 aanvragen in 2010 tweemaal zo veel aanvragen gedaan als totaal in 2009 gedaan zijn.

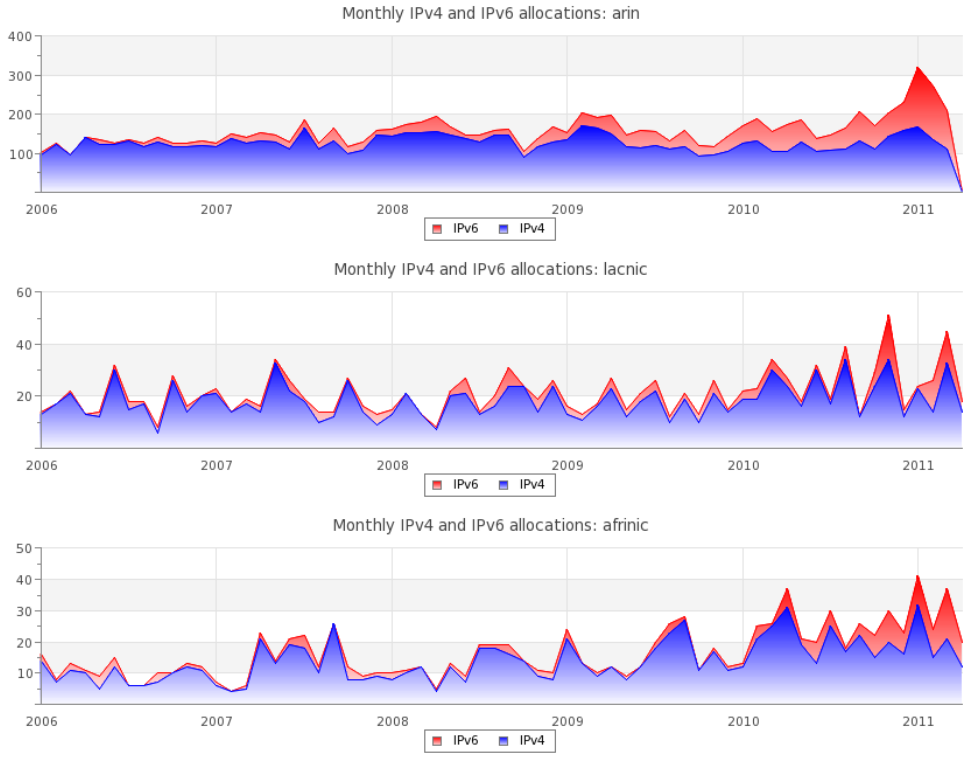
Ook de andere RIR's laten een continue stijging zien in het aantal aanvragen. Het totale aantal aanvragen is 2010 verdubbeld ten opzichte van 2009. Hier is een duidelijke trend te constateren in IPv6 adresaanvraag en –uitgifte.

Tabel 8: Aantal individuele IPv6 toewijzingen (ongeacht adresblokomvang) bij de Regional Internet Registries (RIR's)[15]

	2005	**2006**	**2007**	**2008**	**2009**	**2010**
RipeNCC	96	92	161	431	631	1045
ARIN	59	70	212	230	383	636
APNIC	54	43	63	161	191	669
LACNIC	31	16	25	30	33	50
AfriNIC	3	18	19	16	13	55
Totaal	243	239	480	868	1251	2455

In onderstaande figuren zijn het aantal IPv4 en IPv6 allocaties (ongeacht adresblokomvang) weergegeven per RIR. De eerste figuur laat een zeer grote hoeveelheid aanvragen zien voor APNIC in april 2011. Deze maand zijn er meer dan 1600 IPv4 toewijzingen gedaan, en meer dan 60 IPv6 toewijzingen.





Figuur 11: Het aantal maandelijkse allocaties (ongeacht adresblokgrootte) dat gedaan wordt voor IPv4 en IPv6, weergegeven per RIR (update: 26-04-2011)

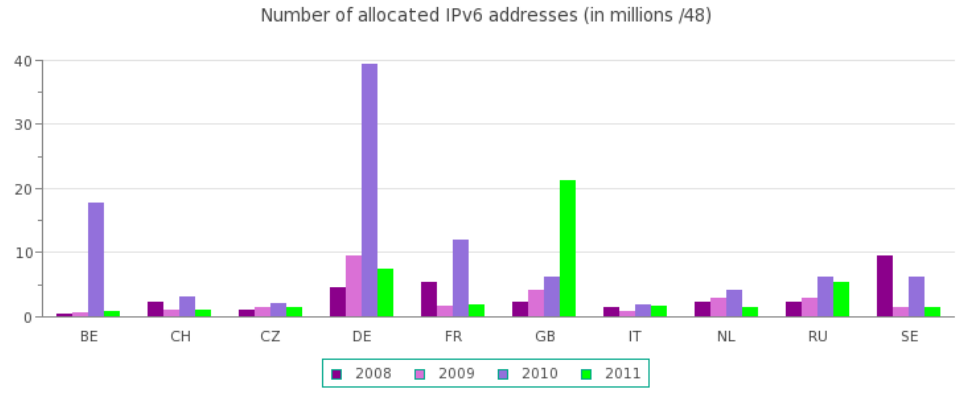
Hoewel het aantal aanvragen voor IPv6 adresblokken in de afgelopen jaren vooral door RIPE NCC en ARIN werden gedomineerd, zijn de landen die bediend worden door APNIC met een flinke opmars bezig. Waar de verklaring voor het grote aantal aanvragen in West-Europa en Noord-Amerika vooral wordt veroorzaakt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

Nederland

In Tabel 9 is te zien dat er door Nederland in 2010 ruim 4 miljoen IPv6 /48's zijn aangevraagd. Ten opzichte van voorgaande jaren is een constante groei in de aanvraag van IPv6 adressen waar te nemen, met af en toe een grote uitschieter, zoals ook weergegeven in Figuur 12.

Tabel 9: Top 10 landen met de meest toegewezen IPv6 adressen (in miljoenen /48's) per jaar

	2007		2008		2009		2010	
1	Australië	268,89	Brazilië	4307,55	VS	15,28	Japan	165,02
2	Engeland	68,75	VS	948,83	Duitsland	9,44	Duitsland	39,39
3	Japan	67,44	Zweden	9,37	Engeland	4,06	VS	34,61
4	VS	8,19	Frankrijk	5,37	**Nederland**	3,01	China	22,22
5	Duitsland	5,77	Duitsland	4,52	Australië	2,88	België	17,69
6	Taiwan	4,26	Engeland	2,36	Rusland	2,88	Frankrijk	11,86
7	Polen	1,18	**Nederland**	2,23	Japan	2,22	Zuid-Afrika	9,83
8	Uruguay	1,05	Rusland	2,16	Frankrijk	1,64	Australië	6,62
9	Canada	0,85	Zwitserland	2,16	Tsjechië	1,44	Zweden	6,23
10	Rusland	0,72	China	1,70	Zweden	1,44	Rusland	6,23
12							**Nederland**	4,19



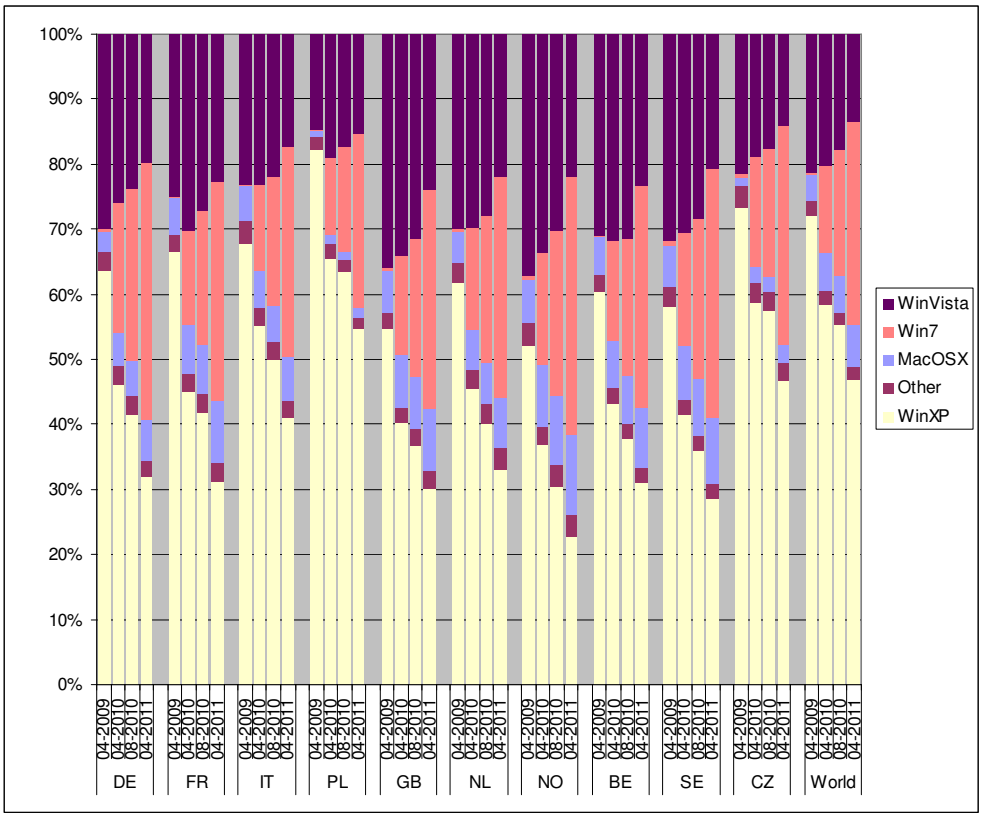
Figuur 12: Hoeveelheid aangevraagde IPv6 adressen (in miljoenen /48) voor de Top 10 landen in Europa met de meest aangevraagde adressen (update: 26-04-2011)

4.2 Ondersteuning 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. In Windows XP wordt IPv6 niet direct ondersteund, maar kan de IPv6 stack wel geïnstalleerd worden[15]. Daarnaast verlopen DNS requests bij Windows XP altijd over IPv4.

In Figuur 13 is te zien dat het aandeel van Windows XP steeds verder daalt. Dit jaar is het aandeel wereldwijd zelfs onder de 50% gekomen. Verder valt op dat het aandeel van Windows 7 sterk groeit, en hierbij voornamelijk het aandeel van Windows XP en Vista overneemt.

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



Figuur 13: Marktaandeel besturingssystemen (procentueel) voor de top 10 Europese landen met de meeste IPv6 allocaties en wereldwijd

4.3 Ondersteuning van IPv6 door ISP's

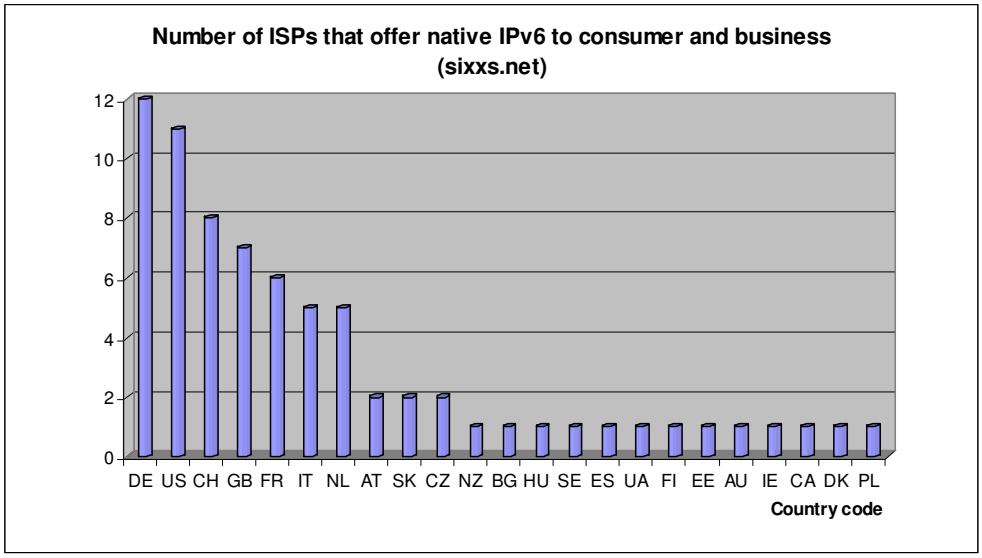
In deze paragraaf wordt gekeken naar het aantal ISP's dat op dit moment native IPv6 verbindingen kan leveren aan gebruikers. Op de vergelijkingssite internetten.nl wordt sinds dit jaar ook de IPv6 geschiktheid vermeld van Nederlandse providers[16]. Hier wordt zowel gekeken naar het gebruik van een native verbinding, alsmede de mogelijkheid om een tunnel op te zetten.

Europa
Een overzicht van ISP's die een native IPv6 verbinding aanbieden aan hun klanten (consumenten en zakelijke klanten) wordt bijgehouden door de website sixxs.net. Op deze website is een overzicht te vinden met de belangrijkste ISP's, onderverdeeld per land.
In Figuur 14 zijn deze resultaten weergegeven in een staafdiagram. In de tweede meting is het aantal ISP's met 5 gegroeid. Ten opzichte van de tweede meting zijn er sindsdien 2 ISP's toegevoegd. Eén Nederlandse provider die hiertoe behoort was in de tweede meting al meegenomen in de volgende alinea.

Nederland
Buiten de gegevens van sixxs.net zijn er in Nederland nog enkele ISP's te vinden die IPv6 verbindingen aanbieden aan een beperkte klantgroep.

[16] http://www.internetten.nl/div/document.asp?id=11224

In totaal zijn er twaalf 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, Proserve Intermax, Luna, Tele2, KPN International en Global Crossing. XS4ALL biedt IPv6 aan voor consumenten. 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.



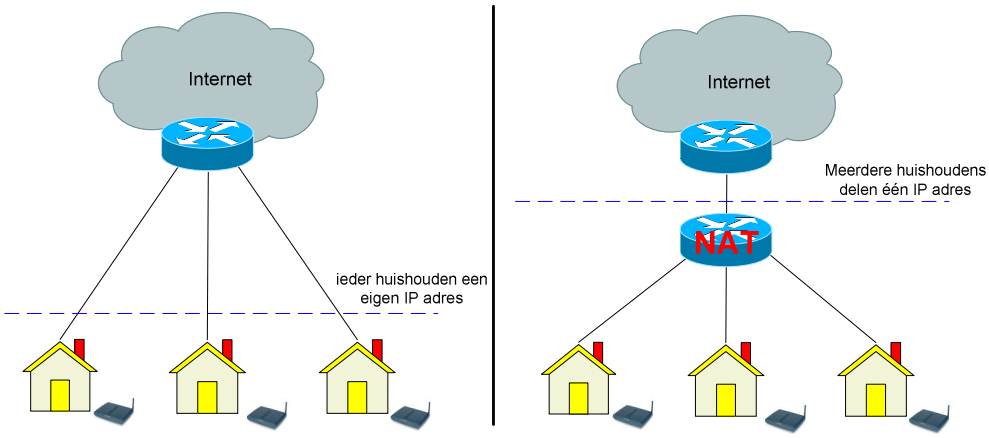
Figuur 14: Aantal ISP's per land dat commercieel IPv6 verbindingen aanbiedt aan consumenten en/of zakelijke gebruikers per 07-04-2011 (bron: sixxs.net)

4.3.1 Large Scale NAT

Uit Hoofdstuk 4 blijkt dat het gebruik van IPv6, ondanks het (bijna) opraken van de verschillende adresvoorraden, het afgelopen halfjaar vrijwel niet is toegenomen. Dit brengt het risico met zich mee dat ISP's gebruik zullen gaan maken van Large Scale NAT (LSN) in hun accessnetwerk, ook wel Carrier Grade NAT (CGN) genoemd. LSN is een techniek waarbij meerdere huishoudens een IP adres delen, zoals voor vaste verbindingen is weergegeven in Figuur 15. Voor mobiele gebruikers wordt deze technologie ook toegepast.

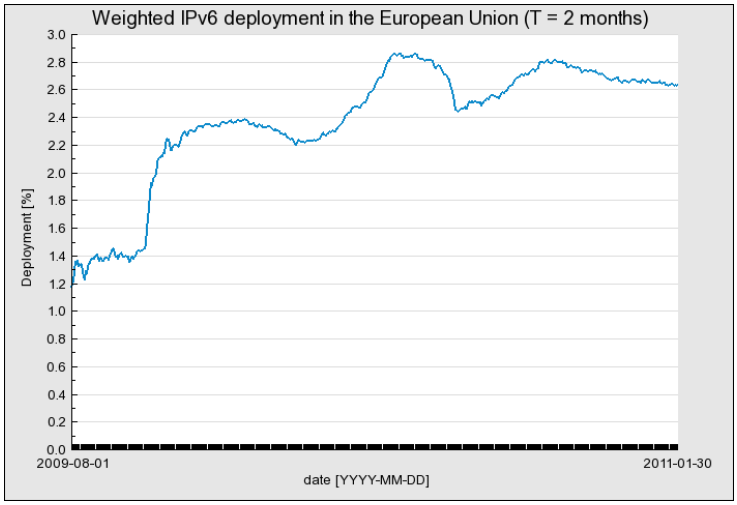
Op zich biedt LSN een oplossing voor ISP's, die niet op tijd IPv6 kunnen bieden, of als content providers hun diensten niet op tijd via IPv6 aanbieden. In het gebruik van LSN schuilen echter ook een aantal nadelen, waardoor het bij voorkeur niet, en anders slechts als tijdelijke oplossing zou moeten worden ingezet. De nadelen hebben onder andere te maken het feit dat er een 'obstructie' in het ISP netwerk komt, waardoor sommige applicaties niet vanzelfsprekend meer werken. Een ander issue is de beperking van het aantal transportsessies[17] dat naar het internet kan worden opgezet. Een uitgebreidere discussie over LSN is te vinden op http://weblog.chrisgrundemann.com/index.php/2011/nat444-cgn-lsn-breaks.

[17] *Transportsessies* zijn verbindingen die worden opgezet als iemand een internetdienst gebruikt. Sommige applicaties gebruiken meerdere sessies tegelijkertijd.

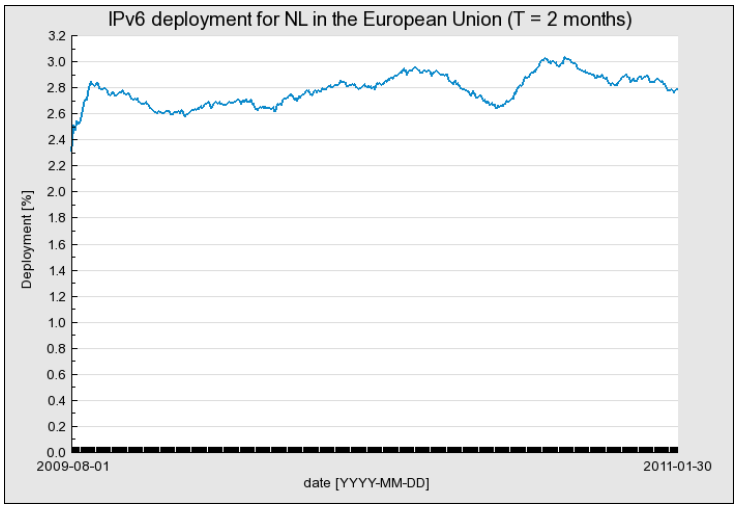


Figuur 15: Traditionele internetverbinding zonder LSN (links) en een verbinding met LSN (rechts)

4.4 IPv6 adoptie door eindgebruikers



Figuur 16: Percentage unieke Europese gebruikers (bepaald over een periode van 2 maanden) die websites over IPv6 kunnen benaderen van 1-8-2009 tot 30-1-2011.



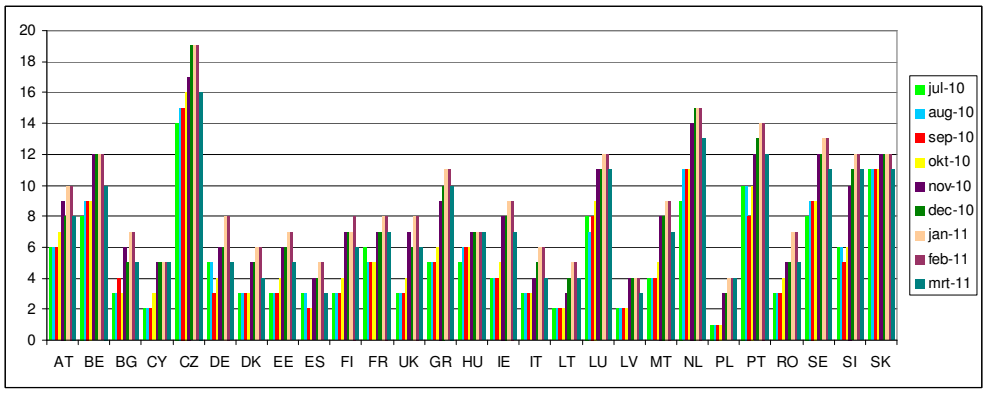
Figuur 17: Percentage unieke Nederlandse gebruikers (bepaald over een periode van 2 maanden) die websites over IPv6 kunnen benaderen van 1-8-2009 tot 30-1-2011.

Europa
Figuur 16 geeft het verloop weer van het percentage Europese Internet gebruikers die in staat is websites via IPv6 te benaderen. Het gaat in dit geval om een gewogen gemiddelde naar het percentage op het Internet aangesloten gebruikers per EU lidstaat. Hoewel de laatste maanden een daling is waar te nemen, laat het gewogen gemiddelde over een jaar een groei laat zien van een aantal tienden van procenten. Ook RIPE geeft aan nog weinig verkeer te zien op basis van gebruikersstatistieken, ondanks een stabiele toename van het aantal IPv6 aanvragen.

Nederland
Figuur 17 geeft het verloop weer van het percentage Nederlandse Internet gebruikers die in staat is websites via IPv6 te benaderen. Er is een kleine groei te zien van enkele tienden van procenten per jaar.

4.5 Websites bereikbaar over IPv6

Bij monitoren van daadwerkelijk gebruik kan er onder andere gedacht worden aan de ondersteuning van IPv6 door gehoste websites. Hiervoor is voor elke Europese lidstaat de top 500 van de meest populaire websites genomen (bron: http://www.alexa.com), waarbij onderzocht wordt of deze bereikbaar zijn over zowel IPv4 als IPv6. In Figuur 18 is een overzicht gegeven van voor de Europese lidstaten vanaf juli 2010.



Figuur 18: Aantal websites in de top 500 meest populaire websites per lidstaat van de EU, die bereikbaar zijn over zowel IPv4 als IPv6 sinds juli 2010.

Europa
Het valt op dat voor de meeste Europese lidstaten het aantal websites dat beschikbaar werd over IPv6 in het afgelopen jaar is toegenomen. Desondanks is het absolute aantal nog steeds laag.

Nederland
Met betrekking tot het aantal populaire Nederlandse websites dat via IPv6 benaderbaar is loopt Nederland nog steeds mee voorop in Europa.

4.6 Conclusie

Er is een stabiele stijging waar te nemen in het aantal IPv6 aanvragen. In 2010 is het aantal aanvragen ten opzichte van 2009 bijna verdubbeld. Ook Nederland laat jaarlijks een stijging in het aantal aanvragen zien. De stijgende groei is bij alle RIR's waar te nemen, maar de sterkste groei is te zijn bij APNIC. De noodzaak voor IPv6 is hier sterker dan bij andere RIR's, aangezien de IPv4 adresvoorraad op 15 april 2011 uitgeput raakte.

Het daadwerkelijke gebruik van IPv6 is nog erg beperkt in Europa. Een kleine 3% van de internetgebruikers is in staat websites over IPv6 te bereiken. Voor Nederland specifiek is dit percentage vergelijkbaar. Het aantal websites dat te bereiken is over IPv6 is nog steeds erg laag, maar stijgt wel licht. In maart 2011 waren er in Nederland 13 van de 500 populairste websites over IPv6 benaderbaar. Hiermee loopt Nederland mee voorop in Europa.

Een beperkt daadwerkelijk gebruik is deels te wijden aan de beperkte ondersteuning van IPv6 door ISP's. Vooral voor consumenten is er weinig verandering op te merken in de beschikbaarheid van IPv6 aansluitingen in Europa. In Nederland is XS4ALL vooralsnog de enige ISP die IPv6 aansluitingen aanbiedt aan consumenten. Op de zakelijke markt is er een zeer lichte stijging waar te nemen. Verder is er kort ingegaan op large scale NAT om de problematiek omtrent het gebruik hiervan te illustreren. In de volgende meting zal hier uitgebreider op ingegaan worden.

5 Ondersteuning IPv6 door hosting providers en leveranciers

In het vorige hoofdstuk is geconstateerd dat er bewustwording is omtrent IPv6, maar dat dit zich nog niet vertaalt in daadwerkelijk gebruik. Onderdeel van het kunnen gebruiken van IPv6 is de ondersteuning van IPv6 in producten en diensten. Hosting partijen spelen hier een belangrijke rol in. In dit hoofdstuk wordt inzicht gegeven in de status van IPv6 ondersteuning voor hostingdiensten enerzijds en consumentenproducten anderzijds. Allereerst wordt ingegaan op World IPv6 Day waarbij websites collectief dual-stack bereikbaar worden gemaakt. Ten tweede worden de ontwikkelingen met betrekking tot IPv6 bij hosting providers besproken, gevolgd door steekproef onder consumentenproducten.

5.1 World IPv6 Day

8 juni 2011 is door de internetgemeenschap uitgeroepen tot “World IPv6 Day”.[18] Deze dag wordt georganiseerd door de Internet Society (ISOC) en heeft als doel om 24 uur lang zoveel mogelijk content providers hun diensten dual-stack te laten leveren. Het gaat hierbij hoofdzakelijk om websites, zoals Google en Facebook, maar ook om Content Delivery Networks (CDN), zoals Akamai en Limelight Networks, die zorgen voor de wereldwijde verspreiding van content, bijvoorbeeld automatische software-updates. Iedere website kan aan deze dag meedoen.

De achterliggende gedachte van een gezamenlijke IPv6 testdag is dat partijen die terughoudend zijn om IPv6 aan te zetten op hun website, wel bereid zijn dit te doen als de grote websites dit ook doen. Deze terughoudendheid heeft onder andere te maken maken met de onbekendheid met IPv6, maar ook met een met een klein percentage eindgebruikers, dat door IPv6-fouten in computersoftware of internetverbinding een time-out op dual-stack websites ervaart. Het doel van World IPv6 Day is om enerzijds partijen de kans te bieden in het kielzog van andere partijen ervaring op te doen met IPv6 en anderzijds problemen met IPv6 in kaart te brengen, zodat deze daarna in producten verholpen kunnen worden.

Het overgrote deel van de consumenten zal op 8 juni niets merken. Echter een klein deel van de gebruikers – ongeveer 0,2%-0,3%[19] – zal op die dag niet alle websites kunnen bereiken. Dit ligt dan in de meeste gevallen niet aan de website, maar aan de software die de consument gebruikt. Op internet[20] kunnen gebruikers controleren of zij problemen kunnen verwachten op World IPv6 Day.

5.2 Hosting providers

In de tweede meting werden interviews en enquêtes gehouden onder ISP’s aan de accesskant en bedrijven en overheden als eindgebruikers. In deze meting is een enquête gehouden onder hosting providers om inzicht te krijgen in de status en

[18] http://isoc.org/wp/worldipv6day/
[19] Measuring and combating IPv6 brokenness, Tore Anderson @ RIPE61, November 2010, http://ripe61.ripe.net/presentations/162-ripe61.pdf
[20] http://test-ipv6.com/

knelpunten aan de aanbodzijde van internetdiensten, in het bijzonder websites. De resultaten hiervan worden in deze paragraaf beschreven.

5.2.1 Enquête

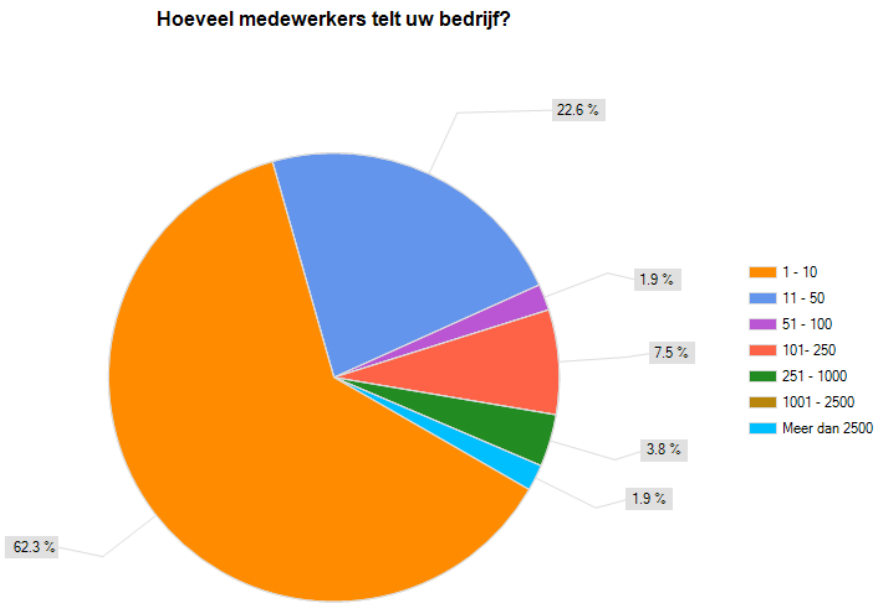
Voor een soepele introductie van IPv6 bij internet providers is het van belang dat voldoende content ook over IPv6 beschikbaar is. Websites vormen hierbij een grote component en Figuur 18 laat zien dat in maart 2011 13 van de 500 (2,6%) populairste websites in Nederland bereikbaar is over IPv6.

Websites kunnen door bedrijven zelf gehost worden of door een hosting provider. Deze enquête is uitgezet bij de laatste categorie. De enquête is onder andere verspreid onder de deelnemers van ISP Belang, ISP Connect en de Dutch Hosting Provider Association (DHPA). In totaal hebben 53 bedrijven de enquête ingevuld.

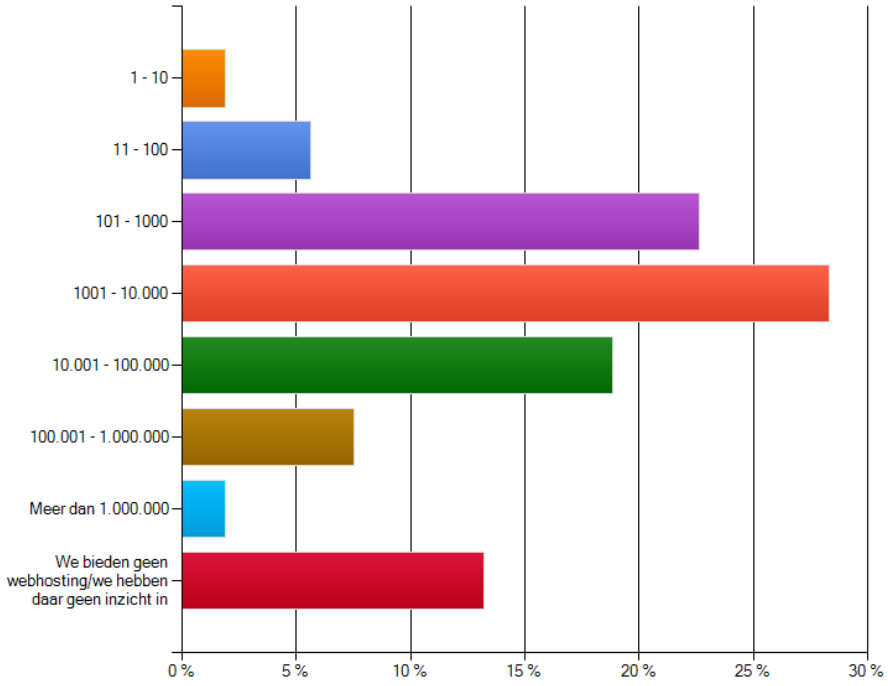
De vragen van de enquête zijn opgedeeld in de volgende categorieën:
1. Algemene bedrijfsgegevens
2. IPv6 plannen en activiteiten
3. Beweegredenen en knelpunten
4. Beveiliging

5.2.1.1 Algemene bedrijfsgegevens

De *algemene bedrijfsgegevens* geven inzicht in onder andere de omvang en diversiteit van de deelnemers. Figuur 19 toont het aantal medewerkers van de deelnemende bedrijven en Figuur 20 toont het aantal websites dat zij hosten. De grafieken laten zien dat hosting providers veelal kleine ondernemingen zijn, die relatief veel websites hosten.



Figuur 19: Aantal medewerkers van deelnemers aan de enquête

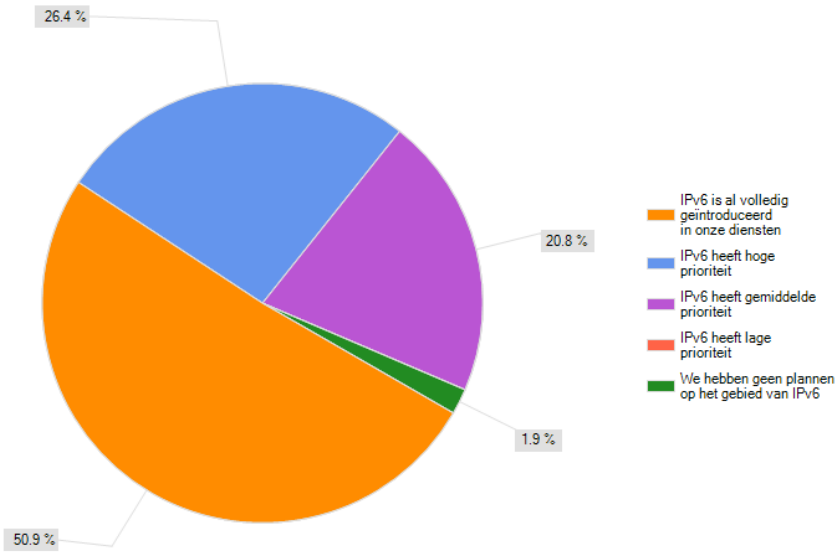


Figuur 20: Aantal websites dat door respondenten wordt gehost

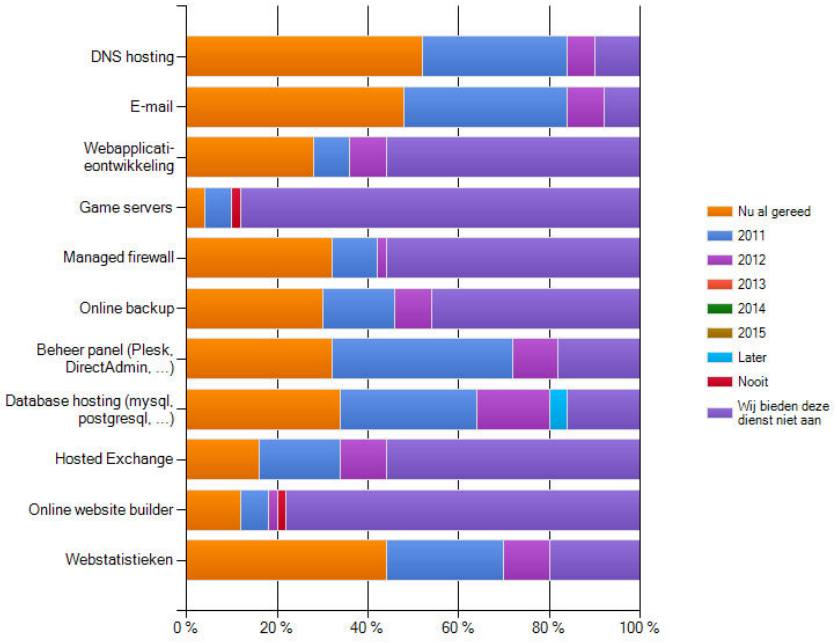
5.2.1.2 *IPv6 plannen en activiteiten*

Veel hosting providers antwoorden positief op de *IPv6 plannen en activiteiten*, die ze hebben. Figuur 21 toont de prioriteit die IPv6 heeft bij verschillende organisaties. Ongeveer de helft van de respondenten heeft IPv6 al geïntroduceerd in hun diensten en bij nog eens een kwart staat IPv6 hoog op de agenda. Bovendien geeft bijna 90% aan zelf of via een datacenter verbonden te zijn met internet via IPv6. Figuur 22 geeft in meer detail weer welke (deel)diensten al over IPv6 geleverd worden of wanneer de respondenten verwachten IPv6 in deze dienst te gaan leveren. Sommige diensten worden niet door alle partijen aangeboden. In Figuur 23 worden deze partijen niet meegenomen in het diagram. Uit deze diagrammen blijkt dat in de loop van 2011 meer dan 75% van de aangeboden diensten over IPv6 geleverd kunnen worden.

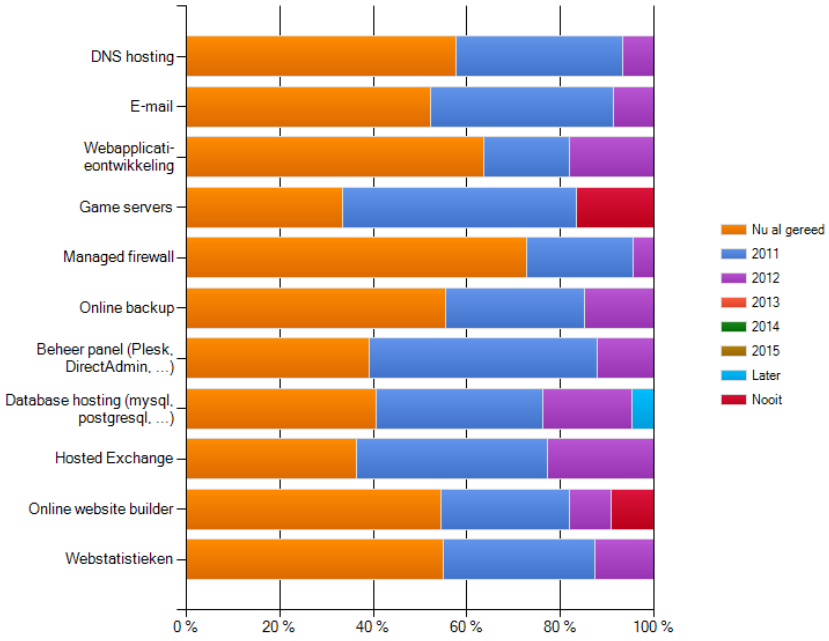
Aan het aantal IPv6 gebruikers en websites, zie Figuur 17 en Figuur 18, is te zien dat het percentage websites dat bereikbaar is over IPv6 vergelijkbaar is met het aantal gebruikers dat staat is IPv6 te gebruiken. Met 13 van de 500 websites (2,6%) scoort Nederland redelijk in vergelijking tot Europa, maar in vergelijking met de 50% van de deelnemende hosting providers die IPv6 in hun diensten aanbiedt lijkt dit tegen te vallen. Een mogelijke oorzaak hiervoor is dat veel websites in de Alexa Top 500 gehost worden door dat deel van hosting providers dat nog niet met IPv6 werkt. Een andere oorzaak is dat de website-eigenaars hun webpagina op eigen systemen hosten. Mogelijk kiest een deel van de website-eigenaren er ook expliciet voor om IPv6 nog niet aan te zetten. World IPv6 Day heeft als doel website-eigenaren over de streep te trekken om hun website dual-stack te gaan draaien.



Figuur 21: Staat IPv6 bij uw organisatie op de agenda?

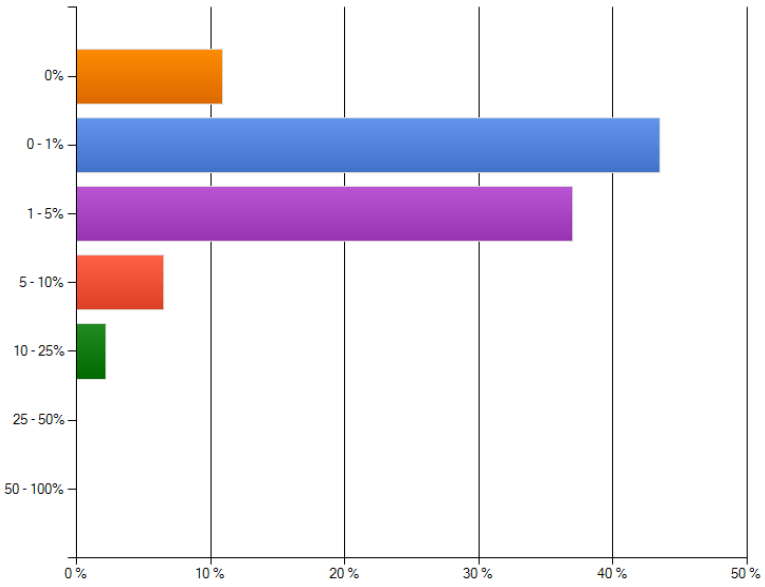


Figuur 22: IPv6 ondersteuning in (deel)diensten van hosting providers



Figuur 23 IPv6 ondersteuning in (deel)diensten van hosting providers, exclusief niet aanbiedende partijen

Met ongeveer 50% van de providers die IPv6 in hun diensten levert valt de hoeveel IPv6-verkeer naar hun diensten wat tegen. Dit is weergegeven in Figuur 24. Dit is te verklaren door de beperkte beschikbaarheid van IPv6 verbindingen voor internetgebruikers, zie Figuur 17.

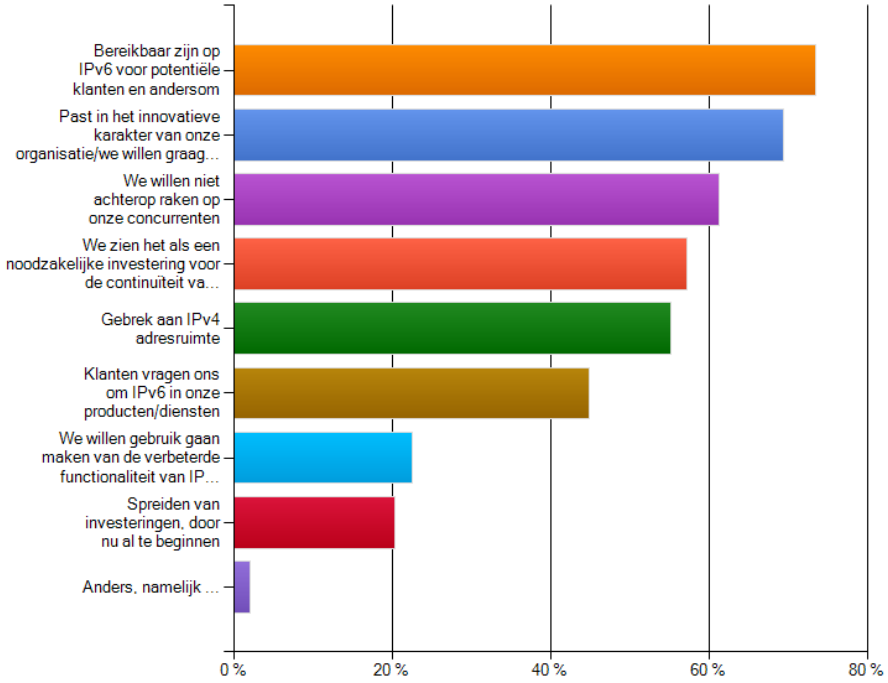


Figuur 24: Hoeveelheid verkeer naar diensten van hosting providers dat daadwerkelijk over IPv6 gaat.

Ook is de bedrijven gevraagd naar hun vraagprijs voor ondersteuning van IPv6 in diensten en geen enkele respondent geeft aan een meerprijs te vragen voor IPv6.

5.2.1.3 *Beweegredenen en knelpunten*

De redenen voor hosting providers om over te gaan naar IPv6 zijn weergegeven in Figuur 25. De belangrijkste redenen hebben voornamelijk te maken met het bereikbaar willen zijn voor gebruikers via IPv6. Hosting providers voorzien geen problemen met hun eigen IP adresvoorraad.



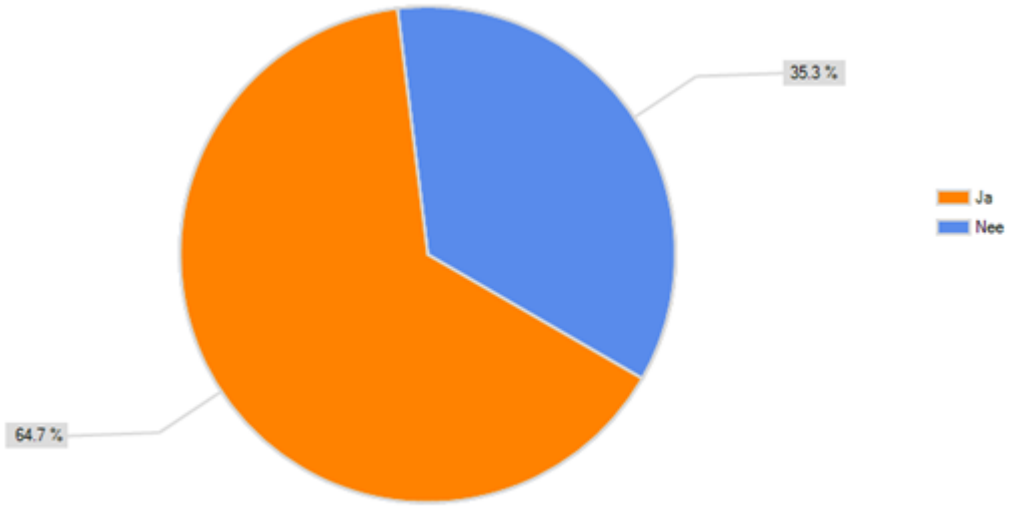
Figuur 25 Beweegredenen van hosting providers om IPv6 te introduceren

De belangrijkste knelpunten ervaart of verwacht men in de ondersteuning van IPv6 in software, zie Figuur 26. Zaken die hierbij genoemd worden zijn onder andere ondersteuning van IPv6 in MySQL, control panels, software die niet om kan gaan met de 128 bits van een IPv6 adres en in het algemeen softwareleveranciers die IPv6 niet in hun producten ondersteunen. Een overzicht van IPv6 ondersteuning in software wordt op verschillende plaatsen bijgehouden.[21,22,23]

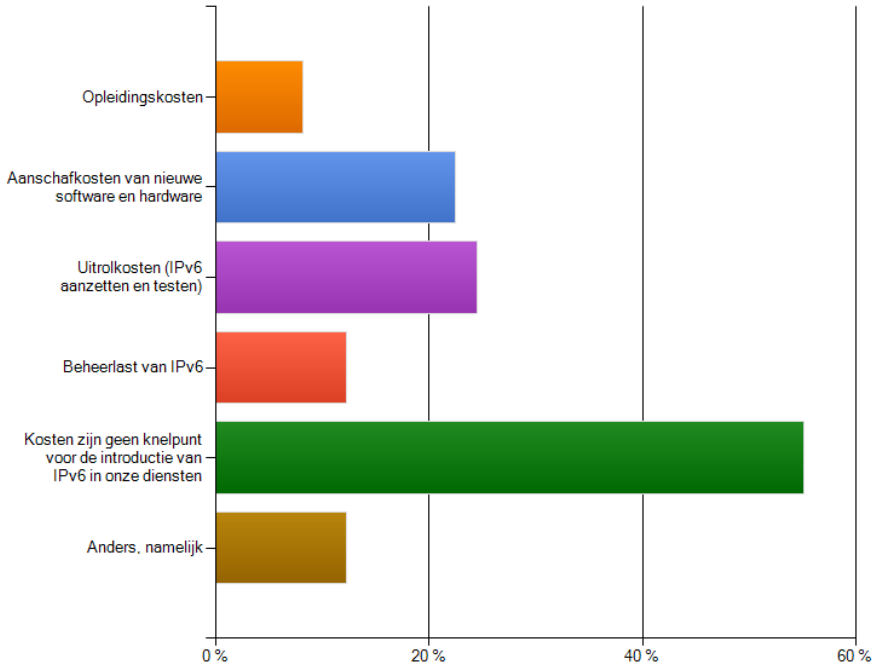
Over hardware zijn de respondenten iets positiever, maar ongeveer 36% ervaart of verwacht ook daar problemen. Hierbij wordt gerefereerd aan features die niet worden ondersteund en bugs in apparatuur.

Eén van de belemmeringen voor de introductie van IPv6, die door ISP's en andere bedrijven en overheden wordt genoemd in de tweede meting, zijn de benodigde investeringen. Bij de hosting providers geeft iets meer dan de helft van de respondenten aan dat kosten geen belemmering vormen. Dit is te verklaren door het feit dat de helft al IPv6 aanbiedt in hun diensten. Onder hosting providers die kosten wel als belemmering zien worden aanschaf- en uitrolkosten gezien als de grootste belemmering, zie Figuur 27.

[21] http://www.deepspace6.net/docs/ipv6_status_page_apps.html
[22] http://ipv6wiki.net/wiki/Portal:Software
[23] http://ip6.nl/software.txt



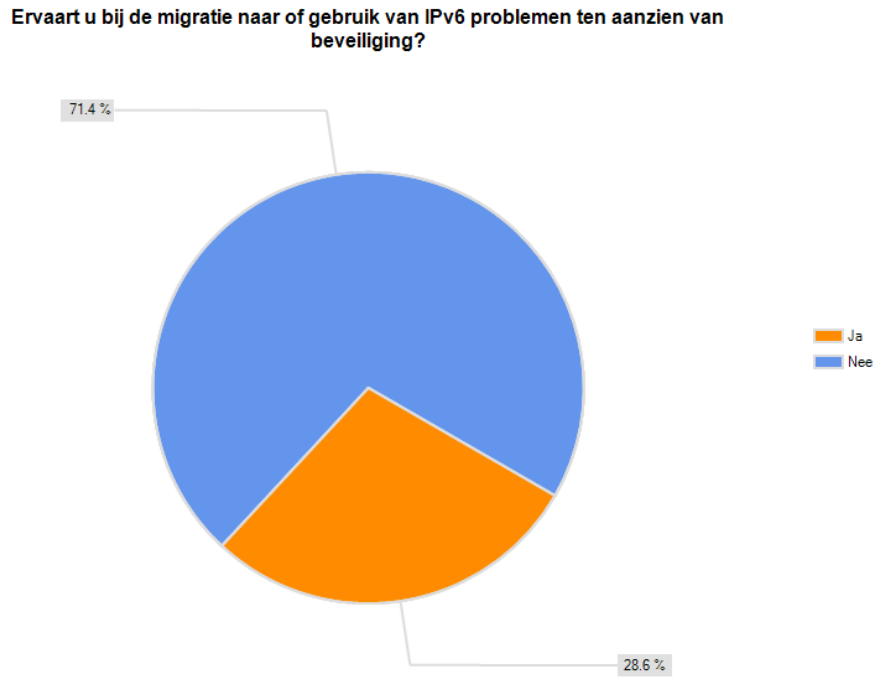
Figuur 26: Percentage hosting providers dat softwareproblemen met IPv6 verwacht of ervaart



Figuur 27: IPv6 gerelateerde kosten die het meeste belemmerend zijn.

5.2.1.4 Beveiliging

Als laatste is gevraagd naar problemen die men ervaart bij de beveiliging van IPv6, zie Figuur 28. Meer dan een kwart van de respondenten geeft aan problemen te ervaren bij de migratie naar of het gebruik van IPv6. In Hoofdstuk 6 zal specifieker worden ingegaan op beveiligingsknelpunten.



Figuur 28: IPv6 beveiliging bij hosting providers

5.2.2 Conclusies

De ondervraagde hosting providers zijn in meerderheid actief op het gebied van IPv6 en geven aan IPv6 in hun diensten te leveren of dit te kunnen leveren mocht dit noodzakelijk worden. Ook verwachten de meeste partijen technisch geen problemen, al zal in sommige gevallen voor een alternatieve oplossing worden gekozen, zoals het gebruiken van producten van een andere leverancier.

De belangrijkste reden voor hosting providers om IPv6 te ondersteunen is het bereikbaar willen blijven voor IPv6 gebruikers. Dit raakt direct aan de core-business van hosting bedrijven. De relatief grote IPv6 activiteit bij hosting providers ten opzichte van internet providers heeft waarschijnlijk ook met het verschil in omvang van de organisaties in beide bedrijfscategorieën te maken. Kleinere bedrijven zijn door hun omvang in staat sneller in te spelen op nieuwe technologieën. Daarnaast zijn de kosten van de introductie van IPv6 voor hosting providers beter beheersbaar dan bij internetproviders met honderdduizenden klanten met bijbehorende modems.

De grootste belemmering bij hosting providers die nog geen IPv6 aanbieden in hun diensten is het gebrek aan IPv6 aansluitingen bij consumenten. Zij zijn geneigd te wachten tot ISP's hun klanten op IPv6 aansluiten zodat er ook bezoekers via IPv6 op door hun gehoste websites kunnen komen.

5.3 Status IPv6 producten voor consumenten

In deze paragraaf wordt onder *IPv6 producten voor consumenten* die producten verstaan die consumenten zelf kunnen kopen ter inrichting van hun huisnetwerk. Hier valt dus niet de router, switch en IPTV ontvanger (Set-Top Box) onder die door de DSL, kabel of fiber leverancier wordt geleverd of gecertificeerd. In veel gevallen

neemt de consument deze apparatuur af bij de operator of wordt deze in bruikleen verstrekt.

In deze meting is een aantal winkels benaderd met de vraag of ze een home server (ook bekend onder namen als network attached storage (NAS), media server en streaming server) verkopen die IPv6 ondersteunt. Als consumenten straks hun internetverbinding over IPv6 geleverd krijgen is het wenselijk dat IPv6 ook daadwerkelijk gebruikt kan worden door apparatuur in het huisnetwerk, zoals media servers en tablets.

Paragraaf 5.3.1 en 5.3.2 geven een overzicht van een aantal steekproeven die uitgevoerd is. Hierbij is aan winkelpersoneel om advies gevraagd over de keuze voor een IPv6 product en wat IPv6 de consument kan bieden. De keuze van de winkels is in dit onderzoek gedaan op basis van wat in het straatbeeld aan computer- en elektronicawinkels voorhanden is. Deze winkels bedienen een groot deel van de Nederlandse bevolking.

Er is een lijst gemaakt met producten die in de winkels aangetroffen werden.
Per product is door middel van een bureaustudie en in sommige gevallen door navraag bij de fabrikant nagegaan of het IPv6 ondersteunt. In Paragraaf 5.3.3 wordt ingegaan op de ondersteuning van IPv6 in wireless access points.

5.3.1 IPv6 producten en kennis bij winkels

De steekproef is gehouden onder vijf verschillende winkels. Tabel 10 geeft per winkel de bevindingen aan. In enkele gevallen raadpleegden verkopers informatiebronnen of werd er onderling overlegd.

Winkel Nr.	Product aanwezig dat IPv6 ondersteunt	Verkoper kent IPv6 ondersteunende producten	Correct advies m.b.t. IPv6 ondersteuning	Kennis over IPv6	Opmerkingen
1	ja	ja	ja	--	Verkoper brengt IPv6 in verband met RAID (disk configratie)
2	nee	n.v.t.	ja	--	Verkoper vindt dat IPv6 sneller is dan IPv4
3	ja	ja	ja	+	Verkoper gaf aan dat IPv6 iets te maken heeft met het opraken van IPv4 adressen
4	ja	nee	nee	--	Volgens verkoper zouden alle producten IPv6 ondersteunen
5	nee	n.v.t.	ja	--	Verkoper gelooft dat residential gateway translatie van IPv4 naar IPv6 zal verzorgen voor alle applicaties

Tabel 10: IPv6 producten en kennis bij winkels. Er is gevraagd naar de nu populaire home server (ook bekend als NAS, media server, streaming server).

In drie van de vijf winkels is een IPv6-ready product beschikbaar. Paragraaf 5.3.2 laat zien dat het hier om slechts één product gaat. Opvallend is ook dat het voorkomt dat een verkoper alle producten als IPv6-ready bestempeld.
De kennis van verkopers bleek in deze steekproef onvoldoende. In een enkel geval wist men het verband te leggen tussen het opraken van IPv4 adressen. 4 van de 5 gevallen werd er onjuiste informatie verstrekt.

5.3.2 IPv6 ondersteuning in home servers.

Tabel 11 geeft een overzicht van 11 producten die in de vijf winkels uit de steekproef van paragraaf 5.3.1 zijn gevonden. Het gaat hierbij om home servers (ook bekend als NAS, media server, streaming server) die veel media gerelateerde features bevatten. Naast standaard opslag functionaliteiten bieden zij ook de

mogelijkheid bijv. een peer-2-peer file sharing client, webserver of streamer te draaien.
De 11 producten die opgenomen zijn in de tabel zijn niet noodzakelijk van verschillende fabrikanten, echter als dit wel het geval is dan is de productlijn wel verschillend. Met een aantal fabrikanten is er contact geweest over de huidige en toekomstige ondersteuning van IPv6.

Product #	IPv6 ondersteuning	Opmerkingen
1	ja	- Ook op management Interface - IPv6 gebruikt als verkoop argument
2	nee	Fabrikant: geen plannen
3	nee	Fabrikant: misschien dit jaar nog, geen garantie
4	nee	Fabrikant: Niet duidelijk aan welke features voldaan moet worden. Voorlopig dus niet
5	nee	
6	nee	
7	nee	
8	nee	
9	nee	
10	ja	IPv6 gaat met firmware update mee
11	nee	

Tabel 11: 11 producten (populaire home server, ook bekend als NAS, media server, streaming server) getoetst op IPv6. Product 1 en 10 zijn van dezelfde fabrikant, echter van verschillende productlijn.

5.3.3 IPv6 ondersteuning in wireless access points

Gedurende het bezoek aan deze vijf winkels werd tevens gekeken naar IPv6 ondersteuning in WiFi 802.11n draadloze switch. Hoewel een WiFi switch in principe voor zijn basis functionaliteit IP transparant dient te zijn, worden deze netwerkelementen vaak wel uitgerust met additionele functionaliteiten die IP gerelateerd zijn.

Van de 17 verschillende draadloze switches die in deze winkels werden gevonden bleek slechts één fabrikant IPv6 te ondersteunen ten behoeve van deze additionele functionaliteiten. Ook gaf deze fabrikant dit zeer duidelijk aan op de verpakking en in de handleiding wordt veel informatie over IPv6 gegeven.

5.3.4 Conclusies

Kennis bij winkels omtrent het nut van IPv6 en de daadwerkelijke ondersteuning van IPv6 is in zeer beperkte mate aanwezig. In sommige gevallen leidt dit ook tot een verkeerd verkoopadvies. Ook de productdiversiteit is erg laag. Juist voor producten die gekocht worden om jaren mee te gaan en die vanwege hun prijs niet snel aan de kant gezet worden is het belangrijk dat IPv6 ondersteund wordt. Om te voorkomen dat consumenten producten kopen die geen IPv6 ondersteunen, terwijl dit wel voordelen kan hebben, is het van belang dat fabrikanten van consumenten producten meer aandacht hebben voor IPv6.

De reactie van fabrikanten met betrekking tot het op de roadmap zetten van IPv6 geeft aan dat hier nog geen sprake is van enige urgentie. Bij de producten waarin wel IPv6 ondersteund wordt, gebruikt de fabrikant dit als verkoopargument. In de vierde meting zal het aantal winkels en de diversiteit aan producten uitgebreid worden.

6 Monitoring van security/veiligheidsincidenten

6.1 Inleiding

Een belangrijk aspect bij de introductie van nieuwe technologie is beveiliging. Dit is een voorwaarde om kwalitatief hoogwaardige dienstverlening te kunnen bieden. Zodoende speelt beveiliging ook bij de introductie van IPv6 een belangrijke rol.

De introductie van IPv6 zou in principe geen (nadelige) veranderingen op de beveiliging tot gevolg mogen hebben. Er zijn echter verschillende aspecten die hier een rol spelen. Deze zijn samen te vatten in een tweetal aspecten:

a) vernieuwingen binnen het protocol IPv6 of de toepassing ervan die van invloed zijn op het beveiligingsniveau van de geboden diensten
b) het beveiligingsniveau van de functionaliteiten of diensten die IPv6 ondersteuning bieden of zouden moeten bieden moet minimaal gelijk zijn aan hun IPv4 tegenhangers

In beide gevallen kunnen deze invloeden ten gunste of ten nadele zijn ten opzicht van de huidige situatie met IPv4.

In de vorige meting is een eerste quickscan gedaan op basis van de bestaande kwetsbaarheden. Op basis daarvan is er geconcludeerd dat er nog weinig kwetsbaarheden zijn. Wel is destijds waargenomen dat ISP's wel beperkingen zien, onder andere op het gebied van beschikbaarheid van functionaliteit, en extra kwetsbaarheden. In deze meting is diepgaander onderzocht welke beveiligingsaspecten een rol spelen bij IPv6 en de acceptatie van IPv6. In dit kader zijn aan de hand van desk research, een enquête en een aantal interviews de stand van zaken en opgedane ervaringen op het vlak van beveiliging van IPv6 in kaart gebracht. Hierbij is gesproken met verschillende partijen, waaronder zakelijke en consumenten ISPs, content leveranciers en hosting providers.

6.2 Bevindingen

Deze sectie beschrijft de opgedane bevindingen. Uit eerdere metingen blijkt dat het gebruik van IPv6 nog erg beperkt is, in veel gevallen is het daarbij nog steeds experimenteel. Dat geldt des temeer voor nieuwe functionaliteit binnen IPv6 zoals mobile IP.

In die zin valt het te verwachten dat er nog veel onbekende kwetsbaarheden in IPv6 en toepassingen daarvan bestaan die via nieuwe, nu nog onbekende, aanvallen en technieken uitgebuit zullen worden. Met IPv4 is er meer dan 20 jaar praktijkervaring en zijn er vele kwetsbaarheden inmiddels bekend en vaak opgelost (bijv. land attack, teardrop attack) bij IPv6 moet dit nog blijken.

6.2.1 Gebrek aan kennis en ervaring

Een belangrijk aspect is dat de kennis van IPv6 bij veel partijen nog beperkt is. Dit komt voor bij alle typen partijen die een rol spelen, waaronder eindgebruikers, dienstleveranciers en systeemleveranciers. Dit kan op allerlei vlakken tot problemen leiden, waaronder het niet aanpassen van "default" instellingen van producten, waardoor ze eenvoudig toegankelijk kunnen zijn voor niet-geautoriseerden. Gebrek aan kennis vormt ook een grote rol bij de applicatieontwikkelaars die niet altijd

voldoende rekening houden met IPv6. Er zijn namelijk niet uitsluitend aanpassingen aan de communicatie nodig, maar ook allerlei andere onderdelen, waaronder configuratie en administratie moet worden aangepast.

Daarnaast geldt dat in IPv6 zaken toch vaak net anders geregeld zijn, hoewel het functioneel sterk overeenkomt met IPv4. Hierbij valt te denken aan het gebruik van Neigbour Discovery ten opzichte van ARP. Dit heeft ook zijn weerslag op bijvoorbeeld policies van beveiligingscomponenten die niet-triviaal zullen afwijken van de policies voor IPv4 verkeer. Ook zijn er nieuwe functionaliteiten die opgenomen moeten worden in de policies. Een belangrijk voorbeeld hiervan zijn de zogenaamde extension headers die gebruikt kunnen worden om de basisfunctionaliteit van IPv6 te kunnen uitbreiden. Dit is geheel nieuw ten opzichte van IPv4 en het is onduidelijk hoe dit zijn weerslag zal vinden in de implementatie van policies in IPv6. Daarnaast geldt ook dat bijvoorbeeld de rol van ICMP anders is geworden. Bij IPv4 is het tamelijk gangbaar dit standaard te blokkeren, bij IPv6 is het gebruik van ICMP noodzakelijk hetgeen zijn weerslag zal hebben op de firewall policies. Ook zullen bepaalde zaken niet meer mogelijk zijn, bijvoorbeeld het scannen van een IP range door de gebruikte lengte van de IPv6 adressen.

Daar staat tegen over dat IPv6 nog weinig gebruikt wordt voor aanvallen, doordat het algemeen gebruik van IPv6 nog heel beperkt is. Hierdoor is er weinig drang om gericht op grote schaal naar beveiligingsproblemen te zoeken in IPv6 en IPv6 implementaties. Het ligt dan ook in de lijn der verwachtingen dat pas bij een veel grotere gebruikersgroep een groot aantal beveiligingsproblemen naar voren zal komen. Qua functionaliteit van IPv6 zijn er wel een aantal beveiligingsproblemen bekend inmiddels, zoals DoS aanvallen op basis van duplicate address detection of het “spoofen” van router advertisements. Echter de meeste problemen zullen veel meer te maken hebben met de implementatieaspecten van IPv6.

Ook bij de partijen die inmiddels wel IPv6 gebruiken of als dienst aanbieden wordt beveiliging nog niet als een groot obstakel ervaren. Dit is waarschijnlijk ook een direct gevolg van het feit dat het gebruik nog beperkt is en daarmee eveneens de risico’s. Daarnaast is er vooral een focus die ligt op het realiseren van de functionaliteit waarbij zich vooralsnog voldoende andere problemen voordoen.

6.2.2 Automatische tunneling IPv6

Het gebruik van automatische tunneling (zoals Teredo) kan grote consequenties hebben voor de beveiliging. Ten eerste zijn vele gebruikers niet op de hoogte dat dit standaard aan staat (bijvoorbeeld bij Windows 7) waardoor er ongemerkt IPv6 verbindingen opgezet worden die dan vaak niet via de gewenste beveiligingsproducten lopen. Dit kan zowel voor de eindgebruikers als de netwerkbeheerders problemen opleveren. In Figuur 13 is te zien dat Windows 7 door meer dan 34% van de Nederlandse internetgebruikers wordt gedraaid. Daarnaast kan het ook de gebruikerservaring benadelen omdat tunneling vaak veel minder efficiënte verbindingen oplevert en in sommige gevallen helemaal niet goed werkt. Ook voor illegale toepassingen kan automatische tunnels interessant zijn, waarbij bijvoorbeeld een botnet op basis van IPv6 wordt gebruikt via een automatische tunneling. Hierdoor kan detectie ervan veel moeilijker worden.

6.2.3 Gebrek aan ondersteuning voor IPv6

Niet alle componenten ondersteunen IPv6 nog in voldoende mate. Dit geldt zowel voor de IPv6 functionaliteiten die ondersteund worden in de apparatuur als de pure beschikbaarheid van IPv6 apparatuur. Dat geldt ook voor beveiligingscomponenten. Voornamelijk op het gebied van detectie en analyse middelen, zoals IDS/IPS, spamfilters, virusscanners en dergelijke is de ondersteuning tamelijk beperkt. Door de beperkte vraag naar deze middelen is er weinig animo om de ontwikkeling te starten.

IPv6 kent ook een groot aantal aspecten die gunstig zijn voor de beveiliging, maar die nog maar beperkt geïmplementeerd zijn. Dit gaat bijvoorbeeld om authenticatiemiddelen voor adrestoekenning (SEND, CGA).

6.2.4 Transparantie (NAT)

Binnen IPv4 wordt NAT (Netwok Address Translation) vaak ingezet als beveiligingstechnologie, met name in de consumentenmarkt. Hoewel de kwaliteit van NAT als beveiligingstechnologie op zijn zachtst gezegd discutabel is, is het ontbreken van NAT in IPv6 een belangrijk knelpunt omdat:

a) de beveiliging anders moet worden ingericht,
b) er andere technologieën moeten worden toegepast.

Bovenstaande heeft als consequenties dat extra investeringen in de ontwikkeling van dergelijke producten vereist zijn en dat er andere rulesets gehanteerd moeten worden. In het hogere segment speelt dit een minder grote rol omdat NAT daar minder wordt ingezet als beveiliging en omdat de marges groter zijn.

Een consequentie van het verdwijnen van NAT is dat een aantal diensten eenvoudiger te realiseren wordt, bijvoorbeeld VoIP. De toepassing van echte firewalls, in tegenstelling tot het gebruik van NAT, kan hier tot een beter beveiligingsniveau leiden. Tevens is gebleken dat regels in bijvoorbeeld firewalls bij IPv6 compacter en daarmee beter beheersbaar kunnen zijn. Bij IPv4 vindt er vaak versnippering plaats van IP ranges (veel kleine, niet opeenvolgende reeksen) waardoor deze ranges ook in de regels terugkomen. Bij IPv6 zijn vooralsnog de reeksen voornamelijk aaneensluitend.

NAT wordt ook vaak aangegeven als mogelijke oplossing van de beperkte adresruimte van IPv4 als alternatief voor IPv6. Zaken als large scale NAT zullen ook zeker toegepast gaan worden wanneer de IPv4 adressen niet meer in voldoende mate beschikbaar zijn en IPv6 nog niet toegepast kan worden. Dit heeft echter wel consequenties voor de traceerbaarheid van gebruikers. Doordat NAT toegepast wordt, wordt het zelfde IPv4 adres gebruikt door meerdere personen tegelijk. In het geval van incidenten is het dan bijzonder ingewikkeld om te achterhalen welke persoon daarvoor verantwoordelijk is. Ook in het kader van een taplast en dataretentie is het veel moeilijker om vast te stellen welke persoon het betreft.

6.2.5 Privacy extentions

IPv6 introduceert een nieuwe functionaliteit onder de noemer privacy extentions. Hierbij wordt een client periodiek voorzien van een nieuw IPv6 adres zodat deze moeilijker is te traceren. Deze functionaliteit, bedoeld ter bescherming van gebruikers, heeft echter ook een keerzijde. Zo kan dit bemoeilijkend werken voor het opstellen van regels voor beveiligingstoepassingen zoals firewalls. Daarnaast

wordt het lastiger om een gebruiker te traceren op basis van een IP adres. Voor zowel bedrijfsnetwerken alwaar de gebruiker deel vanuit maakt, als voor bijvoorbeeld opsporingsdoeleinden kan dit onderzoek naar incidenten bemoeilijken.

IPv6 implementaties gebruiken voor het genereren van een IPv6 adres vaak de standaard EUI-64 hetgeen is gebaseerd op het MAC adres van de netwerk interface kaart. Dit zal nagenoeg uniek zijn met als gevolg dat gebruikers eenvoudig te volgen zijn van het ene netwerk naar het andere aangezien steeds dezelfde 64 bits voor het laatste gedeelte van het IP adres worden gebruikt. Dit kan nadelig zijn in het kader van privacy. Het is echter niet verplicht om deze richtlijn te volgen, bijvoorbeeld door de privacy extensions toe te passen.

6.2.6 Transitie

De transitie van IPv4 naar IPv6 zal een zeer lange periode bestrijken. Dat wil zeggen dat de meeste infrastructuren de komende jaren nog IPv4 zullen ondersteunen naast de groeiende ondersteuning van IPv6. Bepaalde legacy systemen zullen wellicht nog meer dan tien of zelfs twintig jaar in gebruik blijven. Gedurende de tijd dat de twee systemen min of meer volwaardig naast elkaar zullen bestaan, betekent dit ook dat de netwerk- en applicatiebeheerders beide op gelijkwaardig niveau moeten beveiligen. Dit geeft een potentiële aanvaller, dus ook twee mogelijke aanvalsvectoren waaruit hij kan kiezen waarbij hij dus altijd de zwakste zal kiezen. In de tweede meting is al gebleken dat dit risico ervaren wordt als een belangrijke bottleneck door ISP's voor de invoering van IPv6.

6.3 Conclusies

Beveiliging van IPv6 staat vooralsnog veelal in de kinderschoenen. In het algemeen is het kennisniveau van IPv6 beveiliging nog beperkt bij vele partijen. Daarentegen geldt wel dat door het beperkte gebruik, IPv6 op dit moment weinig interessant is om misbruik van te maken. Het valt dus ook te verwachten dat het aantal beveiligingsincidenten en kwetsbaarheden die te maken hebben met IPv6 gestaag zullen toenemen, vooral op het moment dat IPv6 meer wordt gebruikt. Van belang is juist nu al voldoende aandacht te besteden aan de "awareness" van IPv6 beveiliging ook als er nog geen gebruik van gemaakt wordt van IPv6. Daarbij geldt ook dat IPv6 op een aantal aspecten toch op cruciale wijze afwijkt van IPv4 waardoor zaken anders geregeld moeten worden.

Het alternatief voor IPv6 - large-scale NAT - levert ook beveiligingsproblemen op, zeker wanneer er meerdere niveaus van NAT worden toegepast. Het is hierdoor veel moeilijker om vast te stellen wie gebruik maakt van een specifiek IP adres, waardoor het analyseren en beperken van de gevolgen van incidenten moeilijker wordt. Daarnaast is het in het kader van wetgeving zoals dataretentie en de tapverplichting vele malen moeilijker om een IP adres te herleiden tot een persoon.

Nu de introductie van IPv6 langzaamaan op gang komt er in de meeste gevallen nog sprake is van een terugval mogelijkheid naar IPv4. Dat wil zeggen indien er problemen zijn met de verbindingen of toepassingen op basis van IPv6 kan er veelal worden teruggevallen tot het gebruik van IPv4. Echter, naarmate de afhankelijkheid en het gebruik van IPv6 toeneemt, zal ook deze terugvalmogelijkheid beperkter worden. Dit betekent dat wanneer de problemen rond IPv6 niet worden opgelost dit ten koste gaat van de beveiliging.

Gebleken is dat op dit moment beveiliging bij IPv6 nog niet een reëel obstakel wordt ervaren. Dit is mede ingegeven door het beperkte gebruik en de daarmee samenhangende risico's. Daarnaast geldt dat er andere obstakels zijn omtrent de transitie naar IPv6 die een hogere prioriteit hebben. In de toekomst is echter wel te verwachten dat IPv6 beveiliging een belangrijkere rol zal spelen, wanneer afhankelijkheid ervan toeneemt.

7 Conclusies

Op 3 februari heeft IANA de laatste IPv4 adressen verdeeld onder de RIR's. Uit Figuur 5 blijkt dat dit moment uiteindelijk veel sneller dichterbij gekomen is, dan een halfjaar geleden werd voorspeld. De meeste RIR's zullen doorgaan met het huidige beleid omtrent adresuitgifte, totdat hun voorraad is geslonken tot één /8 adresblok. Op dat moment vindt er een aanpassing in het uitgiftebeleid plaats. Enkele RIR's laten dit beleid pas op een later moment ingaan.

APNIC is de eerste RIR die de grens van één /8 heeft bereikt op 15 april 2011, waardoor huidige LIR's nog maar eenmalig een adresblok ter grootte van een /22 kunnen aanvragen. Op deze manier blijft het mogelijk voor nieuwe en opkomende netwerken om in de toekomst een kleine hoeveelheid IPv4 adressen te bemachtigen. RIPE zal waarschijnlijk nog voor het einde van 2011 door haar IPv4 adresvoorraad zijn. Ook dit uitputtingsmoment kan sneller komen dan verwacht, door een nog steeds groeiende hoeveelheid IPv4 adresaanvragen en een 'run' op de laatste IP adressen zoals waargenomen bij APNIC.

De stijging in het aantal IPv6 aanvragen zet door en is vorig jaar verdubbeld ten opzichte van 2009. Er is duidelijk sprake van een groeiend bewustzijn. Ook in Nederland groeit het aantal IPv6 aanvragen jaarlijks. Het daadwerkelijke gebruik van IPv6 is echter nog maar gering en niet wezenlijk veranderd ten opzichte van de vorige metingen. Zowel het aantal eindgebruikers als het aantal websites dat IPv6 ondersteunt, is nog maar enkele procenten. Ook op het gebied van aansluitingen is er nauwelijks verandering te merken.

In de nulmeting werden twee punten van zorg genoemd voor de uitrol van IPv6, namelijk de beschikbaarheid van IPv6 verbindingen voor eindgebruikers en de beschikbaarheid van content op en diensten over IPv6. In de tweede meting is onderzoek gedaan onder ISP's en mobiele operators ten behoeve van het eerste punt. In deze derde meting is een enquête uitgezet onder hosting providers ten behoeve van het tweede punt.

In dit onderzoek geeft ruim de helft van de hosting partijen aan dat IPv6 al volledig geïntroduceerd is in hun diensten. Nog een kwart geeft aan dat dit in de loop van 2011 het geval zal zijn. Alle partijen geven hierbij aan geen meerprijs te vragen voor IPv6. De belangrijkste beweegredenen hebben voornamelijk te maken met het bereikbaar willen zijn voor eindgebruikers via IPv6. Hosting providers zullen zelf niet direct problemen ervaren met hun IPv4 adresvoorraad.

Bijna 65% van de hosting partijen verwachten of ervaren problemen bij de ondersteuning van IPv6 in software. Dit kan een belemmering zijn voor het tijdig introduceren van IPv6 in diensten die nog niet gereed zijn. Daarnaast wordt het gebrek aan IPv6 aansluitingen bij consumenten genoemd als een belangrijke reden om te wachten. Om website-eigenaren over de drempel te trekken wordt op 8 juni 2011 World IPv6 Day georganiseerd. Dit gezamenlijke collectief biedt partijen de kans om ervaring met IPv6 op te doen en mogelijke problemen op te lossen.

Ook is er gekeken naar de IPv6 ondersteuning in consumentenproducten. Veelal is er geen ondersteuning in producten en is kennis bij winkels in beperkte mate

aanwezig. Fabrikanten geven aan dat er nog geen sprake is van urgentie. Bij enkele producten waarin wel IPv6 ondersteund wordt, gebruikt de fabrikant dit als verkoopargument.

Op het gebied van beveiliging staat IPv6 nog in de kinderschoenen. Er is nog maar beperkt gebruik van IPv6 waardoor er weinig beveiligingsincidenten plaatsvinden, zoals eerder bleek uit de tweede meting. De verwachting is dat als het gebruik toeneemt, het aantal kwetsbaarheden ook toe zal nemen. Op dit moment wordt beveiliging daarom nog niet als een reëel obstakel ervaren.

Het is van belang nu al voldoende aandacht te besteden aan de ‘awareness’ van IPv6 beveiliging, ook al wordt er nog weinig gebruik van gemaakt. Onbekendheid met IPv6 biedt ruimte voor beveiligingsincidenten. Het alternatief voor IPv6, large scale NAT, levert ook beveiligingsproblemen op en heeft gevolgen voor de traceerbaarheid van gebruikers, doordat eenzelfde IPv4 adres met meerdere gebruikers gedeeld wordt.