Haalbaarheid Implementatie IPv6 bij NPO

Bart Roos en Marco Wessel
{broos, mwessel}@os3.nl

4 februari 2008

Universiteit van Amsterdam

Samenvatting

Dit rapport richt zich op aandachtspunten, obstakels en kosten waar een organisatie zoals NPO mee te maken krijgt bij het implementeren van het nieuwe Internetprotocol IPv6. Er wordt gekeken naar de stappen die nodig zijn om adresruimte te verkrijgen, het geschikt maken van het netwerk en vervolgens het geschikt maken van de diensten die op het netwerk aangeboden worden aan eindgebruikers op het Internet. We werpen voornamelijk een algemene blik op het onderwerp en behandelen NPO als praktijkcasus.

Inhoudsopgave

Inleiding

In het begin van de jaren '90 werd duidelijk dat er een probleem zou onstaan met de uitgifte van IP-adressen van het gebruikte IPv4-protocol op Internet en dat Classless Inter-Domain Routing (CIDR) niet voldoende zou zijn om dat probleem op te lossen. Een opvolger werd gedefinieerd: IPv6. Dit nieuwe protocol bevat een aantal verbeteringen ten opzichte van IPv4, waarvan de meest opvallende is dat het een grotere adresruimte kent: maarliefst 2^{128} IP-adressen kunnen gebruikt worden, versus 2^{32} in IPv4. IPv6 wordt op dit moment nog niet wijdverspreid gebruikt, maar wordt geleidelijk aan populairder.

Wij zullen onderzoeken in hoeverre het haalbaar is voor een organisatie met een uitgebreid netwerk en dienstenportfolio om IPv6 te implementeren in de netwerkcore en het diensten via IPv6 op het Internet aan te bieden.

Opdracht

2.1 Opdrachtgever

Deze opdracht wordt uitgevoerd voor NPO: de Nederlandse Publieke Omroep. NPO is net als NOS-RTV onderdeel van de Nederlandse Omroep Stichting (NOS). NOS-RTV is de organisatie die programmering zoals het journaal verzorgt.

2.2 NPO-ICT

Een van de activiteiten van NPO is het leveren van ICT-diensten aan omroepen in het publieke bestel. Dat begon met een enkele medewerker die een paar sites op internet beschikbaar maakte en is uitgegroeid tot een volwaardige afdeling met de verantwoordelijkheid voor het beheer van meer dan 250 servers, aangesloten in een netwerk dat zelfs midden in de nacht meer dan een gigabit per seconde aan data het internet opstuurt.

2.3 Achtergrond

NPO is een organisatie die in veel opzichten vooruitstrevend wil zijn. Zo ook in technisch opzicht. Doordat NPO een publieke organisatie is zonder winstoogmerk kan zij een voortrekkersrol spelen in de acceptatie van nieuwe technologieën. Een van die technologieën is de nieuwe versie van het Internet Protocol: IPv6. NPO heeft ons gevraagd te onderzoeken of het haalbaar is voor hen om op korte termijn IPv6 te implementeren in hun netwerk. Hiervoor wil men weten welke stappen ondernomen moeten worden en wat de kosten hiervan zijn.

2.4 Vraagstelling

Kort samengevat is de kernvraag: wat is er nodig om een IPv4 netwerk geschikt te maken om via IPv6 diensten aan te bieden aan eindgebruikers op het internet. Het netwerk van NPO is veelomvattend: het is de aansluiting voor streaming- en webdiensten zoals `www.uitzendinggemist.nl`, maar ook voor de kantoorautomatisering van alle omroepen op het Hilversumse Mediapark en zelfs voor gebruikers op locatie zoals het Glazen Huis van de 3FM Serious Request actie.

Om die reden is gekozen om niet het gehele netwerk te beschouwen, maar slechts

onderzoek te verrichten naar het implementeren van IPv6 op plaatsen waar dat nodig is om diensten aan te bieden aan gebruikers op internet. In het bijzonder gaat het daarbij om websites en mediastreams.

2.5 Aanpak

Bij het implementeren van IPv6 in een netwerk onderscheiden we drie fasen die op volgorde uitgevoerd moeten worden.

2.5.1 Adresruimte

Door het in beschouwing nemen van de grootte en indeling van de huidige NPO IPv4-adresruimte, moet duidelijk worden op welke manier dit zich verhoudt in een IPv6-adresruimte. Hierna is het mogelijk vast te stellen welke adresruimte gewenst is, en hoe deze het beste te verdelen is in subnetten.

Ook is het noodzakelijk te bestuderen wat de mogelijkheden zijn om het gewenste subnet op een zoveel mogelijk provideronafhankelijke wijze te verkrijgen. Hierbij is het ook belangrijk om de richtlijnen van RIPE voor het uitgeven van IPv6 adresruimte in beschouwing te nemen. Het resultaat van deze fase is een advies voor het aanvragen van een IPv6 adresruimte en een overzicht van de directe kosten die dit met zich meebrengt.

2.5.2 Core

Een eerste stap voor het gereed maken van IPv6 in de netwerk core laag is het in kaart brengen van de netwerkinfrastructuur. Daarna kan de IPv6 ondersteuning van de gebruikte apparatuur in kaart gebracht worden.

Het resultaat van deze fase is een advies dat bestaat uit een duidelijk plan voor het IPv6-gereed maken van de core laag van het NPO-netwerk.

2.5.3 IPv6 diensten

Het aanbieden van diensten op het IPv6 platform is de stap die de daadwerkelijke IPv6 voortrekkersrol die NPO in gedachten heeft kan realiseren. Een eerste stap is het in kaart brengen van de verschillende diensten, en de hiervoor gebruikte apparatuur en software, die door NPO worden aangeboden.

Daarna wordt onderzocht voor welke van deze diensten het haalbaar is om deze als eerste via IPv6 aan te bieden. Hierbij zal worden bestudeerd in hoeverre de gebruikte platformen en software gereed zijn voor IPv6, en in welke vorm deze diensten het beste via IPv6 aangeboden kunnen worden.

Het resultaat van deze fase is een advies waarin is beschreven hoe een aantal publieke diensten op IPv6 aangeboden kunnen worden. Hierbij worden alle belangrijke aandachtspunten in beschouwing genomen.

2.6 Eindresultaat

Het rapport dat voor u ligt is het eindresultaat van het project en dient voor NPO als handvat voor het invoeren van IPv6. De stappen die nodig zijn voor het aanvragen van IPv6 adresruimte, het gereed maken van de netwerkcore, en een plan voor het aanbieden van een aantal internetdiensten via IPv6 worden hierbij beschreven.

Naast een praktisch rapport voor NPO is dit rapport ook opgesteld voor organisaties zoals content providers met een vergelijkbare netwerkinfrastructuur, die eveneens het plan hebben om IPv6 te implementeren.

IPv6 introductie

Om een indruk te geven hoe IPv6 tot stand is gekomen en welke voordelen IPv6 biedt ten opzichte van zijn voorganger volgt een korte introductie van het protocol.

3.1 Wat is IPv6

IPv6 is de nieuwe versie van het Internet Protocol, gedefinieerd in RFC2460 [12], en de opvolger van IPv4 (RFC 791 [38]). IPv6 is het resultaat van het IPng (IP next generation) project, gestart begin jaren '90 door het Internet Engineering Taskforce (IETF) om een opvolger van IPv4 te kiezen[3]. Een opvolger voor IPv4 was nodig omdat men zich realiseerde dat het aantal beschikbare IPv4 adressen op ten duur niet voldoende zou zijn om alle systemen op het groeiende Internet van een adres te voorzien.

Veel netwerkhardware en software is inmiddels voorzien van IPv6 ondersteuning. Technisch gezien lijkt niets de ingebruikname van IPv6 in de weg te staan. Een reden waarom IPv6 nog niet op grote schaal in gebruik genomen is kan gezocht worden in het ontbreken van een goede *business case* voor commerciële partijen.

3.2 Vebeteringen in IPv6

De meeste recente IPv6 RFC, 2460[12], geeft een goed overzicht van de verbeteringen ten opzichte van IPv4. We staan kort stil bij de meest opvallende veranderingen.

3.2.1 Adresruimte

Een van de meest belangrijke verbeteringen ten opzichte van IPv4 is de grotere adresruimte die IPv6 biedt. Deze is vergroot van een 32 bits adres naar een 128 bits adres.

Ter illustratie: de 128 bit adresruimte is groot genoeg om elke viekante mm op het aardoppervlakte het equivalent van 155 biljoen (155×10^{12}) keer de IPv4 adresruimte te voorzien[65]. Uiteraard is een dergelijke bezetting niet te realiseren, omdat er altijd adresruimte verloren gaat bij het hiërarchisch verdelen van de adresruimte.

Een ander voordeel van de grotere adresruimte is dat het opnieuw mogelijk is om elk aan het Internet gekoppeld device een globaal bereikbaar IP adres toe te wijzen. Hierdoor zijn technologieën zoals Network Address Translation (NAT), die met name op het gebieden als VoIP, streaming en end-to-end security (IPSEC) voor problemen kunnen zorgen.

Ten slotte maakt de grotere adresruimte *stateless autoconfiguration* mogelijk. Hiermee kunnen aangesloten systemen zichzelf een globaal IPv6 adres toekennen, zonder het gebruik van DHCP[63] . Het IP adres wordt hierbij afgeleid van een prefix die middels een router advertisement wordt verspreid en het MAC adres van de netwerkinterface van het systeem.

3.2.2 Efficiëntie

De IPv6 pakket header is vereenvoudigd ten opzichte van IPv4 door het optioneel maken of laten vervallen van een aantal headervelden. Ook is de checksum die bij elke hop door routers opnieuw werd berekend in IPv4 komen te vervallen. Ten slotte is ook het fragmenteren en defragmenteren van IPv6 pakketten door routers komen te vervallen. Dit is vervangen door een 'Packet Too Big' ICMP bericht dat routers naar de afzender kunnen sturen.

Door deze maatregelen vindt er minder processing op routers plaats, en worden bandbreedtekosten voor het routeren van IPv6 headers beperkt.

3.2.3 Beveiliging en authenticatie

De *IP-security* (IPSEC) protocol suite [26][59] is een set protocollen die privacy en authenticatie services aanbieden op IP niveau. IPSEC ondersteuning is optioneel in IPv4 maar een verplicht onderdeel in IPv6.

Het end-to-end gebruik van IPSEC in combinatie met IPv4 wordt momenteel bemoeilijkt door de incompatibiliteittussen IPSEC en het veelvuldig gebruikte NAT protcol [1] .

Door de verplichte ondersteuning van IPSEC in IPv6 en het vervallen van NAT maakt end-to-end authenticatie en privacy op IP niveau mogelijk.

3.2.4 Multicasting

De basiswerking van multicasting is in IPv6 grotendeels hetzelfde als in IPv4. Één van de veranderingen is een *scope* veld waarmee het mogelijk is om aan te geven hoe ver de pakketten verstuurd dienen te worden. Voorbeelden van de mogelijke scopes zijn: link-local, site-local, organisation-local en global. Hoewel deze definities strikter zijn dan het gebruik van een hop-count, is wel extra configuratie en ondersteuning van alle tussenliggende routers noodzakelijk.

Daarnaast zijn *netwerkbroadcasts* komen te vervallen in IPv6 en volledig vervangen door multicasts.

3.3 Recente ontwikkelingen

Rondom de transitie van IPv4 naar IPv6 zijn er een aantal ontwikkelingen gaande. We willen hier kort stilstaan bij de status van de IPv4 adresruimte en actuele initiatieven rondom de invoering van IPv6.

3.3.1 IPv4 beschikbaarheid

Iljitsch van Beijnum heeft in januari 2008 een onderzoek gedaan naar het gebruik van de IPv4 adresruimte [66]. Het blijkt dat het aantal beschikbare IPv4 /8 adresblokken afgelopen jaar met 12 /8's is gedaald naar 43 beschikbare blokken. Het jaar daarvoor daalde het aantal beschikbare adresblokken met 10 /8's naar 55.

De verwachting is dat met de huidige groei halverwege 2011 alle /8 adresblokken door IANA zijn toegekend [20]. Uiteraard hebben de RIRs (Regional Internet Registries) zoals RIPE en ARIN daarna nog de beschikking over vrije adressen, maar het toekennen van nieuwe adresblokken aan de RIRs is dan niet meer mogelijk.

3.3.2 IPv6 transitie

Hoewel het IPv6 protocol al jaren geleden is gedefinieerd is er van een massale overgang op IPv6 nog geen sprake. Het lijkt er op dat veel commercieële partijen wachten op een *killer applicatie* voor IPv6, terwijl op hetzelfde moment het aantal vrije IPv4 adressen langzaam uitgeput raakt.

Nu steeds duidelijker is dat over enkele jaren de IPv4 adresruimte geheel vol zal raken, beginnen er een aantal initiatieven te ontstaan om de IPv6 overgang te stimuleren.

Zo heeft de Amerikaanse overheid middels een memorandum [16] van het Office of Management Budget geëist dat dat de netwerken van overheidinstellingen voor juli 2008 IPv6 moeten ondersteunen. Hoewel er nog geen eisen zijn ten aanzien van de beschikbaarheid van diensten op IPv6 is dit toch een stap in de goede richting. Onze visie is dat als andere overheden wereldwijd ook met dergelijke initiatieven komen, dit de uiteindelijke transitie naar IPv6 kan bespoedigen.

De RIPE Community heeft afgelopen oktober tijdens de RIPE 55 meeting in Amsterdam een statement [48] uitgegeven waarin men ISP's wil aanzetten tot het aanbieden van services via IPv6. Wellicht heeft dit een positief effect op de adoptie van IPv6 in de nabije toekomst.

3.4 NPO Case

NPO kan als publieke organisatie wellicht een voortrekkersrol spelen in de adoptie van IPv6. Hoewel NPO zelf niet direct te maken heeft met de problematiek van

het opraken van IPv4 adressen, zijn er wel een aantal voordelen die IPv6 NPO in de toekomst kan bieden. Een aantal hiervan bespreken we hier.

3.4.1 End-to-end connectiviteit

Het UDP protocol is bij uitstek geschikt voor het gebruik bij streaming media. Een voordeel van UDP is dat het connectionless is, waardoor het in stand houden van een sessie en het verwerken van *acknowledgements* zoals bij TCP niet nodig is.

Echter zorgt het UDP protocol voor problemen in combinatie met NAT. Doordat er geen sprake is van een daadwerkelijke *connection* tussen zender en ontvanger is het voor een NAT router niet mogelijk om UDP pakketten zonder problemen naar de juiste ontvanger door te sturen. Een en ander is te omzeilen door gebruik te maken van het handmatig configureren van *port forwarding*, maar dit is vaak omslachtig voor de eindgebruiker.

Hierdoor zijn organisaties zoals het NPO vaak genoodzaakt om streaming via TCP aan te bieden. Naast extra bandbreedte die *acknowledgements* en eventuele *retransmissies* veroorzaken is er ook extra geheugen en processing power nodig op de streaming servers voor de noodzakelijke *connection tracking*.

IPv6 biedt, net als IPv4 in het beginstadium, de mogelijkheid voor het realiseren van end-to-end connectiviteit tussen alle systemen op het Internet. Hiermee zijn oplossingen zoals NAT niet langer noodzakelijk, en wordt het mogelijk om vaker UDP te gebruiken voor streaming. Dit kan dus voor zowel een besparing op het gebied van bandbreedte als processingpower zorgen.

3.4.2 Multicasting

Live streaming media is bijzonder geschikt voor distributie via multicasting. Doordat een stream in feite vanaf het NPO nog maar één keer verstuurd moet worden is een enorme bandbreedtebesparing haalbaar. Om hier voordeel uit te halen is het wel noodzakelijk dat multicasting in het gehele pad van NPO tot eindgebruiker ondersteund wordt. Medewerking van grote ISP's is hiervoor dus een vereiste.

Op het gebied van multicasting is er ten opzichte van IPv4 grote geen sprake van grote veranderingen. Voor de implementatie van IPv6 zijn ISP's genoodzaakt veranderingen in hun netwerkinfrastructuur aan te brengen. Wellicht is dit een goede kans om multicasting opnieuw onder de aandacht te brengen. NPO zou hier een rol in kunnen spelen door providers actief te benaderen.

3.4.3 Authenticatie

IPSEC is standaard opgenomen in de IPv6 specificatie. Naast *encryptie* van gegevens is ook *end-to-end authenticatie* mogelijk. Dit gebeurt middels het *Authentication Header*

(HA) protocol [25], waarbij het IP pakket inclusief headerinformatie door de verzender wordt ondertekend.

We zien hierbij vooral mogelijkheden om het gebied van *Digital Right Management (DRM)*. Doordat de afkomst van IP pakketten gegarandeerd kan worden zijn er wellicht meer betrouwbare mogelijkheden om bijvoorbeeld het land te bepalen waarin de ontvanger van bijvoorbeeld een videostream zich bevind.

IPv6 adresruimte

Om een globaal beeld te krijgen van de wijze waarop IP adressering plaatsvindt beschrijven we allereerst de wereldwijde structuur die bestaat om de uitgifte van IP adressen en andere internet resources te regelen. Vervolgens bespreken we de mogelijkheden die er zijn om IPv6 adresruimte te verkrijgen. Hierbij besteden we ook aandacht aan relevante regelgeving, procedures, kosten en recente ontwikkelingen op dit gebied. Ten slotte beschouwen we de situatie voor NPO en geven we NPO een advies voor het aanvragen van IPv6 adresruimte.

4.1 Organisatie Internet resources

De Internet Assigned Numbers Authority (IANA) is de organisatie die de wereldwijde IP adresruimte beheert. IANA delegeert het beheer van de IP adresruimte naar de Regional Internet Registries (RIRs) waarvan er wereldwijd 5 bestaan, die met elkaar de gehele wereld dekken.

De RIRs delegeren de adresruimte volgens hun eigen beleid verder naar de Local Internet Registries (LIRs). Tot slot delegeert een LIR zijn adresruimte naar verschillende eindklanten.

In sommige gevallen is er nog sprake van een National Internet Registry (NIR) tussen de LIR en RIR. Dit is met name het geval in Azië en het Pacifisch gebied.

Het Réseaux IP Européens Network Coordination Centre (RIPE NCC) is de RIR die in Europa, het Midden Oosten en delen van centraal Azië verantwoordelijk is voor de uitgifte van IP adressen en AS (autonoom systeem) nummers.

RIPE NCC is niet hetzelfde als RIPE. RIPE is een open organisatie waarbij iedereen kan meedenken over de ontwikkeling van het uitgiftebeleid van internet resources. RIPE NCC is de organisatie die de daadwerkelijke uitvoering van het beleid verzorgt, in dit geval dus het toekennen van IP adresruimte aan LIRs en het bijhouden van de noodzakelijke administratie hieromtrent.

4.2 IPv6 adresruimte verkrijgen

Voordat organisaties aan de slag kunnen met IPv6 is het allereerst noodzakelijk om IPv6 adresruimte toegewezen te krijgen. Een IPv6-adresblok is op verschillende manieren te bemachtigen.

4.2.1 IPv6 adresallocatie via LIR

De meest gebruikelijke methode voor kleinere organisaties is het aanvragen van een adresblok via een LIR. In de praktijk betekent dit dat de internetprovider van de organisatie deze een adresblok toekent. Een probleem hierbij is dat de adresruimte aan de internetprovider is gekoppeld en niet is mee te nemen in het geval dat de organisatie voor een andere internet leverancier kiest.

Problemen ontstaan bij eind klanten die gebruik maken van meerdere leveranciers van connectiviteit (multihomed klanten). Er is bij IPv6 namelijk niet voorzien in provider independent (PI) adresruimte voor eindklanten, zoals dit bij IPv4 het geval is. Dergelijke klanten kunnen het adresblok die via een LIR is verkregen proberen te routeren via BGP. Een probleem hierbij is dat veel providers dergelijk kleine prefixes filteren uit hun BGP routers om de grootte van de routetabellen beperkt te houden [65]. Een alternatief is om als ISP aangemerkt te worden bij RIPE NCC, maar dit zal niet in alle gevallen mogelijk zijn.

Inmiddels wordt er al enige tijd gesproken [50] over een IPv6 direct assignment als equivalent voor een IPv4 PI allocatie. Een dergelijke allocatie is op het moment van schrijven echter nog niet aan te vragen via RIPE NCC. Wel zijn IPv6 direct assignments al opgenomen in de ripe charging schema's [44] van 2007 en 2008.

4.2.2 IPv6 adresallocatie via RIPE NCC

Voor organisaties die zelf als internet service provider functioneren is het mogelijk, indien dit nog niet het geval is, om lid van RIPE NCC te worden. Hierna kan men als LIR rechtstreeks een allocatie bij RIPE NCC aanvragen. Een voorwaarde hiervoor is dat de organisatie aan de adres-uitgiftepolicy's van RIPE voldoet. Een voordeel van deze methode is dat de verkregen adresruimte niet aan een provider is gekoppeld.

Randvoorwaarden Elke RIR voert een eigen beleid met betrekking tot de uitgifte van IP adressen. In dit onderzoek richten wij ons op de Nederlandse situatie en richten we ons uitsluitend op het beleid van RIPE. Het beleid van andere RIRs kan op sommige punten verschillen van het beleid van RIPE, maar zal in hoofdlijnen hetzelfde zijn.

Tot juli 2007 bestonden de eisen voor het verkrijgen van een adresruimte via RIPE NCC tot het zijn van een LIR, het niet zijn van een 'end-site', en een plan hebben voor het maken van minimaal 200 /48 allocaties naar end-users binnen 2 jaar [42].

In mei 2006 verscheen een RIPE policy proposal waarin men de problemen onderkende voor het verkrijgen van adresruimte voor kleine providers met minder dan 200 klanten en instellingen zoals universiteiten en grote bedrijven met meerdere upstream providers [32].

Om het voor dergelijke instellingen toch mogelijk te maken om op een provider onafhankelijke manier IPv6 adresruimte te verkrijgen is het beleid sinds juli 2007 sterk

versoepeld . De eis tot het hebben van een plan voor het maken van 200 /48 allocaties is komen te vervallen. De eis om een plan te hebben om binnen 2 jaar suballocaties naar andere organisaties of end-sites te maken is hiervoor in de plaats gekomen [43].

Allocatie en suballocatie Bij de aanvraag van een IPv6 allocatie door een LIR wordt standaard een /32 toegekend [45]. Organisaties kunnen een grotere toewijzing krijgen indien documentatie overlegd kan worden die dit verzoek ondersteunt. Gezien de enorme hoeveelheid adressen binnen een /32 zal dit slechts in uitzonderlijke gevallen noodzakelijk zijn. Een /32 geeft de mogelijkheid om deze in 65.536 /48 subnetten of 16.777.216 /56 subnetten te verdelen.

De RIPE policy stelt dat een LIR zijn eigen beleid mag bepalen voor het maken van suballocaties [45] . Momenteel is het maken van /48 suballocaties voor end-sites die gebruik willen maken van meerdere subnetten het meest gebruikelijk en beschreven in een RFC [21]. De mimimale allocatiegroote is /64 en biedt ruimte voor een enkel subnet. Allocaties aan end-sites groter dan /48 moeten wel aan RIPE worden gemeld.

Een /48 biedt ruimte aan 65.536 /64 subnetten. Doordat veel end-sites de 65.536 subnetten niet in gebruik zullen nemen is er een risico van het verspillen van internetadressen. Een provider die steeds /48's aan eindklanten toekend heeft dus meerdere /32's nodig indien deze meer dan 65.536 klanten heeft, alhoewel het grootste gedeelte van de adresruimte dan nog ongebruikt is.

Bij het beoordelen van een aanvraag voor extra IPv6 adresruimte gebruikt RIPE de HD ratio [14] om te beoordelen of de reeds toegekende adresruimte wel voldoende is benut. In augustus 2005 is een voorstel ingediend [28] om bij deze berekeningsmethode voor de efficiëntie van adresallocatie uit te gaan van /56 allocaties in plaats van /48 allocaties. Deze wijzigingen zijn inmiddels opgenomen in de meest actuele versie van de RIPE IPv6 policy [45] die dateert van november 2007.

Een LIR die aan alle klanten een /48 toekend heeft dus niet zonder meer recht op aanvullende adresruimte indien de initiële /32 allocatie volloopt. Het is dus voor een LIR belangrijk om dit bij het vaststellen van een suballocatiebeleid in beschouwing te nemen.

Procedures

Om een IPv6 allocatie via RIPE aan te vragen is het noodzakelijk eerst RIPE NCC lid te worden indien dit nog niet het geval is. Daarna kan de aanvraagprocedure van een IPv6 allocatie en bijbehorende reverse zone bij RIPE in gang gezet worden. Ten slotte dient een AS nummer aangevraagd te worden die bij de routering via BGP gebruikt wordt.

RIPE NCC lidmaatschap Organisaties die lid zijn van RIPE NCC worden Local Internet Registries (LIRs) genoemd. De aanvraagprocedure hiervoor is beschreven op de RIPE website [51]. Organisaties die al LIR zijn kunnen direct een IPv6 allocatie aanvragen.

De eerste stap in de aanvraagprocedure is het invullen van het online member application form. Hierna stuurt RIPE NCC de aanvrager een contract en factuur voor de registratie en lidmaatschapskosten. De aanvrager dient de factuur te voldoen en het contract samen met een Kamer van Koophandel uitreksel terug te sturen. Ten slotte stuurt RIPE NCC een welkomstpakket met onder andere toegangsgevens tot de LIR Portal waarmee IP en AS allocaties aangevraagd en bewerkt kunnen worden.

Volgens de informatie op de RIPE NCC website kan de volledige aanvraagprocedure binnen 2 tot 3 weken worden doorlopen.

IPv6 adresruimte aanvragen LIRs kunnen via het IPv6 First Allocation Request Form [47] een IPv6 delegatie aanvragen. De bijbehorende Supporting Notes [46] geven meer informatie over de wijze waarop dit formulier ingevuld dient te worden.

In dit formulier dient de aanvrager een korte beschrijving van de organisatie te geven, en een IPv6 allocation usage plan in te vullen. Dit plan is een eenvoudige tabel waarin de aanvrager de subnetten aangeeft waarin de aangevraagde adresruimte verdeeld wordt. Per subnet dient de subnetgrootte en een korte beschrijving van het gebruik van het subnet aangegeven te worden. Daarnaast wordt per subnet gevraagd of ingebruikname binnen 3 maanden, binnen 1 jaar of binnen 2 jaar plaats zal vinden.

Zoals eerder is aangegeven is de eis voor het aanvragen van een IPv6 allocatie sinds juli 2007 dat er binnen 2 jaar *een* suballocatie moet plaatsvinden. In feite is het dus voldoende om in het adresseringsplan slechts een enkel subnet te definieëren.

Reverse delegation aanvragen Nadat een IPv6 adresblok is toegekend is het mogelijk een reverse DNS delegatie voor dit adresblok aan te vragen. Allereerst dienen de nameservers van de aanvrager geconfigureerd te worden voor de bijbehorende "ip6.arpa" zone. Het aanvragen van de daadwerkelijke delegatie wordt gedaan middels het aanmaken van een "domain object". De 'Reverse Delegation How To' [52] geeft een duidelijke stapsgewijze beschrijving van dit proces.

AS-nummer aanvragen Het hebben van een autonoom systeem nummer (ASN) is van belang voor organisaties die een multihomed netwerk beheren en via BGP tussen de verschillende verbindingen routeren.

Een AS nummer kan zowel via een LIR als via een RIR worden aangevraagd. Voor organisaties die reeds een AS-nummer in bezit hebben via een LIR is het niet noodzakelijk een nieuw AS-nummer aan te vragen indien de organisatie zelf LIR wordt.

In veel gevallen zal een AS-nummer reeds aanwezig zijn, of niet noodzakelijk zijn. Via de LIR portal webinterface van RIPE NCC is het mogelijk een AS nummer aan te vragen.

Naast een AS nummer voor de organisatie zelf is het mogelijk dat klanten ook een AS-nummer nodig hebben indien deze een multihomed netwerk beheren. Voor LIRs is het dus mogelijk om AS nummers voor klanten aan te vragen.

Catagorie	Maximum score	Jaarlijkse bijdrage
Extra Small	18	EUR 1300
Small	112	EUR 1800
Medium	864	EUR 2550
Large	5696	EUR 4100
Extra Large	247003	EUR 5500

Tabel 4.1: RIPE ledenbijdragen, 2008

Kosten

Internetresources zoals IP adressen en AS nummer zijn publiek goed. Daarom rekent RIPE NCC geen directe kosten voor de allocatie en het in gebruik hebben van dergelijke resources. Wel is er sprake van een eenmalige 'sign-up fee' en een jaarlijkse 'service fee' die afhankelijk is van de hoeveelheid resources dat in gebruik is door de LIR.

De kosten worden jaarlijks met instemming van de LIRs vastgelegd in de 'RIPE NCC Charging Scheme'. In het 'RIPE NCC Charging Scheme 2008' [44] is te zien dat de eenmalige en jaarlijkse kosten sinds 2004 steeds zijn gedaald. Dat is waarschijnlijk mogelijk doordat het aantal leden sinds 2004 jaarlijks met 10 tot 12 % is toegenomen, waardoor de kosten meer verspreid worden.

Berekeningsmethode De eenmalige sign-up fee voor 2008 bedraagt EUR 2000. De hoogte van de jaarlijkse bijdrage is afhankelijk van de hoeveelheid resources dat de deelnemer in gebruik heeft. Hiervoor wordt elke deelnemer in één van de catagoriën extra small, small, medium, large of extra large ingedeeld. Nieuwe LIRs worden in eerste instantie in de catagorie extra small ingedeeld.

Middels het billing score algoritme is het mogelijk de categorie waartoe de deelnemer behoort te bereken. De kosten en maximum score voor het billing score algoritme per categorie [53] zijn weergegeven in tabel 4.1.

De formule voor het berekenen van de billing score is als volgt:

$$S = \sum_{i=1}^{N} a_i \times t_i$$

S = Billing score
a_i = Scoring unit
t_i = Tijdfunctie van allocatie i (jaar van allocatie - 1992)
N = Aantal allocaties

Elke allocatie i heeft een eigen scoring unit. Deze zijn terug te vinden in tabel 4.2.

De scoring unit voor het in gebruik hebben van een /32 IPv6 allocatie is 1.0. Een andere relevante scoring unit is die voor een AS-nummer assignment. Voor 2008

IPv4 allocatie	IPv6 allocatie	ASN assignment	Scoring unit
/22	/33		0.5
/21	/32	1	1.0
/20	/31	2	2.0
/19	/30	4	4.0

Tabel 4.2: RIPE Scoretabel, 2008

geldt dat alleen AS-nummer assignments tussen 1 oktober 2006 en 30 september 2007 worden meegenomen in de berekening. De scoring unit voor een AS nummer is eveneens 1.0, maar wordt dus slechts eenmalig meegenomen in de berekening.

Het gaat hierbij alleen om allocaties en assignments die gemaakt zijn door de LIR zelf. IP reeksen en AS nummers die reeds via een andere partij zijn verkregen worden niet meegenomen in deze berekening.

4.3 NPO Case

Voor de NPO case beschrijven we eerst de huidige IPv4 situatie en de gewenste IPv6 situatie. Daarna geven we NPO een advies voor het verkrijgen van een IPv6 adresruimte, inclusief een overzicht van de bijbehorende kosten.

4.3.1 Huidige situatie IPv4

Op dit moment maakt NPO gebruik van een IPv4 subnet, 145.58.0.0/16, origineel verkregen van SURFnet. Daarnaast heeft NPO een eigen autonoom systeem, AS25182, ten behoeve van de routering tussen verschillende netwerkleveranciers.

De adresruimte is vrijwel in alle gevallen onderverdeeld in /24 subnetten, waarbij de subnetten per functie zijn verdeeld. Verschillende functies zijn voor de internetlaag in dit geval bijvoorbeeld: DNS, streaming, omroep.nl webservers, hostingnetwerk voor omroepen, etc. In de gevallen dat het /24 subnet ontoereikend is, zijn er meerdere /24 subnetten toegekend of in enkele gevallen een groter subnet dan /24.

Het aantal adressen dat zich binnen de /16 van NPO bevindt is ruim voldoende voor adressering van de huidige netwerkinfrastructuur en biedt voorlopig voldoende uitbreidingsruimte. Alleen het vollopen van /24 allocaties vormt een mogelijk knelpunt, hoewel dit over het algemeen eenvoudig is op te lossen door het vergroten van het subnet, of het toekennen van een extra /24 allocatie.

4.3.2 Gewenste situatie IPv6

De voorkeur van NPO gaat uit naar een provider onafhankelijke adresruimte, waarmee de gewenste onafhankelijkheid van netwerkleveranciers te realiseren zal zijn. Daar-

naast wil NPO voldoende adresruimte hebben om suballocaties naar de verschillende omroepen en bedrijfsonderdelen te maken.

4.3.3 Advies

Doordat NPO ICT onder andere internettoegang en verschillende hostingdiensten voor de diverse omroepen verzorgt, is NPO niet alleen een eindgebruiker. Volgens de regelingen van RIPE NCC kan NPO hierdoor aangemerkt worden als ISP, waardoor een RIPE NCC lidmaatschap mogelijk is.

De nieuwe regelingen stellen dat LIRs voor het aanvragen van IPv6 adresruimte een plan moeten hebben om binnen 2 jaar een suballocatie naar een end-user of organisatie te doen. Ook dit zal voor NPO zeker haalbaar zijn.

Nadat een IPv6 allocatie aan NPO is toegekend, heeft deze de beschikking over een /32 subnet. Hiermee heeft NPO de mogelijkheid om /48 subnetten te alloceren aan de verschillende omroepen en bedrijfsonderdelen. Het aantal van 65.536 /48 subnetten zal hiervoor meer dan voldoende zijn.

Het is onwaarschijnlijk dat er ooit sprake zal zijn van het volraken van de /32 wanneer deze is verdeeld in /48's. Daarom speelt de keuze tussen /56 en /48 subnetten voor suballocatie een mindere belangrijke rol voor NPO. Het onderwerp subnetting zal bij de bespreking van technische details verder worden besproken.

Kosten

Voor NPO is de eenmalige sign-up fee voor 2008 van toepassing. De kosten hiervoor bedragen EUR 2000. Nieuwe LIRs worden automatisch ingedeeld in de extra small catagorie. De jaarlijkse lidmaatschapskosten voor deelnemers in deze catagorie bedragen EUR 1300.

Een AS nummer is reeds in het bezit van NPO. Het enige dat NPO als LIR moet aanvragen is dus een IPv6-allocatie. Voor het berekenen van de billing score is er dus sprake van één allocatie met een scoring unit van 1.0:

$$\begin{aligned} S &= a_i \times t_i \\ &= 1 \times (2008 - 1992) \\ &= 16 \end{aligned}$$

Dit resulteert in een billing score S van 16, waarmee NPO onder de maximumscore van 18 blijft voor de extra small catagorie volgens de kostenstructuur van 2008. Indien er geen aanvullende allocaties noodzakelijk zijn, is dus te verwachten dat NPO de komende jaren in de extra small, of hooguit in de small catagorie ingedeeld zal blijven.

Netwerk

Om diensten over IPv6 aan te kunnen bieden, moet het netwerk daarop voorbereid zijn. Alle apparatuur in het pad van client naar de over IPv6 aan te bieden dienst moet het protocol ondersteunen of (in het geval van bijvoorbeeld layer 2 switches) ongewijzigd kunnen doorsturen.

5.1 Netwerkcore

Afhankelijk van de grootte van het netwerk kan het implementeren van IPv6 eenvoudig of juist heel complex zijn. De meest simpele netwerken hebben één router die het netwerk, bestaande uit enkele switches, verbindt met het internet. Complexere netwerken maken gebruik van meerdere subnets, virtuele LANs en zowel interne als externe routers.

5.2 Switching

Switching gebeurt op een laag onder het IP-protocol. Voor eenvoudige situaties is dus geen aanpassing van de switches nodig en is ondersteuning voor IPv6 net zo min nodig als ondersteuning voor IPv4. Voor uitgebreidere (managed) switches geldt echter dat een beperkte ondersteuning wel gewenst of noodzakelijk is. Hierdoor blijven deze switches ook te beheren na een volledige overstap op IPv6 waarbij IPv4 niet (meer) beschikbaar is.

Er is één specifiek probleem dat kan ontstaan in laag-2 switches bij het gebruik van IPv6. In IPv4 wordt voor neighbour detection gebruik gemaakt van broadcasts met het ARP protocol. In IPv6 wordt daarvoor gebruik gemaakt van een nieuw protocol, dat gebruik maakt van multicast. Veel uitgebreidere switches 'helpen' IPv4 multicast door op zoek te gaan naar Internet Group Message Protocol (IGMP) berichten. Door die berichten te verwerken kunnen de switches multicast streams alleen naar die poorten doorsturen waar zich een ontvanger van de multicast stream bevindt. Afhankelijk van de switch kan dir mechanisme in combinatie met IPv6 problemen veroorzaken omdat voor IPv6 geen gebruik wordt gemaakt van IGMP. De switch kan dan besluiten de neighbor detection berichten niet door te sturen, waardoor een IPv6 host zichzelf nooit bekend kan maken op het netwerk. De host zal dus onbereikbaar zijn. Niet alle switches hebben last van dit probleem. Het kan verholpen worden door de *IGMP Snooping* optie uit te zetten.

5.3 Externe routering

De externe routering (naar het Internet toe) wordt in alle *multihomed* netwerken met hetzelfde protocol gedaan: het Border Gateway Protocol (BGP)[40]. Dit protocol is een path vector protocol, wat inhoudt dat het in essentie op dezelfde manier werkt als een distance vector protocol [61]: het berekent het kortste pad naar een bestemming. Het verschil tussen een distance vector protocol en een path vector protocol is dat de router in het laatste geval bij updates een volledig pad toegestuurd krijgt naar elke bekende bestemming. Aan de hand daarvan kan de router beslissen of dat een goed pad is: het kan bijvoorbeeld zijn dat de router configureerd is om bepaalde paden niet te gebruiken. Een distance vector protocol laat die informatie weg en geeft alleen een 'afstand' mee, aan de hand waarvan een router beslist het pad wel of niet te gebruiken.

BGP werkt aan de hand van expliciet geconfigureerde *peers*. Met die peers wisselt het informatie uit over bereikbare bestemmingen.

5.3.1 Multi-protocolondersteuning

Bij het opzetten van een verbinding met een peer, wordt onderhandeld over welke *capabilities* (mogelijkheden) de beide systemen hebben. Een van die onderhandelbare mogelijkheden zijn de *multiprotocol extensions* [31]. Door aan te geven dat de router die mogelijkheid ondersteunt, kan BGP buiten IPv4, waarvoor het ontworpen is, ook andere protocollen ondersteunen zoals IPv6 en zelfs IPX of AppleTalk.

Afhankelijk van het gerouteerde protocol zal de configuratie ervan met BGP verschillen. Echter, omdat IPv6 en IPv4 conceptueel grotendeels gelijk zijn is de ondersteuning van functionaliteit en het gebruik van BGP met de twee protocollen gelijk. Ook de configuratie geschiedt om die reden op dezelfde wijze [8].

5.3.2 Peering

Afhankelijk van de implementatie zal het nodig zijn om IPv6 peerings apart op te zetten of kunnen ze gecombineerd worden. In apparatuur van Cisco moet dat bijvoorbeeld apart gedaan worden. Bij de meest gebruikte Internet Exchanges is peering op IPv6 reeds mogelijk en in productie. Een voorbeeld daarvan is de AMS-IX. Om op AMS-IX te peeren op IPv6 hoeft slechts een IPv6-adres aangevraagd te worden voor de router, waarna begonnen kan worden met het aanmaken van peerings [67]. Een toenemend aantal AMS-IX leden maakt van deze mogelijkheid gebruik. Op dit moment zijn dat voornamelijk Internet Service Providers en organisaties die tunnels aanbieden. Nog niet veel Internet Access Providers bieden IPv6 aan hun klanten aan. Noemenswaardige uitzonderingen zijn SURFnet en de verscheidene andere Nationale Researchnetwerken (NRENs).

5.3.3 Transit

Om globale connectiviteit te verkrijgen op IPv6 is een leverancier van transitconnectiviteit nodig. Een toenemend aantal leveranciers kan in die behoefte voorzien. Enkele voorbeelden hiervan zijn Level3, Global Crossing en Tiscali [56]. Voor organisaties die daartoe in aanmerking komen kunnen de NRENs ook dienen als leverancier van transitconnectiviteit.

De exacte manier waarop IPv6 transit afgenomen wordt verschilt per aanbieder, maar verschilt gewoonlijk weinig van de manier waarop IPv4 transit wordt afgenomen.

5.3.4 Interne routering

Er bestaan meerdere protocollen voor interne routering. We behandelen er drie.

RIP

RIP, het Routing Information Protocol, is een Distance-Vector routing protocol. De meeste actuele versie van dit protocol is RIPv2 [29]. Het gebruikt de hop-count tussen twee netwerken om beslissingen te maken over de beste route tussen de netwerken. RIP ondersteunt IPv6 in de vorm van RIPng (RIP next generation) [30]. Dit protocol is functioneel gelijk aan RIPv2. Vrijwel alle aanwezige kennis over het gebruik van RIPv2, met uitzondering van kennis over de samenstelling van de packets, is direct toepasbaar. De verschillen tussen RIPv2 en RIPng zijn als volgt [68]:

- RIPng ondersteunt geen authenticatie maar gaat uit van de beschikbaarheid van IPSec.
- RIPv2 ondersteunt het toevoegen van tags aan routes, RIPng niet.
- RIPv2 en RIPng hebben verschillende manieren om het next-hop adres in de packet te encoderen

RIP is bedoeld voor kleine netwerken en is dus niet geschikt voor grotere netwerken. Zo is het maximum aantal hops vastgesteld op 15 en worden updates gepropageerd door elke 30 seconden de gehele routing tabel te verspreiden, wat op grotere netwerken voor veel extra verkeer kan zorgen.

RIPv2 en RIPng zijn niet compatibel met elkaar. De twee protocollen kunnen echter wel naast elkaar gebruikt worden.

OSPF

Het Open Shortest Path First (OSPF) protocol is een hierarchisch link-state protocol [61]. Elke router krijgt updates over hoe het netwerk in elkaar steekt en houdt een

graaf bij van de verbindingen. Vervolgens berekent de router naar elk netwerk het beste pad.

OSPF bestaat in twee versies: OSPFv2[36] en OSPFv3[11]. Versie 2 wordt gebruikt voor IPv4 en versie 3 voor IPv6. De twee versies zijn verschillend van elkaar. Hoewel het mogelijk geweest zou zijn om OSPFv2 uit te breiden met ondersteuning voor IPv6, is ervoor gekozen om dat niet te doen zodat het protocol zelf ook verbeterd kon worden.

OSPFv3 is functioneel voor het grootste deel gelijk aan OSPFv2.Het is namelijk nog altijd een link-state protocol en gebouwd op dezelfde basis aan pakkettypen, etc. De verschillen gaan voornamelijk om details, waaronder[24]:

- OSPFv3 werkt op een link, in plaats van op een subnet
- OSPFv3 gebruikt link-local IP-adressen, OSPFv2 gebruikt normale adressen
- OSPFv3 kent, net als RIPng, geen authenticatie maar gaat uit van IPSec

OSPF is een betere keus dan RIP voor grotere netwerken. Het heeft geen ingebouwde hoplimit en omdat het niet elke 30 seconden een volledige routetabel stuurt is er ook geen probleem met netwerkbelasting.

Hoewel ook OSPFv2 en OSPFv3 niet compatibel met elkaar zijn, is het net als met RIP mogelijk de twee versies naast elkaar te gebruiken.

iBGP

iBGP, Interior BGP, is feitelijk hetzelfde als het reguliere BGP-protocol, met slechts een andere behandeling door routers. De protocollen zijn gelijk. Voor het gebruik van iBGP met IPv6 hoeven dus geen speciale voorzieningen worden getroffen ten overzichte van het reguliere BGP.

5.3.5 Aandachtspunten

Voor RIPng en OSPFv3 geldt dat het aparte protocollen zijn die apart geïmplementeerd moeten worden op de routers. Dat houdt in dat een extra proces moet draaien op de router met extra geheugengebruik voor zowel het proces zelf als de extra routes. Ook houdt dit mogelijk in (afhankelijk van de implementatie) dat de protocollen los van elkaar beheerd dienen te worden.

5.4 Firewalling

Firewalls worden door vrijwel alle organisaties ingezet om hun netwerken te beschermen tegen indringers. Veel gebruikers (zowel organisaties als thuisgebruikers) gebrui-

ken een firewall in combinatie met Network Address Translation (NAT) [57]. Het gebruik van interne addressering [41] helpt daarbij voorkomen dat externe hosts direct toegang hebben tot het interne netwerk.

IPv6 maakt, dankzij de enorme hoeveelheid adressen, interne addressering en NAT overbodig. Een goede firewall is dus van groot belang. Die kan op twee manieren geïmplementeerd worden: een losse netwerkappliance (daarin modules die in routers geplaatst kunnen worden inbegrepen) of software op de host zelf.

5.4.1 Host-based

Er zijn veel verschillende platforms die IPv6 ondersteunen. Vrijwel allemaal hebben ze ingebouwde faciliteiten voor het firewallen van netwerkverbindingen.

Microsoft ondersteunt IPv6 firewalling standaard in Windows XP met Service Pack 2 of nieuwer in de Windows Firewall. Een limitatie bestaat: de firewall werkt altijd voor beide protocollen tegelijkertijd. Het toestaan van een bepaalde service op IPv4 zal dus automatisch leiden tot het toestaan van dezelfde service op IPv6 [64]. Voor Windows Server 2003 vanaf Service Pack 1 geldt dezelfde limitering. Windows Vista maakt gebruik van een compleet vernieuwde TCP/IP stack, met daarbij ook een nieuwe versie van Windows Firewall. De eerder genoemde limieten bestaan hierin niet [33].

Apple's MacOS X ondersteunt IPv6, inclusief GUI configuratie, sinds versie 10.4 (Tiger). De GUI ondersteunt echter niet het instellen van de IPv6 firewall. De functionaliteit is in het OS wel aanwezig doormiddel van het 'ip6fw' commando, waar IPv4 ingesteld wordt met het commando 'ipfw'. Het gebruik van de commando's is, afgezien van afwijkende benamingen, identiek.

In Linux gebeurt het firewallen van IPv6 op een soortgelijke manier. Voor IPv4 wordt gebruik gemaakt van het commando 'iptables', het IPv6-equivalent is 'ip6tables'. Ook hier is het gebruik identiek aan de commando's voor IPv4.

OpenBSD wordt vaak gebruikt voor firewalls en wijkt af van de meeste andere unices ten opzichte van de firewall. Veelal maken IPv4 en IPv6, zoals in o.a. Linux, gebruik van aparte firewalls. In OpenBSD echter, wordt voor de beide protocollen dezelfde firewall gebruikt met dezelfde commando's. Er wordt op geen enkele manier onderscheid gemaakt en het is mogelijk om bijvoorbeeld een poort met een enkel commando open te te zetten voor zowel een specifiek IPv4- als IPv6-adres. Voor de overige besturingssystemen geldt dus dat het gebruik van IPv6 dus extra beheer op het gebied van firewalling vereist.

5.4.2 Appliances

Ook in de wereld van Firewall Appliances zijn er veel opties. Een veelgebruikt platform voor firewalls in het netwerk is OpenBSD, zie daarvoor de Host-based firewalls. We bespreken hier enkele firewall-appliances.

CheckPoint, de software die o.a. Nokia gebruikt in hun firewall appliances, ondersteunt IPv6 sinds de FireWall-1 Next Generation, Feature Pack 3 release [6]. De mogelijkheid bestaat dat een licentie nodig is om IPv6 rules aan te maken [54].

Cisco's PIX firewalls ondersteunen IPv6 vanaf PIX versie 7.0 [10]. De Firewall Service Modules (FWSM) voor Catalyst 6500 en 7600 switches ondersteunen ook het gebruik van IPv6, mits in *Routed Firewall Mode* [7].

Juniper's Netscreen firewallproducten ondersteunen IPv6 vanaf ScreenOS versie 5.0 [23].

5.5 NPO Case

5.5.1 Topologie

Het netwerk van NPO bestaat uit drie logische lagen:

- Intranet (Aansluitingen naar desktops e.d.)
- Core (Aansluitingen naar het Internet en interconnectie tussen de andere lagen)
- Internet (Aansluitingen naar streaming servers e.d.)

De Corelaag is de laag die voorziet in de connectiviteit met het internet voor de Internet- en intranetlagen. De Internetlaag bevat alle infrastructuur voor diensten die vanaf het Internet bereikbaar zijn: webservers, streaming servers, mailservers, etc. Afgezien van tests op lokale schaal is een implementatie van globaal bereikbare IPv6-services, zoals het streamen van een video naar een client ergens anders op het Internet, dus onmogelijk zonder ondersteuning in de Corelaag.

De Intranetlaag voorziet in connectiviteit voor de gebruikers bij de omroepen. Daar bevinden zich onder andere de desktop-PC's van de medewerkers, binnen NPO beter bekend onder de noemer kantoorautomatisering.

Zoals eerder beschreven moet, om IPv6 te kunnen aanbieden, eerst de netwerkcore voorbereid zijn. Die bestaat bij NPO uit een tweetal Cisco 6500 routing switches, voorzien van verbindingen tussen elkaar, de andere delen van het NPO-netwerk en met verscheidene Internet-gerelateerde netwerken zoals AMS-IX, SURFnet en KPN.

5.5.2 Subnetting

In tegenstelling tot de huidige situatie met IPv4 bestaan bij IPv6 best-practices voor het gebruik van subnets. Uitgaande van de situatie dat NPO een LIR wordt bij RIPE zal zij de beschikking krijgen over een /32-subnet. De best-practices schrijven vervolgens voor dat per aangesloten end-site een /48 gealloceerd wordt. Om een dergelijke allocatie te maken hoeft niets gedaan te worden aangaande melding bij RIPE zoals

dat het geval is voor LIRs die meer dan hun assignment window[1] aan IPv4-adressen willen alloceren. Indien een end-site meer ruimte nodig heeft dan een /48 moet dat in overeenstemming met RIPE gedaan worden. Gezien dat een /48 bestaat uit 2^{16} /64-subnets, zal dat bij NPO niet voorkomen.

De /32 kan in het begin opgedeeld worden in drie /48's voor NPO's intranet, core en internet-laag. Deze /48's zijn verder te verdelen in /64 subnetten voor verschillende onderdelen zoals webhosting, streaming, verschillende afdelingen, etc. In een later stadium kan per omroep een /48 worden toegekend.

5.5.3 Routing en switching

Om IPv6 te kunnen implementeren moet bij de twee core routers begonnen worden. De Cisco 6500 series ondersteunen IPv6 volledig: deze machines kunnen dit protocol in hardware afhandelen zodat er geen performanceproblemen ontstaan. Hierdoor is er ook geen gevaar dat de snelheid van IPv4-verkeer inzakt omdat de processor overbelast is met het routeren van IPv6. Wel is kan het noodzakelijk zijn dat er een Cisco softwareversie met IPv6 licentie op de routers aanwezig is.

Standaard staat het routeren van IPv6 in de Cisco 6500 uit. Het aanzetten is feitelijk een kwestie van niet meer dan een enkel commando invoeren en IPv6-adressen toewijzen aan de verschillende interfaces.

NPO gebruikt alleen Cisco 6500 series voor laag-3 routering. Het is dus op dit moment nog niet nodig om veranderingen te maken aan andere switches die alleen voor laag-2 switching zorgen.

Routing Protocollen

Het netwerk maakt gebruik van BGP4 en OSPF om routing informatie tussen de verschillende routers up-to-date te houden. Voor beide is het nodig wat aandacht te geven aan de configuratie om IPv6 te ondersteunen.

BGP4 Ondanks dat BGP ontworpen is voor IPv4 is het goed voorbereid op andere protocollen door middel van de eerder besproken Multiprotocol Extensions. Het Cisco 6500-platform ondersteunt het gebruik van BGP4 met IPv6. Cisco heeft uitgebreide documentatie beschikbaar [8] waarin gedetailleerd wordt welke stappen genomen moeten worden om BGP en iBGP met IPv6 te implementeren, inclusief welke specifieke commando's daarvoor nodig zijn.

OSPF Bij OSPF is een andere weg ingeslagen: IPv6 wordt als een nieuwe versie van het protocol geïmplementeerd: OSPFv3. NPO maakt nog gebruik van OSPFv2 en zal

[1] Het maximaal aantal IP-adressen dat per klant mag worden gealloceerd in 12 maanden waarvoor geen toestemming van RIPE nodig is [49]. De assignment window wordt groter naar mate de LIR meer laat zien goed met de policy om te gaan.

dat ook moeten blijven doen aangezien OSPFv3 niet geschikt is voor IPv4. Dat houdt dus in dat de routers een extra routing proces moeten draaien.

Echter, in tegenstelling tot OSPFv2 voor IPv4, gebeurt bij Cisco's 6500 switches de configuratie en het opstarten daarvan automatisch. Waar bij OSPFv2 de gebruikte interfaces indirect worden geconfigureerd via het `router`-commando, gebeurt dat bij OSPFv3 direct bij de configuratie van de interface. Ook voor de configuratie van OSPF in combinatie met IPv6 heeft cisco uitgebreide documentatie beschikbaar [9].

Transit

Net als voor IPv4 heeft iedere organisatie die via IPv6 op het gehele internet bereikbaar wil zijn een leverancier van transitconnectiviteit nodig. NPO neemt voor IPv4 onder andere transit af van het nationale Nederlandse onderzoeksnetwerk SURFnet. Gezien het feit dat SURFnet ook IPv6 connectiviteit aanbied ligt het voor de hand dat zij ook NPO's leverancier wordt van IPv6 transitconnectiviteit. Het gebruik van een bestaande leverancier beperkt de extra configuratie tot een minimum.

Peering

NPO is aanwezig op de AMS-IX en NL-IX Internet Exchanges. Op beide exchanges is peering op basis van IPv6 mogelijk. NPO wil graag een indruk hebben met hoeveel van de huidige peering partners het potentieel mogelijk is om via IPv6 te peeren. Om dit te bepalen hebben we een korte analyse uitgevoerd aan de hand van beschikbare data van NPO zelf en via de RIPE NCC whois database.

We hebben gemerkt dat niet alle LIRs hun IPv6 allocaties in de RIPE database aan een AS nummer hebben gekoppeld. Hierdoor is de onderzochte informatie niet volledig. Omdat de belangrijkste peering partners van NPO zich bevinden in Europa hebben wij ons beperkt tot informatie uit de RIPE NCC databases. De gebruikte gegevens dateren van 17 januari 2008.

Uit de RIPE database waarin NPO de informatie over peering partners bijhoudt blijkt dat NPO op dit moment met 196 verschillende autonome systemen peert. Van de 196 AS nummers is van 181 ASNs informatie in de RIPE database beschikbaar. De overige 15 AS nummers vallen onder het beheer van een andere RIR.

Voor alle AS nummers hebben we middels een *inverse lookup* op het 'route6' attribuut in de whois achterhaald aan welke van deze autonome systemen een IPv6 adresreeks is gekoppeld. Het blijkt dat van 45 autonome systemen een IPv6 allocatie bekend is in de RIPE NCC database.

Een volledig overzicht van de 45 potentiële IPv6 peers en de gevolgde werkwijze is te vinden in bijlage A.

	Aantal	% Totaal	% In RIPE DB
Totaal aantal AS-en	196	100%	-
Bekend in RIPE database	181	92%	100%
Onbekend in RIPE database	15	8%	0%
AS-en met IPv6 allocatie	45	23%	25%

Tabel 5.1: Potentiële IPv6 peers

IPv6 services aanbieden

Een eerste stap naar het aanbieden van webservices via IPv6 is te bepalen hoe dit binnen de huidige IT-architectuur past, en hoe deze architectuur in de toekomst zal veranderen. Voor grotere omgevingen is met name het aspect van loadbalancing hierbij interessant. Het blijkt dat het realiseren van *IPv6 loadbalancing* zeker niet triviaal is. Ten slotte is het belangrijk om de mate van IPv6 ondersteuning voor veelgebruikte webservices in kaart te brengen.

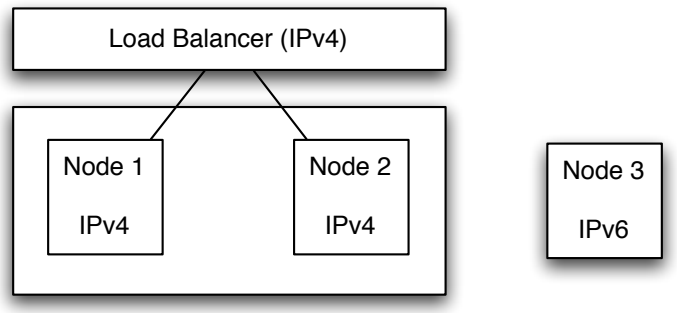
6.1 Architectuur

Binnen een bestaande IT-architectuur zijn er twee verschillende methoden om IPv6 webservices aan eindgebruikers aan te bieden. Beide modellen zijn in verschillende situaties toepasbaar en hebben elk hun specifieke voor- en nadelen.

6.1.1 Single-stack omgevingen

Het meest eenvoudige model is een nieuwe IPv6 single stack omgeving naast de huidige IPv4 infrastructuur op te zetten. Figuur 6.1 geeft een schematische weergave van deze situatie.

Een dergelijke opstelling zal voor sommige webservices voor de front-end zijde mogelijk zijn. Aan de back-end zijde kan het soms noodzakelijk zijn dat de IPv4 en IPv6 nodes van eenzelfde datastore of applicatie gebruik maken. Voorbeelden hiervan zijn een applicatielaag in een 3-tier webserveromgeving of een gezamelijke datastore in een mailomgeving.



Figuur 6.1: Gescheiden single-stack omgevingen

In het back-end is het echter mogelijk om slechts één van de IP protocollen te gebruiken. Het gehele backend kan feitelijk dus op IPv4 gebaseerd zijn, of in een later statium geheel op IPv6. Uiteraard is het in het laatste geval wel noodzakelijk dat IPv4 nodes wel IPv6 connectiviteit nodig hebben voor communicatie met het back-end. Hierbij ligt het echter meer voor de hand om alle nodes van zowel IPv4 als IPv6 connectiviteit te voorzien en gebruik te maken van een dual-stack oplossing.

Een voordeel van deze methode is dat het mogelijk is om de IPv4 productieomgeving en nieuwe IPv6 omgeving grotendeels van elkaar te scheiden. Nameservers zorgen er middels een onderscheid tussen A en AAAA [62] voor dat clients met de juiste nodes worden verbonden.

Een nadeel van dit model is het extra beheer van de gescheiden omgevingen. Daarnaast zijn er initieel extra harwareresources nodig voor het realiseren van de extra IPv6 omgeving. Echter, wij gaan er vanuit dat het gebruik van IPv4 omgekeerd evenredig zal zijn met het gebruik van IPv6, waardoor geldt:

$$ResourcesIPv6 + ResourcesIPv4 = Constant$$

Bij een stijgende populariteit van IPv6 kunnen resources dus worden omgezet van IPv4 naar IPv6. Hierbij is uiteraard geen rekening gehouden met een algemene toenemende vraag naar de aangeboden webservices, waardoor de totale benodigde hoeveelheid resources toch zal stijgen.

6.1.2 Dual-stack omgeving

Een meer ingrijpend model voor de huidige IPv4 infrastructuur is het geheel dual stack uitvoeren van de nodes die de web services verlenen. Hierbij is het noodzakelijk dat de nodes in de huidige IPv4 infrastructuur ondersteuning bieden voor IPv6. Dit geldt uiteraard ook voor de gebruikte software binnen de huidige infrastructuur.

Het voordeel van deze methode is dat er geen initiële extra hardwareresources en beheer nodig is voor een extra omgeving. Een nadeel van dit model is dat de IPv4 productieomgeving en een IPv6 experimenteeromgeving met elkaar gecombineerd zijn, en elkaar daardoor kunnen beinvloeden.

6.2 Loadbalancing

Bij grotere IT-infrastructuren zal veelal *load balancing* gebruikt worden om web services aan te bieden. In een dual-stack omgeving zijn er verschillende mogelijkheden om de IPv4 en IPv6 resources te combineren of juist zoveel mogelijk van elkaar te scheiden. De verschillende mogelijkheden worden besproken in de loadbalancing-sectie van dit document.

6.2.1 Architectuur

Er bestaan verschillende loadbalancing technieken met elk hun eigen voor- en nadelen. Ook zijn er in een gemengde IPv4/IPv6 omgeving verschillende architecturen voor het inrichten van de loadbalanced omgeving denkbaar.

Technieken

Een veel gebruikte load balancing techniek is een load balancer die functioneert als proxyserver. Bij deze techniek gaan zowel de *requests* van de clients naar de webservice als de *responses* van de webservice terug naar de client via de proxy. Het nadeel van deze methode is dat de load balancer al het verkeer moet verwerken, waardoor dit een bottleneck kan vormen.

De methode die bij uitstek geschikt is voor infrastructuren die grote hoeveelheden dataverkeer te verwerken krijgen is *direct routing* [71]. De nodes sturen hierbij de responses zonder tussenkomst van de load balancer rechtstreeks terug naar de clients. Hierdoor is dit model beter schaalbaar dan proxy-achtige methoden.

Bij direct routing komen responses binnen op de load balancer, waarna deze alleen het destination MAC adres herschrijft naar het MAC adres van een van de clusternodes. Doordat het IP adres van de afzender niet is gewijzigd zal de clusternode zijn response rechtstreeks naar de client sturen. De load balancer bewaart het client IP adres in een tabel, zodat opeenvolgende datapakketten van dezelfde client naar dezelfde clusternode worden verstuurd. Dit is voor TCP verbindingen essentieel, omdat TCP acknowledgements alleen dan steeds bij de juiste clusternode aankomen.

Een andere, simpelere, methode van loadbalancing is het gebruik van *round robin DNS*. Nadelen hiervan zijn echter dat de load balancing niet heel nauwkeurig is te regelen, en betrouwbare methoden voor failover ontbreken. In specifieke gevallen kan round robin DNS een bruikbaar alternatief zijn ten opzichte van de voorgenoemde methoden.

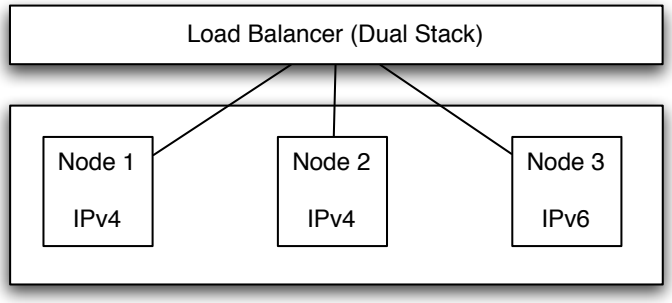
Dual-stack cluster

Een cluster is een verzameling van onafhankelijke systemen dat zich naar gebruikers presenteert als een enkel coherent systeem [58]. In een dual-stack omgeving is het dus belangrijk dat het cluster zowel IPv4 als IPv6 verbindingen kan verwerken.

Om een dual-stack cluster te realiseren is het noodzakelijk dat de load balancer als entry-point voor clients inkomende verbindingen via IPv4 en IPv6 kan verwerken. Voor de clusternodes is het niet altijd noodzakelijk dat deze dual-stack zijn uitgevoerd, en zijn er verschillende mogelijkheden.

Single-stack clusternodes Bij dit model bezit elke clusternodes slechts een enkele IP stack. Doordat er binnen het cluster een combinatie is van IPv4 en IPv6 nodes

is het cluster als geheel als dual-stack. De load balancer zorgt hierbij dus voor access transparency[58]. Figuur 6.2 geeft een schematische weergave van dit model.



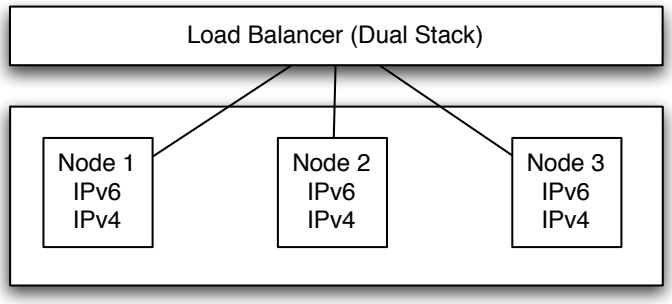
Figuur 6.2: Een dual-stack cluster bestaande uit single-stack nodes

Bij een toenemende hoeveelheid IPv6 verbindingen is het mogelijk IPv4 nodes te herconfigureren als IPv6 nodes. Vanwege het eerder besproken omgekeerd evenredige verband tussen benodigde IPv4 en IPv6 resources heeft dit model geen negatieve invloed op de totale hoeveelheid benodigde resources.

Doordat er verschillende soorten configuraties aanwezig zijn kan dit extra beheerwerkzaamheden tot gevolg hebben. Wel is de configuratie voor de nodes eenvoudiger omdat elke node slechts de configuratie van één IP-stack bezit.

Dit single-stack clusternode model is met name geschikt in situaties waarbij het wenselijk is de productie IPv4 nodes en experimentele IPv6 nodes gescheiden te houden. Daarnaast is het mogelijk dat voor bepaalde services er voor IPv4 andere software is vereist dan voor IPv6.

Dual-stack clusternodes Een andere benadering is het dual-stack uitvoeren van elke clusternode. Dit model is weergegeven in figuur 6.3.



Figuur 6.3: Een dual-stack cluster bestaande uit dual-stack nodes

Een eigenschap van dit model is dat elke clusternode een indentieke configuratie bezit.

Dit kan een postief effect hebben op de beheerkosten van het cluster.

In dit model zijn de IPv4 en IPv6 stacks zeer sterk in elkaar verweven. Een IPv4 productienode is dus tegelijkertijd een experimentele IPv6 node, wat in een testomgeving niet altijd wenselijk is.

Eventueel is het wel mogelijk om op aan bepaalde clusternodes de verwerking van IPv6 verbindingen toe te kennen, en aan de overige nodes de IPv4 verbindingen. Hierdoor onstaat in feite de single-stack omgeving, maar met het voordeel dat de configuraties voor de nodes hetzelfde blijven. Daarnaast is het hierbij mogelijk om dynamisch nodes tussen IPv4 en IPv6 te laten schakelen.

Ten slotte is ook een combinatie van dual-stack en single-stack clusternodes een alternatief. Dit maakt het mogelijk om het aantal IPv6 of dual-stack nodes binnen de huidige IPv4 omgeving langzaam uit te breiden naar een volledige dual-stack omgeving.

6.2.2 IPv6 ondersteuning

Zoals bij meer netwerkonderdelen is het mogelijk om load balancing op twee manieren te doen: met een standaard computer, uitgerust met speciale software, of met een hardware appliance. We bespreken beide opties.

Software

Veelgebruikte software voor load balancing is Linux met de Linux Virtual Server (LVS) [71] kernelopties, eventueel in combinatie met speciale software zoals keepalived [5] die controleert of de achterliggende servers correct functioneren. Helaas bieden LVS en keepalived geen ondersteuning voor IPv6. Er bestaat een patch om IPv6-ondersteuning aan LVS toe te voegen [55], echter is deze sterk verouderd.

Een optie om toch met Linux loadbalancing te doen voor generieke services is een programma met de naam *Loaded* [17]. In tegenstelling tot LVS is Loaded geen onderdeel van de Linux-kernel. Het maakt in plaats daarvan gebruik van de Netfilter-interface in samenwerking met de *QUEUE* target. Doordat LVS daar ook op inhaakt, alleen dan binnen de kernel zelf, is er wat betreft performance waarschijnlijk slechts een miniem verschil. Potentieel nadeel is dat het minder vaak gebruikt – en dus getest – wordt dan LVS. Omdat het een regulier, user-space proces is, zal dat geen invloed hebben op andere processen op dezelfde machine.

Voor het softwarematig loadbalancen van specifieke web-content bestaan er meerdere opties. Een voorbeeld is Apache2 met de *mod_balancer* module. Omdat Apache2 IPv6 goed ondersteunt, doet mod_balancer dat ook automatisch. Een andere optie is HAProxy [69]. Dit is een high-availability web proxy server met ondersteuning voor IPv6. Deze opties werken goed voor het proxyen van web content en kunnen daarbij zelfs voordelen hebben boven het gebruik van load balancers, maar zijn niet geschikt voor het load balancen van streaming content.

Hardware

Load balancers gebaseerd op standaard computers met software zijn niet in alle gevallen voldoende. In gevallen waar bijzonder veel aanvragen binnenkomen kan het beter zijn om een hardware appliance te gebruiken. Deze bieden hardware die geoptimaliseerd (of zelfs speciaal ontworpen) is voor één taak: load balancen. We bespreken enkele populaire opties.

Een van die opties is de Alteon-serie van Nortel Networks. De huidige modellen Alteon Application Switches ondersteunen load balancen op IPv6.

Een andere optie is de Big-IP serie van F5. Een interessante optie in deze producten is de beschikbaarheid van een IPv6 gatewaymodule. Deze module staat toe dat een service die nog niet voorbereid is op IPv4 toch gebruikt kan worden door IPv6 clients. Dit werkt alleen als het protocol zelf geen verwijzingen maakt naar IP-adressen.

6.3 Web services

Om web services op IPv6 aan te kunnen bieden voor internetgebruikers is het uiteraard noodzakelijk dat deze services en de bijbehorende software IPv6 ondersteuning bieden. We bekijken kort de IPv6 ondersteuning van relevante webservices.

6.3.1 Web servers

Het HyperText Transfer Protocol (HTTP) is het protocol waarmee clients (web browsers) zich toegang kunnen verschaffen tot web servers. Over het algemeen is het voor een client niet van belang op welke wijze een webpagina wordt samengesteld, of hoe de achterliggende applicaties en systemen werken.

Hetzelfde geldt met betrekking tot IPv6. Om een website beschikbaar te maken via IPv6 is het belangrijk dat de webserver ondersteuning biedt voor IPv6. Voor de gebruikte systemen in het backend is IPv6 ondersteuning niet direct noodzakelijk om de website via IPv6 ter beschikking te stellen. Voorbeelden van dergelijke achterliggende systemen zijn file-, applicatie- en databaseservers.

De Apache web server biedt volledige ondersteuning voor IPv6 sinds versie 2.0 [60]. In de configuratie is het opnemen van een 'Listen' parameter voor het IPv6 adres voldoende. Ook de lichtgewicht web server lighttpd heeft ondersteuning voor IPv6 [27]. Het inschakelen hiervan is vergelijkbaar met die Apache.

De Microsoft Internet Information Server (IIS) heeft IPv6 voor de 'core-functionaliteit' sinds IIS 6.0. Er zijn echter wel een aantal beperkingen waar rekening mee gehouden dient te worden. Met name op het gebied van SSL, beheermogelijkheden en extra services zoals FTP, SMTP, en NNTP is IPv6 ondersteuning niet of nauwelijks aanwezig [34].

6.3.2 Nameservers

Om webservices via IPv6 ter beschikking te stellen aan gebruikers in ondersteuning hiervan in het Domain Name System (DNS) essentieel. De DNS specificatie is uitgebreid met het AAAA [62] record om IPv6 adressen van hosts op te nemen.

Wat betreft de IPv6 ondersteuning van DNS serversoftware is het belangrijk om het onderscheid te maken tussen de ondersteuning van AAAA records en het daadwerkelijk kunnen verwerken van queries via IPv6 connecties.

Voor een enkele hostnaam is het mogelijk om zowel een A als een AAAA record op te nemen. Op deze manier maakt DNS het mogelijk om IPv6 verkeer naar een andere server te sturen dan IPv4 verkeer. Deze methodiek maakt de eerder besproken single-stack node methoden mogelijk.

De laatste 9.x versie van BIND (Berkeley Internet Name Domain) biedt volledige IPv6 ondersteuning [22]. Indien het onderliggende besturingssysteem IPv6 ondersteuning biedt, dan kan de BIND daemon zowel uitgaande als inkomende queries via IPv6 afhandelen. Ditzelfde geldt voor PowerDNS dat sinds versie 3.0 over volledige IPv6 ondersteuning beschikt [19].

6.3.3 Streaming

Organisaties die (live) video of audio aan eindgebruikers ter beschikking stellen maken hiervoor veelal gebruik van streaming servers. Het is dus belangrijk om de IPv6 ondersteuning van verschillende streaming servers te onderzoeken.

Windows Media Services [35] is onderdeel van de Microsoft Server besturingssystemen, en is met name populair voor het streamen van content in WMV formaat. Sinds versie 9 ondersteunt deze software IPv6, inclusief multicasting. Indien het onderliggende OS is geconfigureerd voor IPv6 zijn er voor Windows Media Server geen aanvullende configuratiewijzigingen noodzakelijk.

Quicktime Streaming server en de opensource variant Darwin Streaming server [2], beide van Apple, bieden geen ondersteuning voor IPv6. Deze software wordt veelal gebruikt voor het streamen van MPEG4 en Quicktime content.

De informatie over eventuele IPv6 ondersteuning van deze software is zeer gebrekkig, maar een korte praktijktest liet zien dat deze software niet op IPv6 adressen luistert. Als onderdeel van een researchproject van de Monash University is een alternatieve IPv6 port van het Darwin project uitgebracht [18], maar hiervan zijn sinds 2005 geen updates meer verschenen.

De streaming server Real Networks wordt uitgebracht onder de naam Helix server, en biedt IPv6 ondersteuning sinds versie 11. Wel zijn er een aantal beperkingen. Zo is er geen IPv6 ondersteuning voor SNMP, Multicasting en differentiated services [39].

Shoutcast van Winamp wordt veel gebruikt voor het streamen van MP3 streams. De meest actuele versie van shoutcast heeft geen ondersteuning voor IPv6. Een korte

praktijktest bevestigt dit. Wel is er een open source alternatief onder de naam Icecast [70], dat wel ondersteuning voor IPv6 heeft ingebouwd.

6.4 NPO Case

Voor NPO is het belangrijk om eerst te bepalen welke webdiensten via IPv6 aangeboden kunnen worden. Daarnaast kan geïnventariseerd worden welke services hiervoor in gebruik zijn en hoe IPv6 door deze services is ondersteund. Ten slotte wordt stilgestaan bij de architectuur en aandachtspunten voor de nieuwe IPv6 situatie.

6.4.1 Welke webdiensten?

NPO heeft aangegeven graag een voortrekkersrol in de adoptie van IPv6 te willen vervullen. Hiervoor is het belangrijk om een aantal services aan de buitenwereld aan te bieden waarvoor een grote belangstelling is.

Wij zijn van mening dat met name uitzendinggemist.nl met daarbij de streams van tv-uitzendingen bij het publiek de meest bekende dienstverlening is van NPO, en dat deze bij uitstek geschikt is om aan te bieden via IPv6. Hiermee wordt een enorme hoeveelheid content via IPv6 aangeboden, wat de adoptie van IPv6 ten goede kan komen.

Om een nog sterkere voortrekkersrol te vervullen is het wellicht mogelijk om via IPv6 streams op een hogere kwaliteit aan te bieden, of meer content aan te bieden dan via IPv4. Dit kan een positief effect hebben op de vraag van eindklanten naar internetaansluitingen met IPv6 connectiviteit.

6.4.2 Services

Met name web-, DNS- en streaming-servers zijn van belang voor het kunnen aanbieden van de webservices via IPv6 aan internetgebruikers.

Webservers

Binnen NPO worden Apache en lighttpd gebruikt als webservers voor de verschillende websites en webapplicaties. Van beide producten zijn reeds de laatste versies in gebruik, dus de IPv6 ondersteuning is hiervoor al aanwezig. Nadat de onderliggende besturingssystemen zijn voorzien van IPv6 adressen is het inschakelen van de ondersteuning voor de webservers dus eenvoudig.

DNS

De laatste versie van BIND is momenteel in gebruik binnen NPO. Zoals vermeld biedt deze de gewenste IPv6 ondersteuning indien het onderliggende besturingssysteem hiervoor geconfigureerd is.

Streaming

In de huidige architectuur zijn er voor de on-demand en live streams clusters aanwezig op basis van Windows Media Services 9. Het cluster wordt gevormd door een load balancer op basis van LVS geconfigureerd via het direct routing model. De clusternodes zijn Windows Server 2003 systemen.

Wat betreft streaming zijn de Windows Media Services 9 klaar voor gebruik met IPv6. De meeste content wordt bij NPO verspreid in WMV formaat, dus hiermee is het grootste gedeelte van de content beschikbaar te maken via IPv6. Zoals aangegeven, is IPv6 loadbalancing met LVS niet zonder meer mogelijk. Dit aspect wordt verderop besproken.

Shoutcast is momenteel in gebruik voor het uitzenden van een aantal radio streams. Ook hiervoor worden meerdere systemen in een LVS cluster gebruikt. Zoals is aangegeven is Shoutcast niet IPv6 compatible. Om alsnog radiostreams op een vergelijkbare manier te verspreiden kan een overstap op Icecast worden overwogen. Daarnaast is dezelfde problematiek van toepassing met betrekking tot de load balacing.

Indien er in de toekomst gekozen wordt voor het streamen met Darwin / Quicktime Streaming Server is het belangrijk rekening te houden met het ontbreken van IPv6 ondersteuning in dit pakket.

StreamGate

StreamGate [15] is een dienst van Dutchview waarbij streamingplatforms van aangesloten providers worden aangewend voor het ontlasten van het streamingplatform van contentaanbieders. Ook NPO maakt hiervan gebruik voor haar livestreams.

De techniek achter StreamGate is eenvoudig: NPO stuurt de beschikbare streams één keer naar de streamingplatforms van de deelnemende ISP's. Zodra een gebruiker een stream opvraagt, komt hij eerst bij de zogenoemde StreamSwitch server terecht. De StreamSwitch server stuurt de gebruiker middels een eenvoudige redirect naar het streamingplatform van de ISP van deze gebruiker. Indien de ISP niet deelneemt aan StreamGate, dan wordt de gebruiker rechtstreeks geforward naar het streamingplatform van de content provider.

Doordat de redirects werken op basis van *URL's* is IPv6 ondersteuning van het StreamGate platform niet direct vereist. Om een uiteindelijke volledige overstap naar IPv6 te maken is dat uiteraard wel een vereiste.

Het is wel wenselijk dat ISP's die IPv6 connectiviteit aan eindklanten aanbieden zoals Bit en Surfnet hiervoor hun streamingplatform IPv6 compatibel maken, indien dat nog niet het geval is. NPO zou hier een rol in kunnen vervullen door in overleg te gaan met de verschillende ISP's die IPv6 connectiviteit aanbieden. De deelnemende providers zijn op dit moment:

- Xs4all
- Tiscali
- Versatel
- Surfnet
- Kpn
- Wanadoo
- @home
- BIT

6.4.3 Gewenste Situatie IPv6

Naast het de IPv6 ondersteuning van gebruikte software is het ook belang de architectuur waarop de IPv6 diensten aangeboden worden in beschouwing te nemen.

Architectuur

Ten aanzien van de architectuur zijn er, zoals beschreven, verschillende mogelijkheden. Tijdens de invoering van IPv6 worden vanzelfsprekend verschillende fases doorlopen, waarbij voor elke fase een andere architectuur passend is.

Voordat IPv6 daadwerkelijk in de productieomgeving wordt toegepast is het nuttig om dit eerst binnen een experimentele omgeving te testen. Belangrijk hierbij is dat de testomgeving geen invloed kan uitoefenen op de productiesystemen. Hiervoor is de eerder beschreven single-stack oplossing met een gescheiden IPv4 en IPv6 omgevingen bij uitstek geschikt.

Zodra de IPv6 configuratie als productieklaar kan worden beschouwd, is het mogelijk IPv6 gefaseerd binnen de verschillende clusters te introduceren. Hierbij is een eerste vereiste dat er IPv6 ondersteuning op de loadbalancers aanwezig is. De verschillende mogelijkheden voor loadbalancing dit te realiseren zijn verderop beschreven.

Een tussenstap is het inbrengen van één dual stack node binnen het cluster. Hierbij is het niet direct noodzakelijk dat de load balancer IPv6 ondersteuning biedt, aangezien het met één node niet vereist is de binnenkomende verzoeken via de load balancer te routeren.

De volgende stap is het introduceren van één dual-stack configuratie voor alle clusternodes. Dit heeft als voordeel dat alle nodes in het cluster dezelfde configuratie gebruiken, waardoor de beheerwerkzaamheden beperkt blijven.

Een eventuele tussenstap is het inschakelen van IPv6 op slechts een beperkt aantal machines. Indien dit goed blijkt te functioneren kan IPv6 op alle machines worden ingeschakeld, waarna alle clusternodes zowel IPv4 als IPv6 connecties kunnen verwerken.

Het is ook mogelijk om een specifieke set clusternodes de IPv4 connecties, en de overige nodes de IPv6 connecties af te laten handelen. Behalve een duidelijke scheiding tussen de machines die IPv4 en IPv6 afhandelen heeft dit niet direct een duidelijk voordeel.

Load Balancing

Gezien de affiniteit van NPO met Open Source Software lijkt het een logische stap om dat ook te doen voor de behoeftes betreffende loadbalancing. Echter maakt NPO voor IPv4 gebruik van LVS, dat nog geen IPv6 ondersteunt.

Ontwikkeling van LVS stimuleren Dit kan wellicht opgelost worden door financiele ondersteuning te bieden voor het ontwikkelen van IPv6-ondersteuning. NPO zou een (freelance) programmeur aan kunnen nemen om deze ondersteuning te implementeren en de resultaten contribueren aan het LVS-project. Ook is het bieden van financiele steun aan het LVS ontwikkelteam wellicht een mogelijkheid. Afhankelijk van de hoeveelheid werk kan dit echter lang duren en daarmee veel geld kosten.

Loaded Op kortere termijn kan gebruik gemaakt worden van loaded. Aangezien loaded geen onderdeel is van de Linux-kernel en slechts opereert op packets die door de netfilter queue aangereikt worden zal het gebruik ervan geen invloed hebben op de IPv4-loadbalancing of services, zelfs indien de software zou crashen. Loaded kan dus naast de huidige LVS kernel modules op dezelfde loadbalancing systemen in gebruik genomen worden. Dat maakt het uitermate geschikt voor een initiële testuitrol naast IPv4.

Hardware Enkele medewerkers van NPO maken zich zorgen dat de LVS load balancers op korte termijn niet meer genoeg performance bieden voor de groeiende hoeveelheid netwerkverkeer. Het kan dus ook zeer de moeite waard zijn om te onderzoeken of een op hardware gebaseerde load balancer meer performance biedt. Zoals eerder beschreven is de Alteon-serie van Nortel daarbij een goede keus gezien de ondersteuning van IPv6. Het gebruik van hardware load balancers brengt wellicht meer kosten met zich mee dan het stimuleren van de ontwikkeling van IPv6-ondersteuning in LVS.

Vervolgonderzoek

Gezien de beperkte beschikbare tijd voor dit onderzoek hebben wij ons gericht op een aantal specifieke punten. Voor een volledige organisatiebrede implementatie van IPv6 is nog aanvullend onderzoek noodzakelijk. We noemen hier twee concrete punten waarvoor verder onderzoek gewenst is.

7.1 Back-end

In ons onderzoek is met name het aanbieden van IPv6 diensten aan de 'internet-kant' besproken. Hiervoor is het niet direct noodzakelijk dat ook de back-ends van de verschillende websites en webapplicaties IPv6 ondersteunen. Bij een volledige overstap op IPv6 is het waarschijnlijk gewenst om ook de back-end systemen naar IPv6 te migreren.

In een vervolgonderzoek kan de IPv6 ondersteuning van de verschillende back-end services zoals databases en fileservers onderzocht worden. Daarnaast is het ook belangrijk om te bestuderen of er consequenties zijn voor veschillende intern ontwikkelde applicaties bij een overstap naar IPv6.

7.2 Kantoorautomatisering

Het aanbieden van IPv6 binnnen de kantoorautomatisering kan vrij complex zijn. Hiervoor moet onderzocht worden op welke wijze een overschakeling van IPv4 only, naar dual-stack, en uiteindelijk naar IPv6 only gerealiseerd kan worden.

Voor het toekennen van IPv6 adressen aan client systemen is IPv6 stateless address autoconfiguration [63] ontwikkeld. Doordat het autoconfiguration adres gebaseerd is op het MAC adres van de client machine, wordt hierdoor een stukje privacy van gebruikers ingeleverd. Een mogelijke oplossing hiervoor zijn de privacy extensions voor stateless autoconfiguration [37]. Hierbij genereren clients met een bepaald interval een random IPv6 adres. Hierbij zijn IP adressen echter weer uitermate slecht terug te leiden naar clients, wat ook weer ongewenst kan zijn uit beheer- en security-oogpunt.

Een heel ander nadeel van autoconfiguration is dat er geen aanvullende parameters zoals een DNS server mee zijn te geven naar de client systemen. Zolang er sprake is van een dual-stack omgeving kan de client de IPv4 DNS servers die via DHCP zijn verkregen gebruiken. Bij een volledige overstap naar IPv6 geeft dit echter wel een probleem. Als oplossing hiervoor is DHCPv6 [13] bedacht, echter is de ondersteuning hiervan in besturingssystemen zoals Windows en OS X nog niet aanwezig.

Ook is het belangrijk om te onderzoeken in hoeverre verschillende client applicaties IPv6 ondersteuning bieden voordat een overstap op IPv6 wordt overwogen.

Waarschijnlijk is ook een gedeeltelijke implementatie van IPv6 in de kantoorautomatisering noodzakelijk voordat NPO webdiensten aanbied via IPv6. Het zal voor systeembeheerders en ander personeel binnen NPO namelijk gewenst zijn om de via IPv6 aangeboden diensten te kunnen benaderen via IPv6 vanuit het interne netwerk. Als tussenoplossing hiervoor kan bijvoorbeeld het gebruik van 6to4 tunnels [4] worden overwogen.

Ten slotte is het belangrijk dat bij een overstap op IPv6 er voldoende kennis aanwezig is bij het beheer- en helpdeskpersoneel. Hoe een en ander het beste vormgegeven kan worden kan in een vervolgonderzoek worden onderzocht.

Conclusie

Naar onze mening is het in gebruik nemen van IPv6 door NPO zeker mogelijk. Het aanvragen van provideronafhankelijke IPv6 adresruimte via RIPE is zonder problemen mogelijk. Daarnaast is ook het gereed maken van de netwerkcore zonder problemen te realiseren. Ook het daadwerkelijk aanbieden van een aantal diensten via IPv6 is volgens ons haalbaar. Hiervoor moeten echter wel een aantal aandachtspunten meegenomen worden.

IPv6 Load balancing Op dit moment is het aanbod aan hardware en software dat op een generieke manier applicaties kan loadbalancen nog gering. Echter, dat geldt ook voor de hoeveelheid verkeer op IPv6.

Dit houdt dus in dat een gebrek aan loadbalancing voor IPv6 diensten in een experimentele fase geen probleem zal vormen. Wel is het verstandig om een high-availability failover opstelling te gebruiken zodat voor een op IPv6 aangeboden dienst wel een hoge beschikbaarheid is te garanderen. In een uiteindelijke productieomgeving is IPv6 loadbalancing wel een vereiste.

Streaming Ons onderzoek heeft uitgewezen met name op het gebied van streaming veel software nog geen IPv6 ondersteuning biedt. Windows Media services, dat ook door NPO in gebruik is, biedt wel goede IPv6 ondersteuning. Indien er in de toekomst het gebruik van andere streamingsoftare wordt overwogen, is het zinnig de IPv6 ondersteuning van de software in beschouwing te nemen.

Extra beheer Bij elke extra dienst komt extra beheer kijken. Dat geldt ook voor IPv6. Op systeemniveau verandert er weinig: eenmalig een extra IP-adres invoeren en, in bepaalde gevallen, IPv6-ondersteuning aanzetten is voldoende. Echter, op netwerkniveau houdt het in dat er meer subnetten moeten worden verdeeld, minimaal één extra routing protocol moet worden gebruikt en dat extra peerings opgezet moeten worden om verkeer zo snel en goedkoop mogelijk op de plaats van bestemming te krijgen.

De voortrekkersrol die NPO op het gebied van IPv6 nastreeft is naar onze mening zeker haalbaar. Met name uitzendinggemist.nl geniet een grote bekendheid onder het Nederlandse publiek. Door deze site inclusief de achterliggende on-demand streams op IPv6 aan te bieden, wordt er een grote hoeveelheid content beschikbaar gemaakt. Dit kan ervoor zorgen dat er een grotere vraag ontstaat naar IPv6 connectiviteit bij internetaansluitingen voor thuisgebruikers. Dit zal zeker het geval zijn als NPO kiest om extra of hogere kwaliteit content uitsluitend beschikbaar te stellen via IPv6.

In de toekomst kan IPv6 voor NPO met name op het vlak van streaming voor voorde-

len zorgen. Via IPv6 zal het door het ontbreken van NAT eenvoudiger mogelijk zijn om gebruik te maken van meer efficiente UDP streams.

Voor het aanbieden van IPv6 voor kantoorautomatisering en het gebruik van IPv6 binnen de back-end systemen is aanvullend onderzoek noodzakelijk.

Dankwoord

Wij willen graag onze dank uit laten gaan naar de medewerkers van NPO voor hun gastvrijheid en hulp bij ons onderzoek. In het bijzonder daarbij onze twee begeleiders Ed van Vuuren en Dirk-Jan van Helmond die ons evenals Jeroen Vos en Jeroen Zwarts voorzien hebben van het antwoord op bijna al onze vragen. Buiten hen willen wij graag ook de andere medewerkers bedanken die elk een deel van hun tijd aan ons hebben afgestaan voor het beantwoorden van vragen, genereren van ideeën, etc.

Overzicht IPv6 peers

De volgende 45 autonome systemen zijn aangemerkt als potentieële IPv6 peeringpartners voor NPO.

- ALTECOM (AS16030)
- ASN-BICS (AS6774)
- CLARANET-AS (AS8426)
- DUOCAST-AS (AS31477)
- EASYNET (AS4589)
- ENTANET (AS8468)
- EUNET-FINLAND (AS6667)
- FINECOM (AS15600)
- FREENETDE (AS5430)
- GRAFIX-IS (AS16131)
- HWNG (AS12989)
- INIT7 (AS13030)
- InterNLnet (AS20507)
- KABELFOON (AS15435)
- KPN (AS286)
- K-ROOT-SERVER (AS25152)
- LAMBDANET-AS (AS13237)
- LDCOMNET (AS15557)
- LeaseWeb (AS16265)
- LINK11 (AS34309)
- LINXTELECOM (AS3327)
- MULTIPLAY (AS35028)
- NEDERLANDNET-AS (AS31383)
- NETCOLOGNE (AS8422)

- NL-BIT (AS12859)
- NL-CONCEPTS (AS12871)
- OBIT-AS (AS8492)
- ON-AS (AS34419)
- OPENCARRIER-AS (AS41692)
- RDSNET (AS8708)
- RIPE-NCC-RIS-AS (AS12654)
- SCAN-PLUS-AS (AS12399)
- SCARLET (AS12634)
- SIG (AS20932)
- SURFNET-NL (AS1103)
- SWISSCOM (AS3303)
- TDC (AS3292)
- TELEKOM-AT (AS8447)
- TELENOR-NEXTEL (AS2119)
- TIC (AS1836)
- UNILOGICNET-AS (AS28788)
- UPC (AS6830)
- VIRGINRADIO (AS34763)
- WIKIMEDIA-EU (AS43821)
- XS4ALL-NL (AS3265)

Werkwijze

Om tot deze lijst te komen hebben we de volgende werkwijze gebruikt (shell commando's):

```
# Whois informatie NPO ophalen
whois -h whois.ripe.net AS25182 > npo-whois.txt

# Lijst met ASNs peering partners samenstellen
awk '/^import:/ {print $3}' npo-whois.txt | sort | \
 uniq > npo-peers.txt
```

```
# Route6 attributen van ASNs opvragen
cat npo-peers.txt | while read line; do whois -h \
 whois.ripe.net -T route6 -i origin "${line}"; \
 done > temp.txt

# Lijst ASNs potentiele IPv6 peerings samenstallen
awk '/^origin/ {print $2}' temp.txt | sort | \
 uniq > ipv6-peers.txt

# AS names potentiele IPv6 peerings opvragen
cat ipv6-peers.txt | while read line; do whois -h \
 whois.ripe.net -T aut-num "${line}"; done > temp3.txt
awk '/^as-name/ {print $2}' temp3.txt > \
 ipv6-as-names.txt

# Lijst ASN en AS names samenvoegen
paste -d , ipv6-as-names.txt ipv6-peers.txt | \
 sort > ipv6-peerinfo.txt
```

Bibliografie

[1] B. Aboba and W. Dixon. IPsec-Network Address Translation (NAT) Compatibility Requirements. RFC 3715 (Informational), Mar. 2004. Available from: http://www.ietf.org/rfc/rfc3715.txt.

[2] Apple Inc. Darwin Streaming Server [online]. 2007. Available from: http://dss.macosforge.org/ [cited 30 januari 2008].

[3] S. Bradner and A. Mankin. The Recommendation for the IP Next Generation Protocol. RFC 1752 (Proposed Standard), Jan. 1995. Available from: http://www.ietf.org/rfc/rfc1752.txt.

[4] B. Carpenter and K. Moore. Connection of IPv6 Domains via IPv4 Clouds. RFC 3056 (Proposed Standard), Feb. 2001. Available from: http://www.ietf.org/rfc/rfc3056.txt.

[5] A. Cassen. Keepalived for Linux [online]. Sept. 2007. Available from: http://www.keepalived.org/ [cited 29 januari 2008].

[6] Checkpoint Software. Check Point First To Secure IPv6, Peer-To-Peer, Instant Messaging Applications And Microsoft File Sharing And Print Services [online]. Available from: http://www.checkpoint.com/press/2002/ipv6_081402.html.

[7] Cisco Systems. Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide [online]. Available from: http://www.cisco.com/en/US/docs/security/fwsm/fwsm31/configuration/guide/ipv6_f.html.

[8] Cisco Systems. Implementing Multi-protocol BGP [online]. Available from: http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_c/sa_bgpv6.htm.

[9] Cisco Systems. Implementing OSPF form IPv6 [online]. Available from: http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_c/sa_ospf3.htm.

[10] Cisco Systems. What's New in Cisco PIX Firewall 7.0 [online]. Available from: http://www.ciscopress.com/articles/article.asp?p=379751.

[11] R. Coltun, D. Ferguson, and J. Moy. OSPF for IPv6. RFC 2740 (Proposed Standard), Dec. 1999. Available from: http://www.ietf.org/rfc/rfc2740.txt.

[12] S. Deering and R. Hinden. Internet Protocol, Version 6 (IPv6) Specification. RFC 2460 (Draft Standard), Dec. 1998. Updated by RFC 5095. Available from: http://www.ietf.org/rfc/rfc2460.txt.

[13] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, and M. Carney. Dynamic Host Configuration Protocol for IPv6 (DHCPv6). RFC 3315 (Proposed Standard), July 2003. Updated by RFC 4361. Available from: http://www.ietf.org/rfc/rfc3315.txt.

[14] A. Durand and C. Huitema. The H-Density Ratio for Address Assignment Efficiency An Update on the H ratio. RFC 3194 (Informational), Nov. 2001. Available from: http://www.ietf.org/rfc/rfc3194.txt.

[15] Dutchview Webcasting. Streamgate [online]. 2008. Available from: http://www.dutchview.nl/69/webcasting/streamgate/ [cited 31 januari 2008].

[16] Federal CIO Council Architecture and Infrastructure Committee. IPv6 Transition Guidance [online]. Feb. 2006. Available from: http://www.cio.gov/documents/IPv6_Transition_Guidance.doc [cited 25 januari 2008].

[17] S. Friedrich, S. Krahmer, L. Schneidenbach, and B. Schnor. *Loaded: Server Load Balancing for IPv6*. IEEE Computer Society, 2006. Available from: http://doi.ieeecomputersociety.org/10.1109/ICNS.2006.71.

[18] D. Grimm. QuickTime/Darwin/MPEG4 Streaming Server IPv6 Support project [online]. 2005. Available from: http://www.ctie.monash.edu.au/DSS-IPv6/ [cited 30 januari 2008].

[19] B. Hubert. PowerDNS [online]. 2007. Available from: http://www.powerdns.com/ [cited 30 januari 2008].

[20] G. Huston. IPv4 Address Report [online]. Jan. 2008. Available from: http://www.potaroo.net/tools/ipv4/index.html [cited 25 januari 2008].

[21] IAB and IESG. IAB/IESG Recommendations on IPv6 Address Allocations to Sites. RFC 3177 (Informational), Sept. 2001. Available from: http://www.ietf.org/rfc/rfc3177.txt.

[22] Internet Systems Consortium, Inc. BIND (Berkeley Internet Name Domain) [online]. 2008. Available from: http://www.isc.org/index.pl?/sw/bind/index.php [cited 30 januari 2008].

[23] Juniper Networks. Juniper Networks NetScreen ScreenOS 5.0 IPv6 [online]. Available from: http://cn.juniper.net/products/integrated/dsheet/110028.pdf.

[24] D. Kalogeras. Open Shortest Path First v3 [online]. Available from: http://www.6diss.org/workshops/see-2/routing-internal.pdf.

[25] S. Kent and R. Atkinson. IP Authentication Header. RFC 2402 (Proposed Standard), Nov. 1998. Obsoleted by RFCs 4302, 4305. Available from: http://www.ietf.org/rfc/rfc2402.txt.

[26] S. Kent and R. Atkinson. Security Architecture for the Internet Protocol. RFC 2401 (Proposed Standard), Nov. 1998. Obsoleted by RFC 4301, updated by RFC 3168. Available from: http://www.ietf.org/rfc/rfc2401.txt.

[27] J. Kneschke. lighttpd [online]. 2008. Available from: http://www.lighttpd.net/ [cited 30 januari 2008].

[28] K. Lindqvist and G. Huston. RIPE Policy Proposal 2005-08 [online]. Oct. 2005. Available from: http://www.ripe.net/ripe/policies/proposals/2005-08.html [cited 23 januari 2008].

[29] G. Malkin. RIP Version 2. RFC 2453 (Standard), Nov. 1998. Updated by RFC 4822. Available from: http://www.ietf.org/rfc/rfc2453.txt.

[30] G. Malkin and R. Minnear. RIPng for IPv6. RFC 2080 (Proposed Standard), Jan. 1997. Available from: http://www.ietf.org/rfc/rfc2080.txt.

[31] P. Marques and F. Dupont. Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing. RFC 2545 (Proposed Standard), Mar. 1999. Available from: http://www.ietf.org/rfc/rfc2545.txt.

[32] J. P. Martinez. IPv6 Address Allocation and Assignment Policy [online]. Apr. 2007. Available from: http://www.ripe.net/ripe/policies/proposals/2006-02.html [cited 23 januari 2008].

[33] Microsoft. Windows Firewall in Windows Server 2003 Service Pack 1 [online]. Available from: http://technet2.microsoft.com/windowsserver/en/library/5961045b-146e-48cf-98d2-0bd43c9862771033.mspx?mfr=true.

[34] Microsoft. IPv6 and IIS 6.0 [online]. 2003. Available from: http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/4c7c6bce-213a-4125-bc36-2202e3b4c8c8.mspx [cited 28 januari 2008].

[35] Microsoft Corporation. Windows Media Services [online]. 2007. Available from: http://www.microsoft.com/windows/windowsmedia/forpros/server/server.aspx [cited 30 januari 2008].

[36] J. Moy. OSPF Version 2. RFC 2328 (Standard), Apr. 1998. Available from: http://www.ietf.org/rfc/rfc2328.txt.

[37] T. Narten and R. Draves. Privacy Extensions for Stateless Address Autoconfiguration in IPv6. RFC 3041 (Proposed Standard), Jan. 2001. Obsoleted by RFC 4941. Available from: http://www.ietf.org/rfc/rfc3041.txt.

[38] J. Postel. Internet Protocol. RFC 791 (Standard), Sept. 1981. Updated by RFC 1349. Available from: http://www.ietf.org/rfc/rfc791.txt.

[39] RealNetworks, Inc. Helix Server Administration Guide [online]. Sept. 2005. Available from: http://service.real.com/help/library/guides/HelixServerWireline/wwhelp/wwhimpl/java/html/wwhelp.htm [cited 30 januari 2008].

[40] Y. Rekhter and T. Li. A Border Gateway Protocol 4 (BGP-4). RFC 1771 (Draft Standard), Mar. 1995. Obsoleted by RFC 4271. Available from: http://www.ietf.org/rfc/rfc1771.txt.

[41] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, and E. Lear. Address Allocation for Private Internets. RFC 1918 (Best Current Practice), Feb. 1996. Available from: http://www.ietf.org/rfc/rfc1918.txt.

[42] RIPE. ripe-388 IPv6 Address Allocation and Assignment Policy [online]. Sept. 2006. Available from: http://www.ripe.net/ripe/docs/ripe-388.html [cited 23 januari 2008].

[43] RIPE. ripe-412 IPv6 Address Allocation and Assignment Policy [online]. July 2007. Available from: http://www.ripe.net/ripe/docs/ripe-412.html [cited 23 januari 2008].

[44] RIPE. ripe-420 RIPE NCC Charging Scheme 2008 [online]. Nov. 2007. Available from: http://www.ripe.net/ripe/docs/ripe-420.html [cited 23 januari 2008].

[45] RIPE. ripe-421 IPv6 Address Allocation and Assignment Policy [online]. nov 2007. Available from: http://www.ripe.net/ripe/docs/ripe-421.html [cited 23 januari 2008].

[46] RIPE. ripe-422 Supporting Notes for the IPv6 First Allocation Request Form [online]. Nov. 2007. Available from: http://www.ripe.net/ripe/docs/ripe-422.html [cited 23 januari 2008].

[47] RIPE. ripe-425 IPv6 First Allocation Request Form [online]. Nov. 2007. Available from: http://www.ripe.net/ripe/docs/ripe-425.html [cited 23 januari 2008].

[48] RIPE. RIPE Community Resolution on IPv4 Depletion and Deployment of IPv6 [online]. Oct. 2007. Available from: http://www.ripe.net/news/community-statement.html [cited 25 januari 2008].

[49] RIPE NCC. Assignment Window How-To [online]. Available from: http://www.ripe.net/rs/ipv4/aw.html.

[50] RIPE NCC. RIPE NCC General Meeting October 2006 Minutes [online]. Oct. 2006. Available from: http://www.ripe.net/membership/gm/gm-october2006/minutes.html [cited 23 januari 2008].

[51] RIPE NCC. Becoming a Member [online]. Aug. 2007. Available from: http://www.ripe.net/info/faq/membership/newlir-setup.html [cited 23 januari 2008].

[52] RIPE NCC. Reverse Delegation How To [online]. Sept. 2007. Available from: http://www.ripe.net/rs/reverse/reverse_howto.html [cited 23 januari 2008].

[53] RIPE NCC. RIPE NCC Billing Procedure and Fee Schedule 2008 [online]. Oct. 2007. Available from: http://www.ripe.net/membership/billing/procedure.html [cited 23 januari 2008].

[54] Sean Murray-Ford. IPv6 How-To [online]. Available from: http://www.nokia.com/NOKIA_COM_1/About_Nokia/Press/White_Papers/pdf_files/techwhitepaper_ipv6_howto.pdf.

[55] Seiji Tsuchiike. Linux Virtual Server for IPv6 [online]. Available from: http://www.yggr-drasill.com/LVS6/.

[56] SixXS. SixXS FAQ [online]. Available from: http://www.sixxs.net/faq/connectivity/?faq=ipv6transit.

[57] P. Srisuresh and M. Holdrege. IP Network Address Translator (NAT) Terminology and Considerations. RFC 2663 (Informational), Aug. 1999. Available from: http://www.ietf.org/rfc/rfc2663.txt.

[58] A. S. Tanenbaum and M. van Steen. *Distributed systems: principles and paradigms*. Pearson Education, 2006.

[59] R. Thayer, N. Doraswamy, and R. Glenn. IP Security Document Roadmap. RFC 2411 (Informational), Nov. 1998. Available from: http://www.ietf.org/rfc/rfc2411.txt.

[60] The Apache Software Foundation. Apache HTTP Server project [online]. 2008. Available from: http://httpd.apache.org/ [cited 30 januari 2008].

[61] S. A. Thomas. *IP Switching and Routing Essentials*. Wiley, Jan. 2002.

[62] S. Thomson and C. Huitema. DNS Extensions to support IP version 6. RFC 1886 (Proposed Standard), Dec. 1995. Obsoleted by RFC 3596, updated by RFCs 2874, 3152. Available from: http://www.ietf.org/rfc/rfc1886.txt.

[63] S. Thomson and T. Narten. IPv6 Stateless Address Autoconfiguration. RFC 2462 (Draft Standard), Dec. 1998. Obsoleted by RFC 4862. Available from: http://www.ietf.org/rfc/rfc2462.txt.

[64] M. Tulloch. IPv6 Support in Microsoft Windows [online]. Available from: http://www.windowsnetworking.com/articles_tutorials/IPv6-Support-Microsoft-Windows.html.

[65] I. van Beijnum. *Running IPv6*. Apress, 2006.

[66] I. van Beijnum. 2007 IPv4 Address Use Report [online]. Jan. 2008. Available from: http://www.bgpexpert.com/addrspace2007.php [cited 25 januari 2008].

[67] A. Vijn. IPv6 at AMS-IX [online]. Available from: http://www.ams-ix.net/more/aiad/IPv6atAMS-IX.pdf.

[68] Wikipedia. Routing Information Protocol [online]. Available from: http://en.wikipedia.org/wiki/Routing_Information_Protocol.

[69] Willy Tarreau. HAProxy - The Reliable, High-Performance TCP/HTTP Load Balancer [online]. Available from: http://haproxy.1wt.eu/.

[70] Xiph open source community. Icecast.org [online]. 2008. Available from: http://www.icecast.org/ [cited 30 januari 2008].

[71] W. Zhang. Linux Virtual Server for Scalable Network Services [online]. 2000. Available from: http://www.linuxvirtualserver.org/ols/lvs.pdf [cited 28 januari 2008].