IPv6

De eerste echte stappen

Afstudeerverslag

Auteur: Vincent Verheijen
Datum: 12-03-2012
Plaats: Eindhoven
Versie: 1.0

Gegevens student(e)

Naam + voorletters student:	Vincent A. L. Verheijen
Studentnummer:	2107605
Opleiding:	Informatica Voltijd (afstudeerrichting IMS)
Stageperiode datum:	Van 15-08-2011 t/m 31-01-2012

Gegevens bedrijf

Naam bedrijf/instelling:	Simac ICT Nederland
Afdeling:	O&E Network Engineering
Plaats:	Veldhoven
Naam + voorletters bedrijfsbegeleiders:	N. van der Steen
Functie bedrijfsbegeleider:	manager

Gegevens docentbegeleider

Naam + voorletters docentbegeleider:	P. van den Broek

Wijzigingshistorie

Versie	Datum	Wijzigingen
0.1	1-10-2011	Eerste opzet verslag
0.2	5-3-2012	Toevoegen Bijlagen
0.2.5	15-3-2012	Verbeteringen na feedback
0.3	22-3-2012	Complete tekst minus samenvatting
0.4	25-3-2012	Tekst compleet
0.6	26-3-2012	Spelcheck door derde en afwerking
1.0	27-3-2012	Final na feedback bedrijfsbegeleider

Voorwoord

Deze Scriptie is gemaakt tijdens en na mijn afstudeer stage voor de opleiding ICT Management en Security aan de Fontys Hogeschool ICT.

De afstudeeropdracht is uitgevoerd bij Simac ICT Nederland, een ICT dienstverlener en automatiseerder. Deze scriptie beschrijft het door mij doorlopen afstudeerproces en het product wat daaruit is voortgekomen.

De afstudeer opdracht bestond uit het bestuderen van en advies uitbrengen over technieken om IPv6 te implementeren voor web services en werknemers connectiviteit, even als het onderzoeken van de mogelijkheden voor het verkrijgen van een IPv6 internetverbinding en mogelijke alternatieven mocht dat niet mogelijk zijn.

Graag wil ik de volgende personen bedanken voor hun bijdragen:

- Dhr van den Broek, docentbegeleider tijdens de afstudeerperiode, voor de inspiratie en uiteenzetting van wat een goede stage periode in houdt.
- Dhr Luc Aelen en dhr Tom van Haandel, bedrijfsbegeleiders, voor de goede samenwerking en hun kritische doch rechtvaardige blik op mijn werk.
- Dhr van der Steen, voor het geven van de kans om mijn afstudeerstage bij Simac te lopen.
- De collega’s van Simac voor hun prettige samenwerking en hun bereidheid om mijn vragen te beantwoorden.

Inhoudsopgave

Samenvatting

De afstudeerperiode die in deze scriptie wordt beschreven is door Vincent Verheijen uitgevoerd bij Simac ICT Nederland in Veldhoven, een automatiseerder en ICT dienstverlener met namen gericht op het midden en groot bedrijf.

De 3.7 miljard IPv4 adressen op internet zijn op. In 2012 al zullen in Europa Alle IPv4 adressen zijn verdeeld over ISP's en bedrijven. Het zal dan niet meer mogelijk zijn voor bedrijven of ISP's om meer adressen aan te vragen. De opvolger van IPv4 staat al klaar in de vorm van IPv6. IPv6 beidt ruimte voor $3{,}4 \times 10^{38}$ adressen. Een nagenoeg onuitputtelijke voorraad. Maar IPv6 en IPv4 kunnen niet rechtstreeks met elkaar communiceren. En de omschakeling naar IPv6 zal niet in een keer gebeuren. Dus wat is de beste manier om deze overgang aan te pakken? Wat moet er gebeuren?

Als ICT dienstverlener is het Simac's taak om op deze vragen een antwoord te hebben nog voor de klant ze nodig heeft. De eerste vragen die gesteld gaan worden zijn: Hoe zorgen we er voor dat onze website via IPv6 bereikbaar is, en hoe zorgen we er voor dat onze werknemers IPv6-only websites kunnen bekijken? En om dat mogelijk te maken, hoe zorgen we voor een IPv6-enabled internet verbinding?

De afstudeer opdracht was het vinden van de antwoorden die deze vragen op een zo eenvoudige, goedkope en veilige manier oplosten en dat in een rapport te verwerken (bijlage E)

In het vooronderzoek is naar zo veel mogelijk transitie technieken gezocht (technieken die ontwikkeld zijn voor de overgang van IPv4 naar IPv6) waarna geïnventariseerd is hoe ze werken en of ze geschikt zijn voor een of meer van de onderzoeksvragen en voor het Simac netwerk. Voor elke van de 3 onderzoeksvragen zijn daar 2 of 3 bruikbare technieken uitgekomen die nader onderzocht zullen worden in de onderzoeksfase. Deze zijn Dual stack, Stateful NAT64 en translating-proxy. Tunneling en 6to4 worden onderzocht als alternatieven voor een native IPV6 internet verbinding.

In de onderzoeksfase zijn deze uitgekozen technieken nader onderzocht. Eerst op de voor en nadelen van elk in the algemeen los van precieze de toepassingen en daarna specifiek per onderzoeksvraag. Daar is een lijst met de voor- en nadelen uit gekomen voor elke techniek bij elk van de onderzoeksvragen.

Met deze gegevens is vervolgens per onderzoeksvraag advies uitgebracht over de beste techniek om te gebruiken. In het ideale geval is dual stack de beste oplossing met veruit de meeste toekomstbestendigheid, maar de implementatie ervan heeft een grote impact en moet met zorg worden voorbereid. NAT64 en een translating proxy zijn echter snel te implementeren en hebben een lage impact, maar zijn niet toekomstbestendig.

Zolang er nog geen haast bij is, is dual stack de beste optie. Maar begin hier wel zo snel mogelijk mee. Hoe eerder er mee begonnen wordt hoe lager de kosten uitvallen omdat de tijd ervoor genomen kan worden. En zelfs als een klant nog geen IPv6 wil gaan gebruiken de komende paar jaar, houdt er nu al rekening mee in het inkoopbeleid en zorg voor IPv6 ondersteuning in zo veel mogelijk hardware en software. Dit voorkomt extra kosten en maakt een overgang eenvoudiger.

Summery

The internship described in this thesis was carried out by Vincent Verheijen at the company Simac located in Veldhoven, A ICT service provider whose focus is medium to large businesses.

The 3.7 billion IPv4 addresses on the internet have been exhausted. In 2012 Europe will have divided all of its available addresses among Its ISP's and companies. From then on it will no longer be possible for ISP's or companies to acquirer new IPv4 addresses if they need them. The successor to IPv4 is standing ready in the form of IPv6. IPv6 has room for 3.4×10^{38} addresses, a virtually limitless supply. The problem is IPv4 and IPv6 can't communicate directly with each other, and the switchover to IPv6 won't happen overnight. So what will be the best approach to take with the transition to IPv6? What needs to be done?

As an ICT service provider it is Simac's responsibility to have the answers to these questions before their customers need them. The first questions that will be asked are: How do we make sure our website is available on IPV6, How do we make sure our employees can access IPv6 only websites and to make both of those possible: How do we get an IPv6 enabled internet connection and what are the alternatives if that's not yet possible?

The purpose of this internship was to find the answers that solve these questions in the simplest, cheapest and most secure manor and write a report about it (attachments E/ Bijlage E)

The exploratory research phase started by trying to find as many transition mechanisms (mechanism that help with the transition from IPv4 to IPv6) as possible. The workings of each mechanism were described first and their suitability in answering one or more of the three main questions and their compatibility with the Simac network was assessed. For each of the three questions 2 or 3 possible candidates were identified that will be further examined in the main research phase. These are: Dual stack, stateful NAT64, and translating proxies. Tunneling and 6to4 have been identified as alternatives to a native IPv6 internet connection.

In the research phase these selected mechanism have been further studied. The in first part the pros and cons of each was considered in general without looking at the specific application area. Afterwards each was considered specifically for each of the application area's identified in the research questions.

Using that data a recommendation was made for each of the questions as to what was the best mechanism to use. In the ideal scenario dual stack is the best, most future proof option. But its implementation takes time and has a big impact on the network so needs to be planned carefully. NAT64 or a translating proxy on the other hand are very fast to deploy and have a very small impact on the network, but are not future proof.

As long as there is no hurry go with dual stack. But start this transition as soon as possible. The sooner it is started the cheaper it will be in the end because you can take your time. Even if a customer doesn't yet want to implement IPv6 in the coming years it's a good idea to start making IPv6 support a requirement for all new hardware and software. This will prevent unexpected extra costs and smooth the transition.

Verklarende woordenlijst

IPv4	Internet protocol version 4. De standaard waar het internet op dit moment op werkt. Iedere host op internet heeft een 32bit IP adres (voorbeeld: 203.0.113.5) dat gebruikt kan worden om computers te identificeren en te vinden.
IPv6	Internet protocol version 6. De opvolger van IPv4. Maakt gebruik van 128bit adressen die hexadecimaal worden uitgeschreven (voorbeeld: 3ffe:1900:4545:3:200:f8ff:fe21:67cf)
IETF	IETF staat voor "Internet Enginering Task Force". IETF heeft tot doel het beter laten functioneren van het internet. Het wil dit doelen bereiken door het verschaffen van technische documenten van een hoge kwaliteit. Deze documenten, RFC's genaamd, zijn gratis publiekelijk beschikbaar en gaan over alles van het beschrijven van standaarden tot het beschrijven van current best practice, tot het verschaffen van relevantie informatie. Het IETF is een organisatie gebaseerd op open en vrijwillige deelname. Iedereen die interesse heeft mag mee doen. IETF werkt op basis van consensus. Iets wordt pas tot standaard uitgeroepen als er een ruwe consensus over is bereikt binnen alle leden.
RFC	RFC staat voor "Request For Comments" Als het IETF een document publiceert heet het een RFC en heeft het een eigen RFC nummer. De naam geeft aan dat elk document open staat voor commentaar voor iedereen die dat wil. RFC's hebben verschillende statussen, de belangrijkste daarvan zijn, standaard, proposed standard, informational, obsolete/historic, en experimental.
IANA	IANA staat voor "Internet Assigned Numbers Authority" Het is de organisatie die verantwoordelijke is voor het verdelen van IP adressen onder de verschillende regionale organisaties. Maar ook voor het bijhouden van TCP en UDP port nummers voor bekende applicaties en indirect met het bijhouden van de registratie van domain namen. IANA bestond tot mid jaren 90 uit 1 man. IANA is inmiddels onderdeel geworden van ICANN (wat staat voor Internet Corporation for Assigned Names and Numbers) wat de nieuwe organisatie is die verantwoordelijk is voor alle hiervoor genoemde onderdelen. IANA is nu enkel verantwoordelijk voor het verdelen van de IP adressen. Hierdoor ontstaat nog wel een verwarring tussen IANA en ICANN.
RIR	RIR staat voor "Regional Internet Registries", RIR's zijn organisaties die zich bezig houden met het verdelen van de grote IP blokken die ze krijgen van IANA onder de ISP's en bedrijven in hun regio. De Europese RIR is RIPE NCC.
ISP	ISP staat voor internet service provider. Dit zijn bedrijven die internet verbindingen aanbieden aan bedrijven en particulieren.

Transitie mechanisme	In dit document betekent dit een netwerk techniek ontwikkeld om de overgang van een IPv4 netwerk naar een IPv6 netwerk mogelijk te maken of te ondersteunen. Technieken bedoeld om communicatie tussen IPv4 en IPv6 mogelijk te maken vallen hier ook onder.
Address range	Een reek aaneensluitende IP adressen meestal onder beheer van een instantie of bedrijf. Deze adres reeksen hebben allemaal dezelfde pre-fix, (het eerste gedeelte van het adres) waar het laatste gedeelte van het adres vrij te gebruiken door de eigenaar van de reeks. Een voorbeeld van een address range is 198.51.100.0 t/m 198.51.100.255 Maar 198.51.100.50 t/m 198.51.100.127, kan ook. Een reeks met een veel kortere prefix is ook mogelijk waardoor er meer adressen in de reeks zitten.

1 Inleiding

De (IPv4) adressen op internet zijn op. De ~3.7 miljard adressen[(1)] waar IPv4's 32bit adres ruimte voor biedt zijn verdeeld. De Internet Assigned Numbers Authority (IANA) heeft de laatste 5 'blokken' van ~16 miljoen adressen elk verdeeld over de 5 Regional Internet Registries (RIR) in januari 2011, die de taak hebben deze blokken verder op te delen onder internet providers en bedrijven. APNIC, de RIP voor zuid oost Azië, heeft al zijn adressen 3 maanden na het verkrijgen van hun laatste block al opgedeeld en de Europese RIR (RIPE NCC) zal zijn uitgeput in 2012 is de verwachting. De andere RIR's zullen binnen een paar maanden tot een jaar volgen.

Dit zal betekenen dat bedrijven straks geen nieuwe IPv4 adres ranges meer kunnen krijgen voor hun bedrijf, en dat internet service providers (ISP's) geen nieuwe adressen hebben voor nieuwe klanten als hun bestaande voorraad is opgebruikt.

De oplossing staat klaar in de vorm van IPv6. Dit protocol biedt 128 bits aan adres ruimte en moet IPv4 gaan vervangen. IPv4 en IPv6 kunnen echter niet rechtstreeks met elkaar communiceren, en de verwachting is dat het nog jaren zo niet decennia gaat duren voordat IPv4 is uitgefaseerd. Beide protocollen zullen dus lange tijd naast elkaar bestaan op internet, en vormen daardoor in feite 2 aparte internetten die elkaar niet kunnen zien.

Maar hoe zorg je ervoor dat ze samen kunnen werken. Hoe zorg je ervoor dat jouw (web) services voor zowel het IPv4 als het IPv6 internet bereikbaar zijn. Hoe zorg je ervoor dat jouw werknemers gebruik kunnen maken van services op beide netwerken?

Simac ICT Nederland is als ICT service provider een van de eerste bedrijven die met deze vragen te maken gaat krijgen. Daarom heeft Simac dit project in het leven geroepen om bovenstaande vragen te beantwoorden vanuit het oogpunt van een bedrijf dat nu nog enkel een IPv4 netwerk heeft.

Voor beide vragen zijn verschillende oplossingen, met elk hun eigen voor en nadelen. De verschillende methodes worden geïnventariseerd, beschreven, en de voor en nadelen worden tegen elkaar afgewogen waarna een advies wordt uitgebracht.

Dit stageverslag is als volgt opgebouwd. In hoofdstuk 2 word het bedrijf beschreven, in hoofdstuk 3 word de opdracht behandeld, in hoofdstuk 4 bespreken we het onderzoek in hoofdstuk 5 besprek we het resultaat van het eerste deel van de opdracht,

[(1] 32bits is genoeg voor 4.3miljard adressen maar door de verdeling ervan en gereserveerde ruime voor anderen doeleinde blijven er in de praktijk ongeveer 3.7miljard over voor gebruik op internet)

2 Simac

2.1 bedrijfsbeschrijving

Simac Techniek NV, opgericht in 1971 en sinds 1986 genoteerd aan de beurs in Amsterdam, is een technologiebedrijf actief in de Benelux en Midden-Europa. Simac levert en onderhoudt bij middelgrote en grote organisaties hoogwaardige technologie ter verbetering van de bedrijfsprocessen. In totaal werken er bij Simac bijna 900 mensen verdeeld over meerdere vestigingen in Nederland, België en Luxemburg.

Simac Techniek NV bestaat uit werkmaatschappijen, de Simac-bedrijven, met een breed assortiment aan oplossingen, producten en diensten in de volgende bedrijfssegmenten:

ICT-infrastructuren
Ontwerp, implementatie en beheer van infrastructuren voor informatie- en communicatietechnologie.

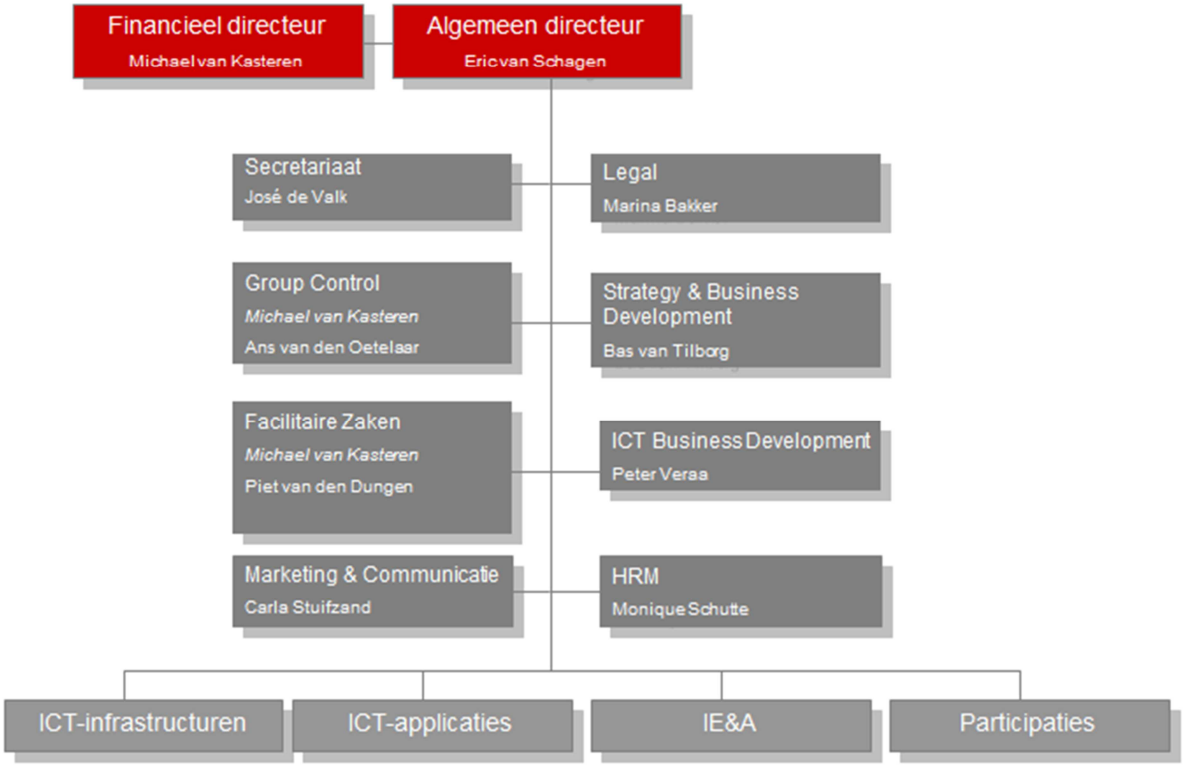
ICT-applicaties
Ontwerp, bouw en levering van branchespecifieke en oplossingsgerelateerde applicaties.

Industriële Elektronica & Automatisering
Levering van producten, projecten en diensten op het gebied van industriële elektronica en automatisering.(Bron Simac.nl)

Dit project wordt uitgevoerd uit naam van Simac ICT Nederland

Simac ICT Nederland neemt al jaren een onderscheidende positie in op de markt van outsourcingspartijen in Nederland. Onze dienstverlening richt zich op outsourcing van infrastructuur- en werkplekbeheer voor middelgrote en grote organisaties. Door een hechte en langdurige relatie met de klant zijn we in staat voortdurend de klant te ondersteunen met passende oplossingen en diensten. Dat geldt zowel voor de invulling van het beheer als voor de inzet van technologisch hoogwaardige kennis. Die kennis vertalen we voor de klant enerzijds in innovatieve en doelmatige projecten. Anderzijds kan de klant op basis van detachering een beroep doen op onze professionals. De klantgerichte inzet van de combinatie beheer - projecten - detachering maakt ons uniek op de markt waarop we ons richten. (Bron Simac.nl)

2.2 **Organigram**



Simac ICT Nederland bv
- Bernard Dortmans
- Paul de Rouw

Simac ICT België
- Patrick Bontinckx

Simac 3Services bvba
- Daniel van Hove

Simac ICT Luxemburg
- Daniel vander Heyden

Simac Business Applications
- André Wielaard

Simac Business Solutions
- Wim van der Velden

Simac Datacollect bv
- Peter Bouwmans

Simac Onderwijs bv
- Marina Bakker

Simac Triangle bv
- Rudie Piessens

Simac Electronics bv
- Marcel Leenen

Simac Masic & TSS bv
- Marc de Regt

Simac QuadCore bv
- Har Heuberger

Allied Data Technologies bv
- Jeroen van Eersel

APTS bv
- Ruud Bouwman

Genexis bv
- Gerlas van den Hoven

Sensite Solutions bv
- Jan Vet/Pim Adang

Simac ICT Tsjechië/Slowakije
- Dirk van Brussel
- Jaroslav Stefl
- Dusan Bruoth
- Martin Jirecek

3 De Opdracht

3.1 Achtergrond

Het internet is tegenwoordig bijna niet meer weg te denken, ook niet in het bedrijfsleven. Het is een belangrijk middel dat bijna alle bedrijven nodig hebben om zaken te kunnen doen. Van hun communicatie naar de klant toe met websites en social media, tot snelle onderlinge communicatie met andere bedrijven tot hun eigen werknemers die de informatie op internet nodig hebben om hun werk goed te kunnen doen.

Maar het in 1978 tot standaard verheven protocol waarop het internet gebaseerd is, Internet protocol version 4 (IPv4), is nooit ontworpen op de explosieve groei van die het internet de laatste 2 decennia heeft meegemaakt. Het probleem is dat om met elkaar te communiceren over het internet heeft elke apparaat een eigen unieke IP adres nodig zodat ze elkaar kunnen identificeren en vinden. IPv4 heeft 32bits aan adres ruimte en biedt daarmee ruimte voor 3.7 miljard adressen. Deze adressen raken echter op; zijn eigenlijk al op.

De Internet Assigned Numbers Authority (IANA) heeft namelijk de laatste 5 'blokken' van ~16 miljoen adressen elk verdeeld over de 5 Regional Internet Registries (RIR) in januari 2011. APNIC, de RIP voor zuid oost Azië, heeft al zijn adressen 3 maanden laten ook opgebruikt en de Europese RIP (RIPE NCC) zal zijn uitgeput in 2012 is de verwachting. De andere RIR's zullen binnen een paar jaar volgen. Voor mensen en bedrijven met al een IPv4 adres(range) zal dit niet direct veel gevolgen hebben, maar nieuwe mensen en bedrijven op internet zullen op een gegeven moment geen nieuw IPv4 adres kunnen krijgen en dus niet meer het internet op kunnen.

De oplossing staat gelukkig al klaar in de vorm van Internet Protocol Version 6 (IPv6). Dit protocol biedt met 128bit adressen ruimte voor 340 Sextillion ($3.4*10^{38}$)) Unique hosts. Het maakt daarnaast een aantal optionele features van IPv4 verplicht en verkleint de overhead die het protocol met zich mee brengt ondanks de langere adressen. Het nadeel is echter dat er geen rechtstreekste backward compatibility is. Iemand met enkel een IPv6 adres kan niet zomaar communiceren met iemand met enkel een IPv4 adres.

Het IPv6 protocol werd tot standard verheven in 1990 omdat al snel na het begin van het publiek beschikbaar maken van internet werd ingezien dat de IPv4 adres ruimte onvoldoende zou zijn. Het originele plan van toen, om IPv6 langzaam aan te introduceren en IPv4 en IPv6 voor langere tijd langs elkaar te gebruiken waarna IPv4 af te bouwen is echter niet gelukt. Zonder noodzaak is de adoptie van IPv6 veel langzaam verlopen dan gehoopt. Nu, 21 jaar later, is de noodzaak er echter wel.

Gelukkig is er niet helemaal stil gezeten de afgelopen jaren. Alle gangbare besturingssystemen bieden ondersteuning voor IPv6, bijna alle op dit moment verkochte professionele netwerk hardware doet dat ook, en het core netwerk van internet is ook bijna volledige IPv6 enabled. Nu begint de tijd te komen voor de volgende stap: de uitrol naar bedrijven en consumenten. In het originele plan zou iedereen nog altijd een IPv4 adres krijgen(of zijn huidige houden) samen met het nieuwe IPv6 adres. Nu zullen er echter binnen afzienbare tijd niet meer genoeg IPv4 adressen zijn. De eerste consumenten en bedrijven met enkel een IPv6 adres zullen dan een feit zijn.

3.2 Beginsituatie

De begin situatie gaat uit van de begin situatie van Simac en haar klanten. Die hebben allemaal een bestaand IPv4 netwerk en een of meer IPv4 internet verbindingen, in veel gevallen met een eigen IPv4 range. Er word nog nergens met IPv6 gewerkt in de productie omgevingen. Een aantal voor internet bereikbare services die regelmatig worden gedraaid zijn webservers(voornamelijk IIS), mail servers(voornamelijk exchange) en eventueel citrix Edge servers. Werknemers kunnen (eventueel via een proxy server) het IPv4 internet bereiken.

3.3 Probleemstelling

Zoals in de inleiding genoemd, de eerste internetgebruikers en bedrijven met enkel een IPv6 adres zijn in aantocht. Deze zullen niet rechtstreeks gebruik kunnen maken van de IPv4 services die Simac en haar klanten op internet aanbieden. Ook zullen er in de toekomst IPv6-only services gaan komen waar de werknemers van Simac en haar klanten gebruik van moeten maken en dat kan niet zomaar met enkel een IPv4 adres.

Het is voor Simac, als ICT service provider, noodzakelijk om voor deze problemen een oplossing klaar te hebben liggen voordat ze voor echte problemen zorgen, voor zichzelf maar ook voor haar klanten.

3.4 Opdrachtomschrijving

De opdracht bestaat uit het beantwoorden van 3 vragen:

- Welke manieren zijn er om de huidige IPv4 websites en services ook via IPv6 beschikbaar te maken?
- Welke manieren zijn er om werknemers toegang te geven tot IPv6-only websites en services?
- Welke manieren zijn er om een IPv6-enabled internet verbinding te krijgen?

Advies uitbrengen over de beste methode om op eenvoudige, kosten effectieve en vooral veilige manier deze vragen te beantwoorden is het hoofddoel van het project. ##

Om dat doel te bereiken zal een rapport worden gemaakt met aanbevelingen.

Hoewel het misschien logischer lijkt om te beginnen met het verkrijgen van een IPv6 verbinding is deze verbinding al door Simac gerealiseerd in hun test lab. Deze vraag is echter nog wel van belang voor klanten maar heeft hierdoor wel een lagere prioriteit gekregen en is daarom achteraan geplaatst.

4 De Uitvoering

4.1 Inleiding

In dit hoofdstuk wordt verder ingegaan op de werkwijzen gebruikt bij het afstuderen. Van elke fase wordt het doel, de activiteiten en de werkwijze beschreven en tot slot volgt een korte evaluatie van de fase.

4.2 Oriëntatie fase

4.2.1 Beschrijving

In de oriëntatie fase is uitgezocht wat er verwacht wordt van de student. Welk producten er opgeleverd moesten worden en hoe Simac die graag uitgewerkt zag. Deze periode is ook gebruikt om de student de tijd te geven om zich in IPv6 zelf te verdiepen en kennis van netwerken op te frissen. Tot slot diende de oriëntatie fase ook om de student bekend te maken met het bedrijf, de werkwijzen en om de relevante werknemers te leren kennen.

4.2.2 Activiteiten

De volgende activiteiten zijn de in de oriëntatie fase gedaan:

- Project initiation document opgesteld (bijlage A)
- Project planning opgesteld
- Communicatie plan gemaakt
- Opdrachtomschrijving opgesteld
- Oriëntatie binnen Simac
- Zelfstudie IPv6, opfrissen IPv4 kennis

4.2.3 Werkwijze

De definitieve opdracht omschrijving is in samenspraak met de bedrijfsbegeleiders als eerst opgesteld en goedgekeurd door zowel Simac als het stage bureau. Aan de hand van die opdracht omschrijving is het PID gemaakt, inclusief communicatie plan en project planning. Na enkele aanpassingen zijn deze documenten goedgekeurd door zowel bedrijfsbegeleiders als de stagebegeleider.

De oriëntatie binnen Simac begon met een rondleiding om een aantal collega's op verschillende afdelingen te ontmoeten, en een rondleiding door het gebouw en de verschillende afdelingen. Ook het meeluisteren in de werkruimte en de kantine was zeker informatief over het reilen en zeilen van Simac.

De zelfstudie van IPv6 bestond voornamelijk uit het zoeken naar relevante documentatie over IPv6 op internet, de RFC's doornemen, en presentaties/webinars van onder andere Cisco bekijken. En tot slot ook een aantal van de door simac opgestelde documenten over eerdere onderzoeken naar een aantal aspecten van IPv6. Voor de stage periode officieel begon was, is door de student met IPv6 geëxperimenteerd op zijn eigen Linux server aan de hand van opdrachten opgesteld door hurricane electric (een grote internet backbone die ook diensten als web hosting en tunneling aanbiedt).

De voornaamste vragen die gesteld zijn tijdens deze zelfstudie waren: wat is IPv6, wat is de ontstaansgeschiedenis, waarom is het ontwikkeld, hoe verschilt het van het nu gebruikte IPv4 (en waarom) en wat is het zelfde gebleven. Toen die vragen adequaat beantwoord waren verschoven de vragen naar: hoe ver is de implementatie van IPv6 op internet, hoe ver zijn de verschillende leveranciers van hard- en/of software met IPv6 en wat zijn de meest gebruikte technieken om IPv6 te implementeren. Deze laatste vragen hadden echter al veel overlap met de onderzoeksvragen en daarom is besloten hier het vooronderzoek af te sluiten.

4.2.4 Evaluatie

De definitieve opdrachtomschrijving en het PID zijn beide goedgekeurd en op tijd ingeleverd. Het communicatie plan en de planning zijn gebruikt als leidraad voor de rest van het project, al is de planning door de grote hoeveelheid overlap binnen de onderwerpen enigszins losjes gehanteerd. De grote lijn is gehanteerd maar er is vaak vooruitgewerkt, maar ook naderhand nog aangepast door nieuwe ontwikkelingen, ideeën en inzichten.

Het vooronderzoek heeft het gewenste resultaat opgeleverd. De opgedane en opgefriste kennis over netwerken, IPv4 en IPv6 samen met wat praktijk ervaring met IPv6 hebben geholpen om sneller grip te krijgen op onderzoeksvragen en de mogelijke technieken sneller te doorgronden.

4.3 Vooronderzoek

4.3.1 Beschrijving

In het vooronderzoek worden zo veel mogelijk transitie technieken gezocht en wordt een voorselectie gemaakt over welke toepasbaar zijn voor de onderzoeksvragen. In een later stadium worden de hier gekozen technieken met elkaar vergeleken per onderzoeksvraag.

Door de grote hoeveelheid transitie technieken was het vooraf verkleinen van de keuzen noodzakelijk. Door er voor te kiezen om het vooronderzoek een apart en uitgebreid deel van het vooronderzoek te maken dient het niet alleen om het aantal in detail onderzochte technieken te verkleinen maar geeft Simac ook referentie materiaal voor andere toepassingsgebieden in de toekomst.

4.3.2 Werkwijzen

Simac is Cisco gold partner en Microsoft certified supplier, dus de ondersteunde en aanbevolen technieken van deze 2 bedrijven zullen worden mee genomen. Vooral Cisco [1] is actief op het gebiedt van IPv6 en heeft meerdere video’s webcasts en White-papers gepresenteerd over de transitie naar IPv6. Maar ook de EU [2] heeft meerdere rapporten en onderzoeken gepubliceerd over IPv6, evenals het Amerikaanse ministerie van defensie [3] en de Europese RIP: RIPE NCC [4]. Verder zijn ook de RFC’s van het IETF [5] [6] over dit onderwerp meegenomen.

Uit deze bronnen is een lijst met bestaande transitie mechanismes samengesteld.

- Dual stack
- NA(P)T-PT
- Stateless NAT64
- Statefull NAT64
- Proxy/ALG
- Load balancers
- Static tunnels
- 6to4
- 6RD
- Teredo
- ISATAP
- DS-Lite

Maar hoe zijn deze technieken te vergelijk, wat zijn de criteria?

Het voornaamste is natuurlijk: is deze techniek überhaupt toepasbaar op een of meer van de onderzoeksvragen? Kan deze techniek de functie vervullen die de onderzoeksvraag verlangt? Maar om de selectie nog wat verder te verfijnen is samen met de bedrijfsbegeleiders nog een aantal andere criteria opgesteld. Samengevat zijn deze:

- IETF status
- Adres/prefix ondersteuning
- Uitgangspunt begin situatie (ipv4 netwerk of IPv6 netwerk)
- Schaalbaarheid/ bottleneck issues
- Beheerbaarheid
- Structurele Beveiligingsissues

Waarom zijn deze criteria belangrijk en waarom worden deze al meegenomen in het vooronderzoek? Een sterke negatieve beoordeling in een van deze criteria kan de techniek onbruikbaar maken voor het bedrijfsleven en daarmee voor Simac en haar klanten. Hierdoor kunnen er meer technieken van tevoren worden weggestreept voor aan het diepgaande onderzoek wordt begonnen waardoor er meer tijd over blijft voor de technieken die daadwerkelijk bruikbaar zijn.

- IETF status

IETF status is heel belangrijk omdat onder andere leveranciers van netwerk apparatuur veel waarde hechten aan de aanbevelingen van het IETF. Als het IETF iets tot standaard uitroept betekend dit dat de techniek waarschijnlijk door velen ondersteund gaat worden en dat men hier voor langere tijd ondersteuning op zal blijven verlenen. In het kort biedt de status “internet standard” bij de IETF een zekere mate van zekerheid. Complicatie voor dit project hierbij is dat IPv6 zelf nog niet deze status heeft bereikt. IPv6 is nog een proposed standaard. Aangezien alle transitie technieken IPv6 gebruiken heeft er ook nog geen een status hoger dan proposed standaard. Een dergelijke status geeft echter wel aan dat het op weg is om mogelijk een internet standaard te worden en dat de kans klein is dat er, anders als bij de “experimental” status, nog veel aan de techniek veranderd gaat worden. Ook leveranciers van netwerk apparatuur ondersteunen vaak (al dan niet op experimentele/proef basis) de proposed standards technieken.

Andere technieken hebben de status informational, experimental and historic. Informational is informatief, het beschrijft in dit geval een manier om een bestaande

techniek, licht aangepast, op een andere manier te gebruiken. Dat geeft aan dat het IETF de techniek (6RD) interessant en robuust genoeg vond om mensen er over te informeren, ook al neemt het IETF deze techniek niet onder zijn beheer (wat het wel doet met internet standards) Het is besloten dat de informational status geen negatief punt is tegen deze techniek.

De experimental status is dat echter wel. Voor het IETF betekent experimental dat de techniek nog niet goed doorgrond is, dat deze potentieel nog onderhevig is aan grote veranderingen en/of dat er nog geen bestaande implementaties van zijn (in hard- of software). Een experimental status is niet direct reden voor afkeur, het kan immers in de toekomst nog een standaard worden, maar het zeker wel een negatief punt in het gebruik van een bepaalde techniek waarmee rekening gehouden dient te worden.

Naam IETF status	**Beschrijving**	**Score**
Internet Standard	Bedrijven werken het liefst enkel met technieken die hier onder vallen vanwege de grote maten van zekerheid die het geeft. Nog geen IPv6 techniek heeft deze echter status bereikt	Positief
Proposed standard	Deze technieken zijn op weg om mogelijk een internet standaard te worden. De techniek zelf staat redelijk vast en worden vaak (eventueel experimenteel) ondersteunend door leveranciers van netwerk apparatuur in (een deel van) hun producten.	positief
Informational	Informatief. Het is geen IETF standaard, maar ze vonden het belangrijk genoeg om mensen erover te informeren.	Neutraal
Experimental	Een experiment. De techniek is nog volop in ontwikkeling en kan nog veranderen. Ondersteuning is erg onzeker	Negatief
Historic	Het IETF heeft bepaald dat deze techniek verouderd is of om andere redenen het gebruik ervan sterk af raad. Technieken met deze status vallen meteen af.	Diskwalificatie

- Adres/prefix ondersteuning

Grotere bedrijven hebben vaak eigen public IPv4 adres range. Zo kunnen hun publieke servers een vast IPv4 adres krijgen op internet, dat zelfs niet veranderd als ze van ISP zouden veranderen. Het wordt dan ook een PI (Provider Independent) address range genoemd. Een eigen IPv4 address range maakt het zelfs mogelijk om de servers via meerderen internet verbindingen bereikbaar te maken, wat multi-homing wordt genoemd.

De mogelijkheid tot multi-homing wordt door bedrijven vaak gezien als essentieel voor het garanderen van de betrouwbaarheid. Tot voor kort had IPv6 niet de mogelijkheid om PI address ranges te krijgen, maar sinds juli 2009 is die mogelijkheid er in Europa wel. Dat maakt ondersteuning van PI adressen een belangrijke overweging bij het kiezen van de juiste transitie technieken.

Veel transitie techniek kunnen met alle soorten adressen overweg, maar een aantal hebben limitatie over het soort adres dat kan worden gebruikt of hebben een vaste 'prefix' waarbij elk adres dat gebruik maakt van die techniek moet beginnen met dezelfde 4 of 8 karakters.

Alle technieken die overweg kunnen met PI adressen scoren een goed op dit onderdeel. Technieken waarbij er eisen aan het IP adres worden gesteld krijgen een aantekening, maar dat is nog niet altijd een reden om een techniek zondermeer af te keuren. Het is echter wel iets waar rekening mee gehouden dient te worden.

Een aantal technieken ondersteunt echter alleen private of local adressen. Dit zijn adressen bedoeld enkel voor een lokaal netwerk. Deze adressen worden niet door het internet gebruikt en worden er dan ook niet door verwerkt. Een techniek die enkel gebruik kan maken van dergelijke adressen is daarom nutteloos voor de onderzoeksvragen en kan daarom meteen worden weggestreept.

Adres ondersteuning	**Beschrijving**	**Score**
Alle adressen	Deze techniek kan met elk IPv6 adres overweg. Er zijn geen eisen waar het adres van de client of server aan moet voldoen	Positief
Vast prefix	Een server die gebruik maakt van deze techniek met een vast prefix moet een IPv6 adres hebben dat begint met bijvoorbeeld 2001:: (teredo) of 2002:: (6to4) waardoor er geen gebruik kan worden gemaakt van een PI adres	Negatief
Moet voldoen aan strenge eisen	Bijvoorbeeld: Stateless-nat64 kan alleen werken als het aan een IPv6 adres meteen kan zien hoe het moet worden omgezet naar een IPv4 adres. Dat kan alleen als het adres voldoet aan strenge eisen. De IPv6 adressen op internet voldoen niet aan die eisen.	Diskwalificatie
Local addresses	Deze adressen zijn enkel bedoeld om te communiceren op lokaal niveau, meestal enkel binnen het zelfde netwerk. Als een techniek alleen deze adressen ondersteunt kan er niet mee met het internet gecommuniceerd worden.	Diskwalificatie

- Uitgangspunt begin situatie

De klanten van Simac en Simac zelf hebben alleemaal een bestaand IPv4 netwerk. Ook is de keuze gemaakt dat nieuwe klanten met nieuw aan te leggen netwerken voorlopig ook nog een IPv4 netwerk krijgen als basis. De meeste technieken gaan uit van een bestaand IPv4 netwerk waar IPv6 aan toegevoegd wordt of kunnen werken in beide situaties. Een aantal technieken gaat echter uit van een bestaand IPv6 netwerk waar IPv4 aan toegevoegd wordt. In de toekomst kunnen deze technieken van belang gaan zijn, maar het is nog te vroeg in de ontwikkeling van IPv6 voor een dergelijke constructie. Bedrijven hebben nog niet genoeg vertrouwen in en ervaring met IPv6 om een dergelijke stap te maken, zelfs voor nieuwe netwerken. Technieken die uit gaan van een bestaand IPv6 netwerk worden afgekeurd.

- Schaalbaarheid/ bottleneck issues

Het is binnen het bedrijfsleven gebruikelijk dat al het verkeer van en naar het internet gecontroleerd wordt door één server/machine. Hoewel de bandbreedte van internet verbindingen flink is gegroeid in de loop der tijd is de hoeveelheid verkeer nog goed te verwerken met één apparaat. Het is echter anders als er gesproken wordt over al het interne netwerk verkeer. Een aantal technieken vereisen dat alle of nagenoeg alle internet netwerk communicatie wordt afgehandeld door één machine. Niet alleen maakt dit het netwerk enorm kwetsbaar voor uitval, ook is het heel slecht schaalbaar bij netwerk uitbreiding en vormt het snel een bottleneck bij piekgebruik. Technieken met problemen hier vallen daarom meteen af.

- Beheerbaarheid

In de ICT dienstverlening is de SLA (service level agreement) de basis van nagenoeg elk onderhoudscontract. In een SLA staan bijvoorbeeld garanties over uptime en hoe snel storing opgelost moeten zijn. Simac als ICT dienstverlener kan haar klanten dergelijke garanties geven omdat Simac zelf ook SLA's heeft bij andere bedrijven om dat mogelijk te maken, die op hun beurt misschien ook weer SLA's hebben om dat mogelijk te maken. Een dienstverlener wil daarom te allen tijde invloed uit kunnen oefenen op alles wat ze aanbieden aan klanten om dergelijke garanties te kunnen geven. Bij veel transitie technieken kan dat ook omdat alle apparatuur onder eigen beheer is of omdat er afspraken gemaakt kunnen worden met een externe partner (ISP, tunnelbroker ect)

Een aantal technieken maakt echter gebruik van bijvoorbeeld relay servers op internet. Deze meestal publiekelijk beschikbare relay servers kunnen onder beheer zijn van de eigen ISP, waardoor er afspraken gemaakt zouden kunnen worden, maar veel zijn dat niet. Veel van dergelijke technieken maken gebruik van andere relay servers voor de zender als voor de genen die antwoordt geeft. Concreet betekent dat dat elk adres op internet een andere relay server kan gebruiken om de verbinding tot stand te brengen. Het is onmogelijk om met al deze relay server beheerders een SLA af te sluiten. Dat betekent dat een dergelijke techniek (deels) onbeheersbaar is. Er kan door Simac geen invloed worden uitgeoefend op de betrouwbaarheid en daarom geen garanties worden gegeven naar de klant toe.

Hoe goed een techniek te beheren is, is het andere facet dat onder beheerbaarheid valt. Goed beheerbare technieken zijn overzichtelijk, geven voorspelbare resultaten en voegen geen onevenredige hoeveelheid complexiteit toe. Een aantal technieken scoorden slecht op één of meer van deze criteria en vielen daarom meteen af.

- Structurele Beveiligingsissues

Beveiliging is een belangrijke overweging bij alles wat met netwerken te maken heeft. Alles dat verbonden is met het internet vormt een risico. Maar met de juiste technieken, een goed doordachte netwerk layout en de juiste beveiligingshard- en software kunnen deze risico's acceptabel worden gemaakt. Simac houdt voor deze keuzes vast aan de op dat moment geldende 'best practice' voor netwerken (tenzij de klant bewust kiest voor een andere oplossing).

Een aantal van de gevonden transitie technieken vereisen echter dat er van deze 'best practice' wordt afgeweken of gaan er zelfs rechtstreeks tegen in. Iedere netwerk engineer weet dat elke verandering aan het netwerk, elke toevoeging, beveiligingsrisico's met zich mee brengt. Dat geldt voor alle transitie technieken en zelfs voor IPv6 in het algemeen. Maar met de juiste implementatie en beveiligingsmaatregelen kunnen de meeste technieken op een verantwoorde manier worden geïmplementeerd. Dit geldt echter niet voor alle technieken. Sommige technieken zijn zelf structureel onveilig of kunnen alleen op een onveilige manier gebruikt worden met betrekking tot de onderzoeksvragen.

4.3.3 Resultaat

Door een kritische blik te hebben tijdens het vooronderzoek is het aantal technieken dat verder onderzocht gaat worden gereduceerd tot twee of drie per onderzoeksvraag. Hierdoor is er meer tijd om de technieken die ook echt bruikbaar zijn grondiger te onderzoeken. Een overzicht van hoe de technieken scoorden op de verschillende criteria is te vinden op pagina 12 en 13 van bijlage E.

Dit overzicht is ook te gebruiken als referentie bij toekomstige IPv6 projecten.

4.3.4 Evaluatie

Hoewel het bestuderen en doorgronden van de verschillende technieken geen problemen opleverden was deze gegevens overzichtelijk op papier krijgen moeilijker dan aanvankelijk gedacht. Ondanks dat de technieken heel erg verschillend konden zijn moesten deze toch zo eenduidig mogelijk worden gepresenteerd. Door te focussen op de samen met de bedrijfsbegeleiders opgestelde criteria te leggen, naast een beknopte uitleg van de werking van de techniek werd de leesbaarheid al flink verbeterd. De later toegevoegde tabel met het overzicht van de toepasbaarheid op de onderzoeksvragen van alle technieken was ook de inspiratie om een tabel met de toepasbaarheid toe te voegen aan het hoofdstuk van elke techniek.

4.4 Onderzoek

4.4.1 Beschrijving

In de onderzoeksfase zullen de in het vooronderzoek geschikt bevonden technieken uitgebreid worden onderzocht. De werking van elk zal in meer detail worden onderzocht en de gevolgen van die werken op het netwerk zullen in kaart worden gebracht.

De onderzoeksfase is opgedeeld in vier delen. (zie tabel)

Om overlap en dubbele teksten te voorkomen zal in het eerste deel elke techniek uitgebreid onderzocht worden en de voor- en nadelen ervan beschreven zonder rekening te houden met het precieze toepassingsgebied uit de onderzoeksvragen. Op deze manier zijn de relevante bevindingen ook gemakkelijk te vinden voor andere toepassingen (bijvoorbeeld e-mail, Citrix servers of VPN) in de toekomst. In elk van de volgende drie delen wordt één van de onderzoeksvragen behandeld. In elk deel worden alle technieken van toepassing op de onderzoeksvraag bekeken in de context ván de onderzoeksvraag. Waarna per techniek allen voor de onderzoeksvraag relevante voor en nadelen nog een keer worden genoemd.

Onderzoeksdeel	**Beschrijving**	**Documentatie**
Algemeen	Hierin worden alle voor- en nadelen van de gekozen technieken beschreven zonder dat er rekening wordt gehouden met een specifiek toepassingsgebied.	Bijlage: E pagina: 16 hoofdstuk: 3
Webservers op IPv6	Hierin worden de voor- en nadelen van de bruikbare technieken beschreven bij gebruik voor webservers.	Bijlage: E pagina: 22 hoofdstuk: 4
Werknemer IPv6 connectiviteit	Hierin worden de voor- en nadelen van de bruikbare technieken beschreven bij gebruik voor werknemer IPv6 connectiviteit.	Bijlage: E pagina: 31 hoofdstuk: 5
IPv6 internet verbinding	Hierin worden de voor- en nadelen van de bruikbare technieken beschreven bij gebruik voor webservers.	Bijlage: E pagina: 37 hoofdstuk: 6

4.4.2 Werkwijze

In het vooronderzoek is al gebleken welke technieken geschikt zijn voor elk van de onderzoeksvragen. Maar welke mogelijke gevolgen heeft een keuze voor een van de technieken precies? Wat zijn de voors en tegens van elke van de mogelijke keuzes?

Hoe past de techniek in het netwerk van Simac of een van haar klanten? Wat voor gevolgen heeft het voor het netwerk? Hoeveel zal er moeten worden aangepast? Hoe kan de techniek worden uitgerold? Hoeveel tijd zou zo'n uitrol kosten? Hoeveel impact heeft die op de rest van het netwerk? Is bepaalde hardware noodzakelijk? Is deze al aanwezig en zo niet wat zou de aanschaf en installatie ervan kosten? Welke software/firmware versie moet minimaal op de hardware draaien? Is de software op de webserver van belang of het besturingssysteem van de werknemer? Hoe toekomstbestendig is de techniek?

Dit zijn een aantal van de vragen die beantwoord moesten worden in de onderzoeksfase. Maar om deze vragen te beantwoorden was het noodzakelijk om eerst meer te weten te komen over de netwerken die Simac in beheer heeft. In gesprekken met de bedrijfsbegeleiders is naar voren gekomen dat dit heel divers is en er dus moeilijk één

netwerktype valt aan te wijzen als zijnde standaard. Van de andere kant wordt er zo veel mogelijk gewerkt conform de geldende 'best practice' richtlijnen. Er is daarom besloten om uit te gaan van een 'best practice' netwerkopstelling.

Wat Simac's leveranciers betreft was het eenduidiger. Cisco is de hoofdleverancier wat netwerkapparatuur betreft en dat zal de focus zijn voor de hardware ondersteuning. Maar conform met recente 'best practice' is het gebruikelijk om de tweedelijns firewall (de firewall tussen het edge netwerk en de rest van het netwerk) bij een andere leverancier te betrekken om zo de impact van fouten en/of security issues bij een van beiden te minimaliseren. De keuze voor deze tweedelijns firewall is in de meeste gevallen McAfee of Microsoft TMG. Deze laatste heeft echter geen IPv6 ondersteuning en valt dus volledig af.

Verder was het belangrijk om na te gaan hoe Simac de toekomst van IPv6 voor zich zag, wat hun visie daarop was. Daartoe is er een interview geweest met een sales medewerker die de visie van Simac ook uitdraagt naar klanten toe. Simac denkt dat de toekomst dual stack gaat zijn, waarbij IPv4 en IPv6 lange tijd naast elkaar op het zelfde netwerk gebruikt gaan worden. De uitrol van IPv6 zien ze van buiten naar binnen. Beginnend met het edge-netwerk door naar de rest van het netwerk met als laatst het core-netwerk met de bedrijfs-kritische servers. Op deze manier kan de ervaring met en het vertrouwen in IPv6 groeien naar mate de impact van de veranderingen stijgt.

Met deze gegevens in de hand kon er gericht onderzoek gedaan worden naar de gestelde vragen. Het algemene onderzoek is geschreven met de netwerken van Simac in gedachten maar zonder rekening te houden met specifieke toepassingen. De 3 andere onderdelen zijn uiteraard ook geschreven met het netwerken van Simac in gedachten, maar rekening houdend met de specifieke toepassingen.

4.4.3 Evaluatie

Deze onderdelen zijn een aantal keer herschreven en geherstructureerd. De eerste keer was er nog geen algemeen onderzoeksdeel. Maar tijdens het schrijven bleek er steeds meer overlap te zitten tussen de verschillende toepassingsgebieden bij dezelfde techniek. Om grote hoeveelheden herhaling te voorkomen is toen besloten om voor een meer modulaire aanpak te gaan en is de algemene informatie in een eigen, apart hoofdstuk gezet. Door deze overlap is ook de planning niet heel strak aangehouden voor deze onderdelen. Er is zowel vooruit als achteruit gewerkt, afhankelijk van de beschikbare informatie. De oplevering van de hoofdstukken is wel redelijk volgens de planning gegaan. Echter bij de eerste oplevering waren er klachten over de leesbaarheid. Er is toen besloten om een meer uniforme hoofdstuk structuur aan te houden met een aantal terugkomende sub-hoofdstukken over specifieke onderdelen zoals beveiliging, ondersteuning, kosten, uitrol, en performance zodat specifieke informatie gemakkelijk terug te vinden is.

4.5 Advies

4.5.1 Beschrijving

Tijdens deze fase is alle verzamelde en gesorteerde informatie gebruikt om een advies uit te brengen over welke techniek voor welk toepassingsgebied het beste is. Daarnaast is op een aantal specifieke gebieden advies uitgebracht over de gevolgen van het gebruik van de techniek en waar rekening mee gehouden dient te worden.

4.5.2 Werkwijze

Met alle relevante gegevens in de hand kan het adviesgedeelte van het rapport worden opgesteld. De adviezen voor de 3 onderzoeksvragen zijn na elkaar in dezelfde fase behandeld en uitgewerkt. Vanwege de overlap was dit de meeste logische optie.

In gesprekken met de bedrijfsbegeleiders is getracht het belang van de verschillende voor- en nadelen te beoordelen en te sorteren. Aan de hand daarvan een keuze gemaakt voor de beste techniek. De onderbouwing daarvoor is beschreven in het eerste gedeelte van het aanbevelingenhoofdstuk van elk van de 3 onderzoeksvragen (bijlage E hoofdstuk 3.3, 4.4 en 5.3.). Vervolgens worden de kosten voor het uitrollen en onderhouden van de techniek besproken. In de rest van dat hoofdstuk worden er aanbevelingen gedaan op een aantal belangrijke gebieden waar de gekozen technieken invloed op heeft zoals Security en DNS en worden er aanbevelingen gedaan over de IP adres structuur en de software ondersteuning.

4.5.3 Resultaat

Voor zowel web services als werknemer connectiviteit is de aanbevolen techniek dual stack geworden. Ook al is het de techniek met de meeste impact op het netwerk, het is de enige techniek die meer is dan een lapmiddel. De enige techniek die Simac ook echt dichter bij een volledige IPv6 implementatie brengt en Simac de benodigde IPv6 ervaring laat opdoen. Daarnaast biedt dual stack ook de minste overhead en ondersteunde het alle type protocollen.

De andere mogelijkheden, zowel proxy als stateful NAT64, blijven beperkt tot een kleine toevoeging in de rand van het netwerk en zijn beide beperkt in de welke protocollen ze ondersteunen. Dat maakt ze van gelimiteerd nut bij de overgang naar IPV6. Maar ze zijn niet nutteloos. Het feit dat ze niet veel meer dan een toevoeging zijn aan het netwerk maakt ook dat ze relatief snel en zonder veel aanpassingen geïmplementeerd kunnen worden. Mocht er ooit haast zijn bij het implementeren van IPv6 dan zijn beide technieken een goede optie. Welke de beste is zal voornamelijk afhangen van de prijs, ervan uit gaande dat ze beiden het beoogde protocol ondersteunen. Maar houdt er rekening mee dat het tijdelijke oplossingen zijn.

Het grootste gevaar met IPv6 is het nog achter blijven van IPv6 security features voor beveiligingen in vergelijking met IPv4. Het is daarom aan te bevelen om nu al IPv6 in gedachte te houden bij het inkopen van netwerkapparatuur en software, ook al heeft de klant nog geen behoefte om IPv6 te gebruiken op korte tot middellange termijn. Ook al is er nu nog geen feature parity met IPv4, zorg dat je weet dat de leverancier er wel mee bezig is en dat die ondersteuning wel minimaal in de planning staat. Hoe eerder hiermee begonnen wordt met inkopen hoe eenvoudiger een overgang naar dual stack zal zijn met een veel kleinere kans op extra kosten door vroegtijdige vervanging van hardware en/of software.

Voor de IPv6 verbinding is natuurlijk de native IPv6 verbinding de beste, maar als dat nog niet mogelijk is de zakelijk IPv6 tunnel een goed alternatief, betrouwbaar, beheersbaar, weinig extra latency, voorspelbare bandbreedte en betaalbaar. Het tweede alternatief, 6to4 wordt eigenlijk in alle gevallen afgeraden voor gebruik binnen het bedrijfsleven. De kans is echter groot dat beide alternatieven niet vaak nodig zullen zijn, aangezien in 2012 bijna alle groter providers IPv6 aan gaan bieden, al dan niet tegen extra betaling.

Als een provider IPv6 gaat aanbieden en de klant is nog niet op IPv6 voorbereid, dan kan het geen kwaad om uit veiligheidsoverwegingen te controleren of IPv6 specifiek uitgeschakeld staat op de first line firewall of op een andere manier wordt geblokkeerd.

4.5.4 Evaluatie

De keuze voor welke techniek het beste was voor de 3 vraagstukken was uiteindelijk het gemakkelijkste gedeelte van deze fase. Moeilijker was het in kaart brengen van de gevolgen. De bedrijfsbegeleiders wilde zeker op het gebied van security en op DNS meer informatie wat er gedaan zou moeten worden en waar rekening mee gehouden moest worden bij een uitrol van dual stack in het bijzonder. Daarvoor is nog een aantal keer gevraagd naar extra informatie, die ook is gevonden. Uiteindelijk ligt er een duidelijk en goed geformuleerde conclusie, een die, naar zo later bleek, ook overeenkomt met de aanbevelingen van de grote spelers op netwerk gebiedt.

Het nieuwe mantra voor networking en IPv6 is namelijk "Dual stack where you can, tunnel where you must, translate when you have a gun to your head."

Conclusies en aanbevelingen

De antwoorden op de onderzoeksvragen zijn als volgt

Webservices beschikbaar maken op IPv6: dual stack, met nat64 of proxy als tijdelijk alternatief (kosten zullen de keuze tussen deze 2 het meest van de tijd bepalen)

Werknemer IPv6 connectiviteit: dual stack, met proxy server als tijdelijk alternatief als er haast bij een IPv6 implementatie is.

IPv6 internet verbinding: een native IPv6 verbinding is altijd de beste optie en vanaf 2012 verkrijgbaar bij het merendeel van de ISP's. Mocht dat nog niet mogelijk dan is een zakelijke tunnel een goed en betaalbaar alternatief.

Er ligt voor Simac een duidelijke aanbeveling: Dual stack. Het is niet de gemakkelijkste optie, maar wel de enige optie die in de toekomst altijd de beste resultaten zal geven en waarop verder gebouwd kan worden wanneer andere services ook via IPv6 aangeboden gaan worden.

Om deze overgang naar dual stack te vergemakkelijken is het aan te bevelen om zo snel mogelijk te beginnen met het aanpassen van het inkoopbeleid en van IPv6 ondersteuning een issue te maken. Het gemaakte rapport kan duidelijk maken aan klanten waarom de keuze is gemaakt voor Dual stack en waarom het nodig is om IPv6 ondersteuning mee te nemen in de overwegingen bij het inkopen.

Voor het verkrijgen van een IPv6 internet verbinding lijkt het erop dat nagenoeg alle grote spelers IPv6 in 2012 willen gaan inzetten. Bij de meeste providers zal dit bij de standaarddienstverlening horen en zullen er geen extra kosten aan verbonden zijn. Het enige serieuze alternatief is de zakelijke tunnel. Maar zoals gezegd, nagenoeg alle ISP's zijn serieus met IPv6 bezig waardoor het waarschijnlijk is dat dit alternatief niet lang nodig zal zijn.

Evaluatie

De stage bij Simac is, denk ik, goed verlopen. De ontspannen en informele sfeer hebben er voor gezorgd dat ik me redelijk snel op mijn gemak voelde bij Simac. Het is wel een groter bedrijf dan waar ik mijn eerste stage heb gedaan en dat zorgde ervoor dat ik wat meer moeite had om iedereen te leren kennen en te weten bij wie ik waarvoor terecht kon, ondanks de rondleiding in het begin.

Het is misschien gemakkelijk om met wat informatie over mezelf te beginnen. Ik ben dyslectisch en heb een autisme spectrum stoornis. De dyslexie betekent meestal niet meer dat dat ik wat meer tijd kwijt ben met typen en er altijd door een derde nagekeken moet worden op spelfouten. Het autisme heeft meer invloed gehad op het verloop van de stage. Een van de dingen die ik op mijn eerste stage heb ondervonden is dat een 40 urige werkweek voor mij best zwaar is. Officieel ben ik ook 80 tot 100% arbeidsongeschikt. Ikzelf denk dat dat veel te hoog is, en dat bleek ook tijdens de eerste stage, maar 40 uur houd ik niet eindeloos vol.

Een van de dingen die ik niet heb ervaren op mijn vorige stage, omdat het een klein bedrijf was (4 werknemers) is hoe lastig ik het vind om met veel mensen om te gaan. In een kleinere setting vind ik het gemakkelijker om op mensen af te stappen. Hier koste me dat wel even moeite. De sfeer bij Simac en het feit dat er meer mensen rondlopen met ‘eigenaardigheden’, maakte dit wel minder lastig dan dat het had kunnen zijn.

Ik wist ook wel van mezelf dat ik dat lastig zou vinden en heb daarom ook een heel technische stage opdracht gekozen waar de techniek het belangrijkste is. Maar de, naar ik dacht, heel heldere stage opdracht, waar ik bewust voor gekozen had, bleek toch breder interpreteerbaar dan ik in eerste instantie had gedacht. Omdat ik dacht dat deze al helder was heeft het wat langer geduurd voor ik hierover in gesprek ging met mijn bedrijfsbegeleiders.

In het vooronderzoek was het heel duidelijk noodzakelijk om helemaal de techniek in te duiken en dat is ook gebeurd. Maar tijdens het onderzoek bleef ik daar een beetje in hangen en moest door de bedrijfsbegeleiders worden aangespoord om het meer toe te gaan spitsen op Simac. Dat is iets waar ik in het vervolg op moet blijven letten.

Van mezelf ben ik ook altijd een autodidact geweest. In een hoekje puzzelen en uitzoeken hoe het zit gaat me altijd goed af en meestal heb ik de problemen snel doorgrond. De benodigde gegevens verzamelen en interpreteren was daarom nooit een probleem tijdens de stage. Het overzichtelijk op papier krijgen van deze gegevens ging me vaak veel minder goed af. Hier is dan ook veruit het meeste tijd in gaan zitten. Mijn dyslexie hielp hierbij ook niet mee. Halverwege de stage, toen het middelste gedeelte van het rapport geherstructureerd moest worden had ik soms moeite om mijn aandacht hierbij te houden omdat het voor mijn gevoel zo langzaam ging. Het interessante gedeelte, het uitzoeken, was voor mijn gevoel al geweest. Wat afwisseling met praktijk onderzoeken had misschien geholpen.

Naar het einde van de stage toe ging het me gemakkelijker af om de Simac specifieke informatie te achterhalen die ik nodig had en ik geleerd om het gewoon te doen. Bereid jezelf voor zo goed als je kan en stap op de mensen af (digitaal of in het echt)

Al met al is het voor mij een erg leerzame stage geweest. Zowel op IPv6 gebied als op persoonlijk gebied.

Bibliography

[1] Cisco. (2011, Aug.) Cisco IPv6. [Online]. http://www.cisco.com/web/solutions/trends/ipv6/index.html

[2] (2011, Oct.) Europa's information sociaty IPv6. [Online]. http://ec.europa.eu/information_society/policy/ipv6/index_en.htm

[3] US Department of Defence. (2010, June) IPv6 Standard Profiles for IPv6 Capable Products Version 5.0 July 2010. [Online]. http://jitc.fhu.disa.mil/apl/ipv6/pdf/disr_ipv6_50.pdf

[4] Matjaž Straus Istenič) RIPE nnc (Luka Koršič. (2011, Sep.) IPv4/IPv6 Transition Mechanisms. [Online]. http://www.ripe.net/ripe/meetings/regional-meetings/dubrovnik-2011/presentations/IPv6_Transition_Mechanisms_Ripe_07092011_v1.2.pdf

[5] IETF. (2008, July) RFC5211 An Internet Transition Plan. [Online]. http://tools.ietf.org/html/rfc5211

[6] IETF. (2011, Apr.) RFC6144 Framework for IPv4/IPv6 Translation. [Online]. http://tools.ietf.org/html/rfc6144

Bijlage A – Plan van Aanpak

IPv6 De eerste echte stappen

Project Initiation Document

Onderwerp	IPv6 webservices en connectiviteit
Opgesteld door:	Vincent Verheijen
Datum:	17-08-2011
Versie:	1.1

Simac ICT Nederland bv
De Run 1101, 5503 LB Veldhoven
Postbus 340, 5500 AH Veldhoven
Tel. (040) 258 29 11
Fax (040) 258 23 10
Internet: www.simac.com/nl/ict

Document historie

Revisies

Versie	Status	Datum	Wijzigingen
0.1	Concept	17-08-2011	Eerste opzet
0.2	Verbetering na feedback	2-09-2011	opdracht verduidelijkt, fouten verbeterd
1.0	Inleveren	14-09-2011	Nagekeken 3de partij, planning uitgebreid
1.1	Verbetering na feedback	16-09-2011	Opbrengst uitbreiden Pagina nummers Spelling

Management samenvatting

Doel van dit document

Dit project initiation document heeft tot doel om het project "IPv6 De eerste echte stappen" te definiëren om zodoende een duidelijk beeld te geven over waarom dit project belangrijk is, wat er wordt gedaan, waarom dit word gedaan en wanneer dit word gedaan.

Aanleiding

Het aantal beschikbare publieke IPv4 adressen op internet raakt op. De vervanging van het huidige protocol staat klaar in de vorm van IPv6. In de toekomst worden enkel nog IPv6 adressen uitgedeeld. Maar IPv6 is niet in staat rechtstreeks te communiceren met IPv4. Dit roept 2 vragen op: hoe komen mensen met enkel een IPv6 adres straks ook op onze website, en hoe komen onze werknemers straks op websites met enkel een IPv6 adres.

Dit project heeft tot doel alle methodes om beide doelen te realiseren, te inventariseren en vervolgens voor en nadelen van elk te onderzoeken en te vergelijken. Voor beide doelen is echter een native IPv6 verbinding nodig. Ook hier zal een onderzoek naar worden gedaan welke mogelijkheden er zijn, en er zal worden ingegaan op wat de mogelijkheden zijn als er geen native opties beschikbaar zijn.

Als testcase zal op het einde van het project een website op IPv6 beschikbaar worden gemaakt aan de hand van de binnen Simac gangbare scenario's.

Aanpak

Er is veel overlap van de verschillende methodes, en daarom zal het vooronderzoek ze tegelijk onderzoeken. Tijdens het uitwerken en testen van de scenario's zal elke gevonden methode na elkaar opgezet en getest worden.

Kosten

De kosten voor het project zijn beperkt. Een student voltijd, 2 begeleiders met in totaal 2 uur begeleidings tijd in de week en gebruik van al bestaande hardware in the testlab.

Opbrengst

De opbrengst is een vergrote kennis van IPv6 binnen Simac zodat de nodige antwoorden al klaar liggen voor ze nodig zijn. Dit zal bijdragen bij het snel kunnen beantwoorden van de onvermijdelijke vraag vanuit de klant over IPv6 en kostenbesparend werken bij het plannen en uitvoeren van de noodzakelijke wijzigingen.

Inhoud

1 Inleiding

1.1 Doel van dit document

Dit is het Project Initiation Document (PID) voor het Afstudeer project "IPv6 De eerste echte stappen". Dit project is aangeboden door en zal worden uitgevoerd bij Simac ICT Nederland (van af nu Simac ICT of simpelweg Simac genoemd). Dit document heeft als doel het project de concretiseren. Dit document zal daarmee de basis vormen voor het beheer en assessment van het project.

Deze PID zal de volgende aspecten van het project behandelen:

- Wat is het doel van het project?
- Waarom is het belangrijk om dit project uit te voeren.
- Wie is er betrokken bij het project en wat is hun taak
- Hoe en wanneer zullen de doelstellingen in deze PID worden gerealiseerd.
- Allereerst word begonnen met een korte beschrijving van Simac, en Simac ICT en de aanleiding voor dit project vanuit het oogpunt van het bedrijf.

Dit document zal gebruikt worden om:

- Aan te tonen dat het project een solide basis heeft, voordat management met het project akkoord gaat.
- Om als basis te dienen waaraan de project voortgang kan worden bijgehouden en getoetst.

1.2 Structuur van dit document

Dit document zal de volgende onderdelen bevatten:

- Inleiding
  Korte beschrijving van het doel van dit document
- Achtergrond
  Een korte beschrijving van het bedrijf en de redenen voor dit project
- Project definitie
  De beschrijving van het project en de initiële business case.
- Communicatieplan
  De planning voor de communicatie binnen het project
- Planning
  Een Weekplanning

2 Achtergrond

2.1 Project Initiation Document

In het PID word kort aangegeven wat het doel is van het project, hoe dit gerealiseerd gaat worden en welke middelen daarvoor ingezet moeten worden. Tevens wordt aandacht besteed aan de tijdsplanning. Het maakt duidelijk welke producten worden opgeleverd en wanneer deze worden opgeleverd. Verder geeft het een duidelijk overzicht van de gemaakte afspraken en de nog te nemen stappen.

2.2 Organisatie

2.2.1 Bedrijfsomschrijving

Simac Techniek NV, opgericht in 1971 en sinds 1986 genoteerd aan de beurs in Amsterdam, is een technologiebedrijf actief in de Benelux en Midden-Europa. Simac levert en onderhoudt bij middelgrote en grote organisaties hoogwaardige technologie ter verbetering van de bedrijfsprocessen. In totaal werken er bij Simac bijna 900 mensen verdeeld over meerdere vestigingen in Nederland, België en Luxemburg.

Simac Techniek NV bestaat uit werkmaatschappijen, de Simac-bedrijven, met een breed assortiment aan oplossingen, producten en diensten in de volgende bedrijfssegmenten:

ICT-infrastructuren
Ontwerp, implementatie en beheer van infrastructuren voor informatie- en communicatietechnologie.

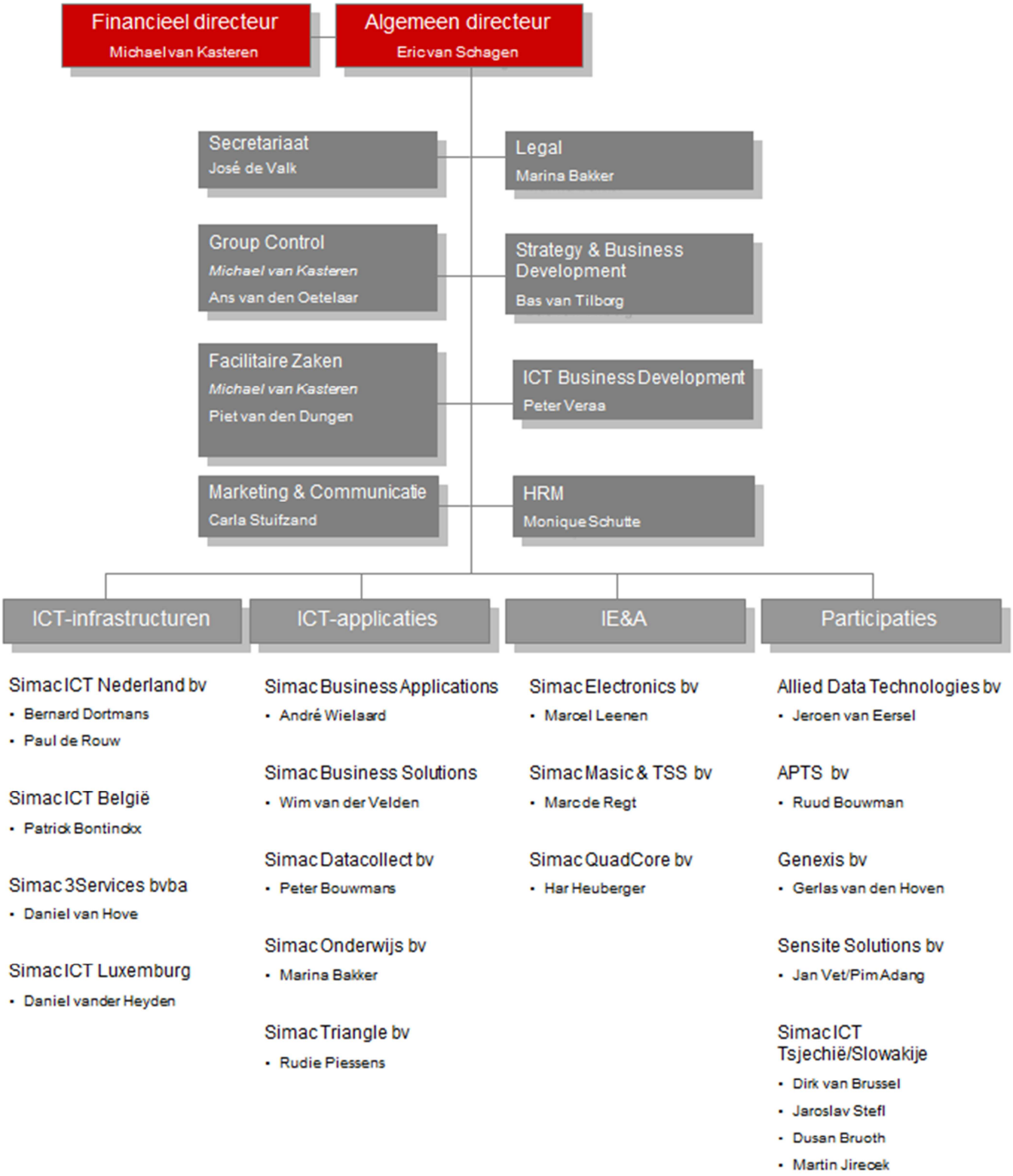
ICT-applicaties
Ontwerp, bouw en levering van branchespecifieke en oplossingsgerelateerde applicaties.

Industriële Elektronica & Automatisering
Levering van producten, projecten en diensten op het gebied van industriële elektronica en automatisering. (Bron Simac.nl)

Dit project wordt uitgevoerd uit naam van Simac ICT Nederland

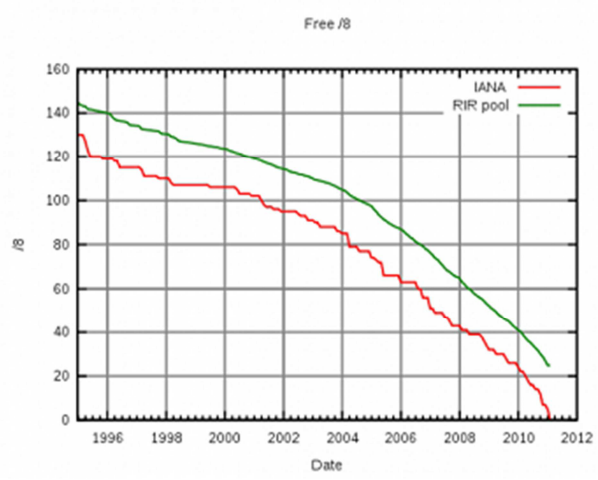
Simac ICT Nederland neemt al jaren een onderscheidende positie in op de markt van outsourcingspartijen in Nederland. Onze dienstverlening richt zich op outsourcing van infrastructuur- en werkplekbeheer voor middelgrote en grote organisaties. Door een hechte en langdurige relatie met de klant zijn we in staat voortdurend de klant te ondersteunen met passende oplossingen en diensten. Dat geldt zowel voor de invulling van het beheer als voor de inzet van technologisch hoogwaardige kennis. Die kennis vertalen we voor de klant enerzijds in innovatieve en doelmatige projecten. Anderzijds kan de klant op basis van detachering een beroep doen op onze professionals. De klantgerichte inzet van de combinatie beheer - projecten - detachering maakt ons uniek op de markt waarop we ons richten. (Bron Simac.nl)

2.2.2 Organigram



2.3 Aanleiding

Het internet is een onmisbaar onderdeel geworden van de communicatie en presentatie naar de buitenwereld toe van bijna ieder bedrijf.
Traditioneel via Websites, maar steeds vaker ook door middel van VOIP en social media,

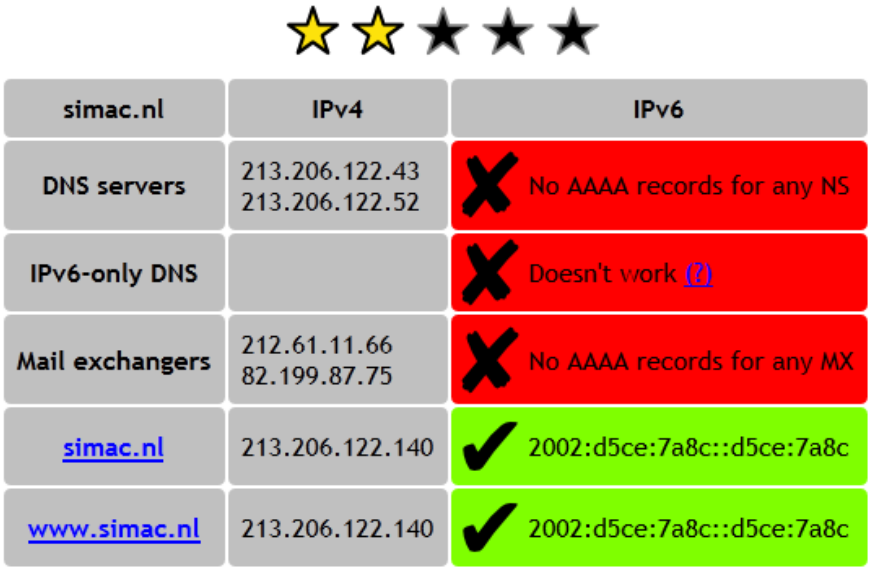


communiceren bedrijven met elkaar en met de klant. Maar om dat mogelijk te maken is minimaal 1 uniek internet adres (een IP adres genoemd) nodig voor het bedrijf. De IPv4 adressen raken echter op.

Internet protocol (IP) is de taal van het internet en op dit moment word voor bijna al het verkeer op internet IP versie 4(IPv4) gebruik. Toen IPv4 in 1977 werd ontwikkeld was dit protocol eigenlijk, volgens een van de ontwikkelaars, Vinton Gray Cerf, bedoeld als experiment. De 4.3 miljard adressen waar IPv4's 32bit adressering ruimte voor biedt leek op dat moment ruim voldoende om een 'experiment' uit te voeren. Het experiment ging echter een eigen leven leiden en groeide uit tot het internet zoals we het nu kennen. Het gevolg was dat de beschikbare adressen snel opraakten.

De oplossing kwam met de introductie van IPv6 in 1998. IPv6 heeft 128bit adressen en biedt daarmee ruimte voor 340 Sextillion ($3.4*10^{38}$)) adressen. Waarom werken we nu dan nog voornamelijk met IPv4? Omdat er geen enkele interoperabiliteit is ingebouwd in IPv6 om te kunnen werken met IPv4 adressen, omdat software eerst moest worden aangepast om IPv6 te kunnen begrijpen en omdat de infrastructuur van internet eerst geschikt gemaakt moet worden voor IPv6. Dat laatste is grotendeels gebeurt, en ook alle gangbare besturingssystemen kunnen inmiddels met IPv6 overweg. Dat samen met het feit dat vorige jaar de laatste IPv4 adres blokken zijn vergeven is het signaal dat er nu door bedrijven serieus moet gaan worden nagedacht over hoe de overgang naar IPv6 moet worden aangepakt. De eerste internetgebruikers met enkel een IPv6 adres staan voor de deur.

De vragen die bedrijven zich binnenkort gaan stellen zijn: hoe kunnen we er voor zorgen dat ook mensen met enkel een IPv6 adres gebruik kunnen blijven maken van onze website en andere internet diensten, en hoe kunnen we onze werknemers toegang geven tot webpagina's die enkel nog op IPv6 te bereiken zijn.



Als vooruitstrevende ICT service provider is Simac een van de eerste bedrijven die concreet met IPv6 aan de slag moet om hun klanten duidelijke antwoorden te kunnen geven en passende oplossingen kunnen bieden.

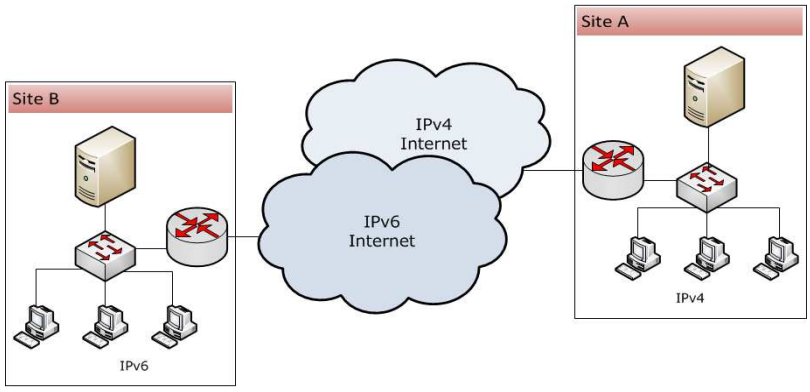
3 Project definitie

3.1 Doelstelling

Het project heeft 3 hoofd doelstellingen:

- Het inzichtelijk maken van mogelijkheden om web- sites en services beschikbaar te maken op IPv6 voor Simac en haar klanten.
- Het inzichtelijk maken van de mogelijkheden om IPv6 only web- sites en services beschikbaar te maken voor de werknemers van Simac en haar klanten.
- Het onderzoeken van de mogelijkheden om een native IPv6 internet verbinding te realiseren en eventuele alternatieven mocht dat niet mogelijk zijn.

Het onderzoek naar het IPv6 enabled maken van web sites en services kan technisch worden gesteld als: hoe zorg ik ervoor als IPv4 netwerk(site A) dat netwerken met enkel een IPv6 adres (site B) verbinding kunnen leggen met mijn op dit moment nog IPv4 netwerk/servers. Dit onderzoek zal omvatten een inventarisatie van alle opties dit mogelijk te maken en de voor en nadelen van elke methode. En vervolgens een aanbeveling doen welke methode(n) de beste zijn in welke situatie.



Het onderzoek naar het beschikbaar maken van IPv6-only web services voor de werknemers zal bestaan uit het inventariseren van alle mogelijkheden om dit doel te bereiken en de voor en nadelen van elke methode te behandelen. De vraag kan technisch als volgt worden samengevat: hoe kan een bedrijf zijn werknemers die nu nog enkel IPv4 adressen hebben (Site A) verbinding laten leggen met netwerken die enkel een IPv6 adres hebben (Site B). Ook dit onderzoek zal zich voornamelijk richten op de netwerk configuratie, maar de benodigde client instellingen worden benoemd en behandeld. Als de inventarisatie is gedaan dan zal een onderbouwde aanbeveling worden gedaan over de beste methode(n) om te gebruiken.

Het onderzoek naar de mogelijkheden voor een native IPv6 verbinding omvat het inventariseren wie, voor de zakelijke markt, een dergelijke verbinding kan aanbieden en waar. Simac zelf heeft inmiddels een native IPv6 verbinding gerealiseerd, maar dergelijke informatie is nog steeds van belang voor de klanten. Ook worden alternative opties onderzocht mocht een native verbinding niet mogelijk zijn.

Tot slot zal er een testcase gerealiseerd worden waarin een website via IPv6 beschikbaar zal worden gemaakt aan de hand van de bij Simac gebruikelijke scenario's.

3.2 Gekozen aanpak

Omdat er 3 verschillende vragen liggen is er voor gekozen om deze 1 voor 1 te beantwoorden naar het waterval model. Ook alle deelonderzoeken (de verschillende gevonden oplossingen) worden na elkaar uitgevoerd omdat ze elke voor zich gebouwen en getest moeten worden.

3.3 Resultaten

3.3.1 Opdracht

De opdracht is onderzoeken op welke manieren de klanten een IPv6 internet verbinding kunnen verwezenlijken, hoe klanten op eenvoudige kosteneffectieve en veilige wijze hun websites en services naast IPv4 ook beschikbaar kunnen maken op IPv6, en onderzoeken op welke manieren bedrijven hun werknemers toegang kunnen geven tot IPv6 only websites en services. Tot slot zal een testcase worden gemaakt waarbij een website via IPv6 bereikbaar zal worden gemaakt aan de hand van de aanbevolen methodes.

3.3.2 Projectplanning

Fase

1. Vooronderzoek

   Onderzoek doen naar IPv6, hoe het werkt, en de verschillen met IPv4. De reeds beschikbare IPv6 kennis bij Simac doornemen. Een idee krijgen van de werkwijze van Simac aan de hand van interviews met het IPv6 kennisteam.

2. Onderzoek Beschikbaar maken web services via IPv6

   De verschillende methodes om het doel te bereiken onderzoeken en inventariseren. De voor en nadelen van elke methode duidelijk uiteen zetten. Elke methode zal worden gerealiseerd in het testlab en getest. Vervolgens zal in het rapport een advies worden uitgebracht over wat de beste methode is en waarom.

3. IPv6 connectiviteit realiseren voor werknemers.

   De verschillende methodes om het doel te bereiken onderzoeken en inventariseren. De voor en nadelen van elke methode duidelijk uiteen zetten. Vervolgens zal in het rapport een advies worden uitgebracht over wat de beste methode is en waarom.

4. Native IPv6 internet verbinding.

   Inventariseren wie een IPv6 Internet verbinding kan realiseren, voor welke prijs, welke snelheid en tegen welke voorwaarden. En voor het geval er nog geen mogelijkheid bestaat voor een native IPv6 verbinding op een bepaalde locatie word er ingegaan op de alternatieve (niet-native) technieken benoemen en behandelen.

5. Case study website beschikbaar op IPv6

   Als case-study word een website beschikbaar gemaakt op IPv6 aan de hand van de aanbevelingen.

3.3.3 Producten

Dit project zal de volgende producten opleveren.

Simac ICT Nederland

IPv6 rapport met de volgende onderwerpen

- Rapport: Web services op IPv6 beschikbaar maken
- Rapport: IPv6 web services beschikbaar maken voor werknemers.
- Rapport: Native IPv6 Internet verbinding.

Fontys Hoge school

- Project initiation document
- Dagenverantwoording
- Scriptie/Stage verslag

3.4 Randvoorwaarden en beperkingen

- Voldoende medewerking vanuit Simac ICT Nederland bv
- Toegang tot internet voor het doen van Onderzoek
- Inzicht in de huidige stand van zaken binnen Simac met betrekking tot IPv6
- Toegang tot Testlab, ivm case study

4 Initiële Business case

Het internet is een onmisbaar stuk gereedschap geworden voor bedrijven in hun communicatie naar de klant en een onmisbare kennisbank voor hun werknemers. Door het opraken van de IPv4 internet adressen en de nagenoeg onvermijdelijke overstap naar IPv6 lopen bedrijven echter het risico dat in de toekomst delen van internet geen gebruik meer kunnen maken van hun website en services. Ook kan het gebeuren dat delen van internet niet langer beschikbaar zijn voor hun werknemers.

Hoewel dit voor de meeste bedrijven nog weinig problemen zal opleveren de komende jaren zullen wel ze in toenemende mate gaat voorkomen. Het is dus belangrijk dat bedrijven beginnen met het nadenken over de noodzakelijke maatregelen in de komende paar jaar. Veel bedrijven zullen rond deze tijd dan ook vragen gaan stellen over IPv6. Als klant gerichte ICT service provider is het voor Simac belangrijk om deze antwoorden voortijdig klaar te hebben, en zelf voortijdig in de eigen (test) omgeving voldoende ervaring met IPv6 op te doen.

Het verkrijgen van een (bij voorkeur) native IPv6 verbinding zal de eerste stap zijn. Het inventariseren wie een dergelijke verbinding kan leveren, waar ze die kunnen leveren, met welke technologie en snelheden en onder welke voorwaarden is dus een belangrijke stap.

Het beschikbaar maken van de bedrijfs web- sites en servies op IPv6 naast IPv4 zal in de meeste gevallen de volgende stap zijn. Elke klant is uniek. Een duidelijk overzicht van de mogelijke oplossingen, de voor en nadelen van elk, en de gevolgen voor de web- configuratie inzichtelijk maakt is dus noodzakelijk voor het maken van de juiste keuze bij het uitrollen van IPv6.

En tot slot het beschikbaar maken van IPv6 connectiviteit aan de werknemers. Deze vraag is minder dringend omdat de verwachting is dat praktische alle websites voorlopig nog beschikbaar blijven op IPv4. Maar het is potentieel wel een erg ingrijpende wijziging die veel gevolgen kan hebben voor zowel de software als de gebruikers op een netwerk. Er kan dus niet vroeg genoeg begonnen worden aan het testen van dergelijke wijzigingen. En om duidelijk te maken welke wijzigingen dat moeten worden, is het noodzakelijk om een inventarisatie te maken van de mogelijke oplossingen en de voor en nadelen van elk in kaart te brengen.

4.1 Aannamen

Voor het uitvoeren van het onderzoek zijn de volgende aannames gedaan.

- De overstap naar IPv6 is noodzakelijk in de toekomst
- Het onderzoek naar de 3 doelen is af te ronden in de gestelde tijd van 20 weken
- Het onderzoek blijft grotendeels binnen de scope zoals gesteld in dit PID (echter, enige overlap met andere lopende IPv6 projecten is te verwachten)

4.2 Kosten

De kosten zijn vrij beperkt. Het Project betreft voornamelijk bureau onderzoek en er hoeft geen extra software of hardware te worden aangeschaft omdat het testlab al is ingericht voor IPv6 onderzoek.

- Stage vergoeding student 450,- Euro per maand.
- Tijd begeleiders geschat op 2 uur per week.
- Gebruik Testlab hardware.

4.3 Baten

Als vooruitstrevend ICT dienstverlener is het voor Simac ICT Nederland belangrijk om in te spelen op de nieuwe ontwikkelingen en voorbereidt te zijn op aankomende veranderingen. IPv6 is een potentieel grote en ingrijpende verandering waar klanten zeker advies over zullen vragen bij Simac. De nodige antwoorden al op de plank hebben liggen zal bijdragen het snel kunnen beantwoorden van de onvermijdelijke vraag vanuit de klant en kostenbesparend werken bij het plannen en uitvoeren van de noodzakelijke wijzigingen.

Bijlage B: Communicatie plan

Goede gestructureerde communicatie is belangrijk in elk project.

Lijst met de hoofdpersonen belangrijk voor dit Project

Naam	Rol	Email	Tel
Vincent Verheijen	Student	vincent.verheijen@simac.com vincent.verheijen@student.fontys.nl v.verheijen@chello.nl	06-17694190
Luc Aelen	Bedrijfsbegeleider	luc.aelen@simac.com	040-258 2274
Tom van Haandel	Bedrijfsbegeleider	tom.van.haandel@simac.com	040-258 2267
Nico van der Steen	O&E Netwerk Enginering team cluster manager	nico.van.der.steen@simac.com	
Peter van den Broek	School begeleider	p.vandenbroek@fontys.nl	0877871138

Lijst geplande communicatie momenten

Wekelijks	Vergadering bedrijfsbegeleiders over project voortgang	Luc Aelen Tom van Haandel Vincent Verheijen
2 wekelijks	IPv6 team vergadering	Luc Aelen Tom van Haandel Vincent Verheijen Nico van der Steen Overige Leden IPv6 team
Eenmalig	Bedrijfsbezoek	Luc Aelen Tom van Haandel Peter van den Broek Vincent Verheijen
Eenmalig	PID Evaluatie	Peter van den Broek Vincent Verheijen
Eenmalig	Scriptie evaluatie	Peter van den Broek Vincent Verheijen

Bijlage C: Project Planning

Dit project zal voor een groot deel uit onderzoek bestaan. Voor elke onderzoeksvraag komen meerdere mogelijke oplossingen naar voren. Er zal vooraf een inschatting worden gemaakt aan de hand van het vooronderzoek over hoeveel mogelijkheden er gevonden gaan worden en aan de hand daarvan de tijd voor elke vraag inplannen.

Hoe wel het misschien logischer is om eerst de connectiviteit te onderzoeken heeft Simac al een IPv6 verbinding gerealiseerd, en daarom heeft dit onderzoek een lagere prioriteit gekregen en zal daarom als laatst worden uitgevoerd.

(voorlopig)

Week 1-4 voorbereiding

- Week1-4 Voor onderzoek
- Week1-2 PID opstellen

Week 5-10 onderzoek Web services online via IPv6

- Week 5-6 Dual Stack
- Week 7-8 Nat64
- Week 9 proxy
- Week 10 Rapport opstellen

Week 11-16 Onderzoek Werknemer IPv6 connectiviteit beiden en opstellen rapport

- Week 11-12 Dual Stack
- Week 13-14 Nat44 + Native IPv6
- Week 15 Proxy
- Week 16 Rapport opstellen

Week 17-18 Onderzoek Native IPv6 Internet verbindingen

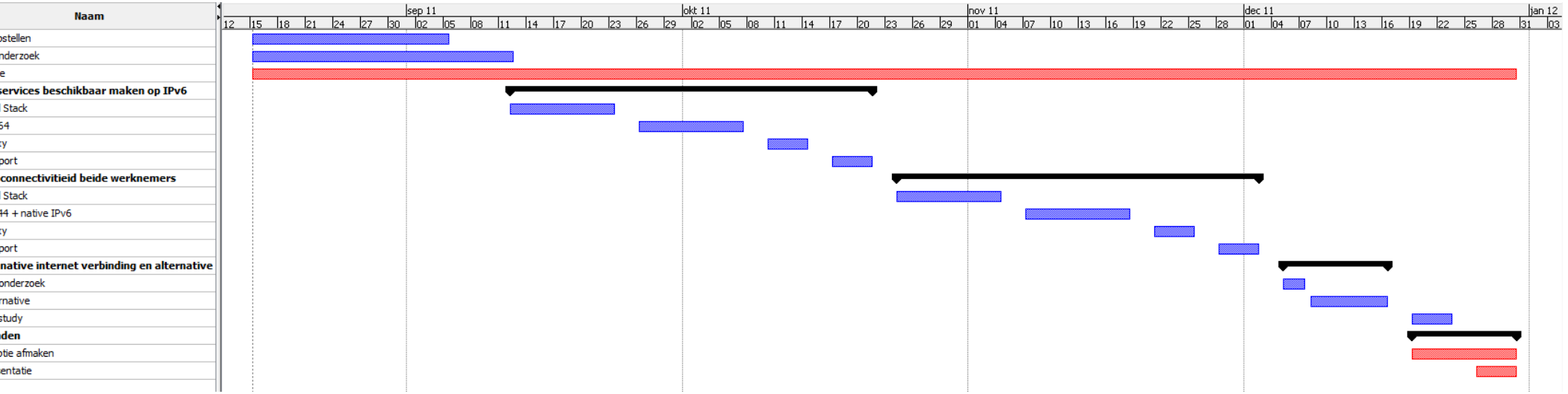
- Week 17 Onderzoek Native IPv6 Internet verbindingen
- week 17-18 Onderzoek Alternatieve IPv6 mogelijkheden
- Week 18 Rapport opstellen

Week 19 Case study

- Week 19 Case, website on-line op IPv6

Week 19-20 Afronding

- Week 19-20 Scriptie afmaken
- Week 20 presentatie


Naam
sep 11
okt 11
nov 11
dec 11
jan 12
12 15 18 21 24 27 30 02 05 08 11 14 17 20 23 26 29 02 05 08 11 14 17 20 23 26 29 01 04 07 10 13 16 19 22 25 28 01 04 07 10 13 16 19 22 25 28 31 03
stellen
nderzoek
e
services beschikbaar maken op IPv6
Stack
64
y
port
connectivitieid beide werknemers
Stack
44 + native IPv6
y
port
native internet verbinding en alternative
onderzoek
rnative
study
den
tie afmaken
entatie

Bijlage D: Opdrachtomschrijving

Gegevens student: ***Informatica / M&S / S /***

Datum:

Studentnr : 2107605

Naam student : Vincent Verheijen

Adres :Gen van Teynstraat 64

Postcode + plaats :5623HP Eindhoven

Telefoon + Mobiel nr : 06-17694190

Email-adres : vincent.verheijen@student.fontys.nl

Email-adres privé (voor alumnibestand): v.verheijen@chello.nl

Voorwaarden om op afstudeerstage te gaan: (*wordt ingevuld door afstudeercoördinator)

Gegevens bedrijf:

Naam stagebiedende organisatie : Simac

Bezoekadres : De Run 1101

Postcode + plaats : 5503 LB Veldhoven

Telefoon : 040 258 29 44

Fax :

Internetadres : www.simac.com

Afdeling : O&E Network Enginering

Naam bedrijfsbegeleider : Luc Aelen

Functie : Network Engineer

Telefoonnummer rechtstreeks : 040 – 258 2274

Emailadres bedrijfsbegeleider : luc.aelen@simac.com

Afstudeerperiode:

Startdatum afstudeerstageperiode: (ZSM)

Einddatum afstudeerstageperiode :

Duo stage: Nee

Stageopdracht goedgekeurd in SAS+: **ja**

Titel van de stageopdracht in SAS+ ***:*** **Ipv6 de eerste echte stappen**

Afstudeeropdrachtomschrijving: **IPv6 de eerste echte stappen**

Een volledige omschrijving van onderstaande vragen kun je vinden in de afstudeerstage brochure,

1. **Beschrijf de probleemanalyse:** (geef aan wat voor het stagebedrijf de aanleiding is geweest om de stageopdracht uit te laten voeren. Wat is voor het stagebedrijf de toegevoegde waarde van de stageopdracht? De beginsituatie en uitgangspunten: inleiding en probleemstelling.)
   De IPv4 internet adressen zijn nagenoeg op. Om te zorgen dat in de toekomst toch iedereen het internet op kan is IPv6 ontwikkeld. Maar hoe manage je de overstap? Hoe zorg je ervoor dat beide technieken naast elkaar kunnen bestaan? Als ICT dienstverlener is Simac een van de eerste bedrijven die met deze vragen concreet aan de slag moet. Een van de eerste vragen die bedrijven stellen is, kunnen mensen met enkel een ipv6 adres straks nog op onze website/webwinkel komen? En kunnen onze werknemers straks op websites komen die enkel via ipv6 beschikbaar zijn?

2. **Beschrijf de afstudeeropdracht.** (m.n. doelstellingen en de op te leveren resultaten en producten van het afstudeerwerk. Geef aan wat je met het uitvoeren van de stageopdracht uiteindelijk voor het stagebedrijf wilt Geef een duidelijke omschrijving van de stageopdracht).

   Realiseer op eenvoudige, kosteneffectieve en veilige wijzen de mogelijkheid om bedrijfswebsites via ipv6 te benaderen, en de mogelijkheid voor werknemers om IPv6-only websites en services te benaderen.

   Als case moet een website op IPv6 bereikbaar worden gemaakt, liefst de corperate website van Simac.
   En tot slot moet worden onderzocht welke mogelijkheden er zijn om een IPv6-enabled internet verbinding te realiseren.

3. **Wat is het onderzoeksaspect binnen de opdracht?** (Wat ga je onderzoeken? Evt. opstellen van een onderzoeksvraag)
   - Welke manieren zijn er om een IPv6 enabled internet verbinding te krijgen?
   - Welke manieren zijn er om de huidige IPv4 web-sites en services ook via IPv6 beschikbaar te maken, en wat zijn de voor en nadelen van elke methode?
   - Welke manieren zijn er om werknemers toegang te geven tot IPv6-only web-sites en services, en wat zijn de voor en nadelen van elke methode?
   - Welke van de hierboven onderzochte methodes zijn het meest geschikt voor Simac en haar klanten.

4. **Wat zijn de methoden en de tools?** (Welke werkwijze en middelen staan jou als afstudeerder ter Beschikking? Welke faciliteiten worden er door bedrijf ter beschikking gesteld?)
   Een eigen werkplek met PC en internet verbinding. Een testlab waar ik cases kan testen. En 2 begeleiders. Verder word ik betrokken bij de al lopende IPv6 werkgroep van Simac.

5. **Welke begeleiding wordt er vanuit het bedrijf gegeven, en welke "betrokkenen" zijn er verder?**
   Er zijn 2 stage begeleiders beschikbaar, Luc Aelen en Tom van Haandel.

6. **Welke vakgebieden spelen een belangrijke rol bij het uitvoeren van de afstudeeropdracht?** (bijvoorbeeld informatieanalyse, ontwerpen, realiseren, beheer en security, ..).
   Onderzoek, (Netwerk)beheer, Security, Realiseren.

7. **Welke POP-aspecten spelen een rol bij het afstuderen?** (welke specifieke taken uit je Persoonlijk OntwikkelingsPlan ga je tijdens het afstuderen uitvoeren?)
   - Plannen en communicatie vaardigheden oefenen en verbeteren.
   - Verdere verdieping netwerken, met namen IPv6.
   - Werkervaring opdoen bij een grotere ICT werkgever.

Bijlage E: Onderzoeksrapport

Simac

Onderwerp	IPV6 – de eerste echte stappen
Opgesteld door:	Vincent Verheijen
Datum:	11 januari 2012
Versie:	1.2

Simac ICT Nederland bv
De Run 1101, 5503 LB Veldhoven
Postbus 340, 5500 AH Veldhoven
Tel. (040) 258 29 11
Fax (040) 258 23 10
Internet: www.simac.com/nl/ict

Inhoudsopgave

1 Inleiding

Dit document heeft tot doel het helpen bij het zetten van de eerste stappen van de overgang naar IPv6. Omdat in Europa de IPv4-adres pool nog niet uitgeput [1] Is op het moment van schrijven zal dit voor de meeste bedrijven drie dingen inhouden. Enerzijds voorbereidingen treffen voor de eerste IPv6-only internet cliënts die men toch toegang wil geven tot de (web) services van het bedrijf. Anderzijds de werknemers toegang geven tot toekomstige IPv6-only services op internet.
En tot slot om de bovenste twee zaken mogelijk te maken, IPv6 connectiviteit realiseren met het internet.

Het document beschrijft een aantal technieken om huidige IPv4 (web-)services beschikbaar te maken op IPv6 en hoe IPv6 connectiviteit geregeld kan worden voor werknemers met enkel een IPv4 connectie.
Van alle technieken zal worden uitgelegd hoe ze werken waarna de voor- en nadelen ervan uiteengezet worden en tegen elkaar worden afgewogen.
Tot slot wordt er ingegaan op hoe bedrijven een native IPv6 connectie kunnen realiseren en wat de alternatieven zijn mocht dit (vooralsnog) niet mogelijk zijn.

Er wordt gekeken naar hoe de gekozen technieken toe te passen bij bestaande IPv4-only netwerken en wat te doen bij nieuwe situaties waarbij er vanuit wordt gegaan dat het netwerk verkeer nog voor een aanzienlijk deel uit IPv4 zal bestaan. IPv6-only sites vallen daarom buiten de scope van dit rapport.

Security is een belangrijke overwegen bij het maken van de keuze voor een bepaalde transitie techniek. Daarom wordt er ook uitgebreid op security in gegaan. maar dit is geen diepgravend security onderzoek.

2 Vooronderzoek

Er zijn in de loop der jaren sinds de standaardisering van IPv6 een aantal transitie technieken bedacht om de overgang van IPv4 naar IPv6 te ondersteunen. In het vooronderzoek wordt een voorselectie gemaakt.
Elke techniek wordt kort beschreven en vervolgens is gekeken of deze toepasbaar is op een of meer van de doelstellingen van dit rapport, de onderzoeksvragen.

Deze vragen zijn:

1. huidige IPv4 (web-)services beschikbaar maken voor IPv6-only internet cliënts
2. huidige IPv4 hosts/werknemers toegang geven tot IPv6-only (web-)services op internet
3. native IPv6 internetverbinding realiseren en mogelijke alternatieven aandragen mocht dit niet mogelijk zijn.

Het Centrale probleem bij vraag 1 is dat IPv6-only hosts verbinding moet kunnen maken met de voor als nog IPv4-only webservers. Een IPv6 naar IPv4 verbinding dus. Vraag 1 zal daarom verkort worden weergegeven als "Web services IPv6→IPv4".

Voor vraag 2 geld dat de nu nog IPv4 werknemers verbinding moeten kunnen leggen met IPv6-only servers. Een IPv4 naar IPv6 verbinding.
Vraag 2 zal daarom worden verkort tot "werknemers IPv4 → IPv6"

Vraag 3 zal worden verkort tot "IPv6 connectiviteit", waarmee bedoeld word dat er connectiviteit word gerealiseerd met het IPv6 internet.

<u>IETF RFC status</u>
RFC's zijn een bekend fenomeen bij iedereen die met netwerken werkt.
Minder bekent is het verschil in status tussen de verschillende RFC's en wat ze betekenen.
De status van een RFC kan een belangrijk criterium zijn om wel of niet voor een techniek te kiezen.
De belangrijkste statussen zijn die van de "standards track". RFC's in deze track zijn uitgeroepen tot internet standaard of zijn op weg om dat te worden. Tot 2011 had deze "standards track" drie statuslevels, maar dat is dat jaar gereduceerd tot twee, de "proposed standards" en de "Internet Standards".
Mogelijke nieuwe standaarden beginnen met de status "Proposed standard". Deze zijn stabiel, goed begrepen en doorgrond, zijn uitvoerig bekeken door de industrie en zij hebben vandaaruit voldoende bijstand gekregen om interessant gevonden te worden. Implementaties of operationele ervaring is niet persé noodzakelijk.
"Internet Standard" is de hoogst haalbare van de twee, maar om deze te halen moet een standaard door meerdere vendors zijn geïmplementeerd en moet er voldoende operationele ervaring mee zijn opgebouwd. Geen enkele IPv6 transitie techniek heeft daarom deze status bereikt op moment van schrijven. De IPv6 standaard zelf is ook nog niet verder gekomen als proposed standaard.

De andere drie statussen van belang voor dit onderzoek, die zich buiten het standardstrack bevinden zijn experimental, informational en historic.
De namen van de eerste twee statussen spreken vrijwel voor zich. Experimental betekent precies dat en wordt niet aangeraden voor gebruik in productieomgevingen. De standaard is nog niet goed doorgrond en nog aan mogelijke veranderingen onderhevig.

informational betekent dat een document relevante informatie bevat over veel verschillende onderwerpen, maar geen nieuwe standaard.
De laatste status die van belang is, is historic. Met deze status wil het IETF zeggen dat deze techniek verouderd is, niet meer van belang voor het huidige internet is of omdat men het gebruik ervan om andere redenen afraad.

Provider independent address space
Met IPv4 is het gebruikelijk voor een middel- tot groot bedrijf om een eigen IP range the hebben. Maar tot voor kort beschikte IPv6 niet over een dergelijke mogelijkheid.
Het was enkel mogelijk om Provider aggregated adressen (PA adressen) te krijgen. Deze hebben echter een aantal nadelen.
De voornaamste hiervan is dat bij een providerwissel omnummering noodzakelijk is. En ook al zou dat betekenen dat enkel de IPv6 prefix veranderd zou moeten worden, dan is dat nog niet zo eenvoudig als de IETF ooit voor ogen had. De tools om dat mogelijk te maken zijn echter niet of nauwelijks verschenen. Met name de mogelijkheid om dit netwerkbreed te doen is nooit verschenen.
Ook multi-homing met dergelijke PA address ranges is moeilijker dan dat het was met IPv4. Hoewel er verschillende methodes in ontwikkeling zijn, zijn deze nog niet klaar voor gebruik, laat staan breed ondersteund.

In Europa (via RIPE-NCC) is het inmiddels echter mogelijk om een PI adres te krijgen, mits aan een aantal voorwaarden wordt voldaan [2].
Iedereen die aan de eisen voldoet kan standaard een /48 krijgen. Een kleinere prefix is mogelijk als hiertoe een goede reden is.
Met een PI adres is omnummering bij een providerwissel niet langer noodzakelijk.
Ook is het op dit moment de enige oplossing multi-homing te kunnen doen op IPv6.
Maar PI address space is pas nuttig als het ook gerouteerd kan worden op internet.
Hiervoor is het noodzakelijk dat prefixen tot /48 worden gerouteerd. Voorheen was de kleinst gerouteerde prefix echter /32.
Inmiddels is echter het routeren van /48 bij het overgrote deel [3] (menselijk leesbaar [4]) van de backboneprovider ondersteund en lijkt daarmee ook algemeen geaccepteerd.
Ondersteuning is voor PI address space is dus een belangrijk criteria in het vergelijken van de verschillende transitie technieken.

2.1 **Dual stack**

toepassing	Dual stack
Webservers IPv6→IPv4	
Werknemers IPv4→IPv6	
IPv6 connectiviteit	

Dual stack wordt beschreven in RFC4213 [5] en heeft de status van proposed standard.
Dual stack betekent dat een host zowel een IPv4 als een IPv6 adres gebruikt. Zo kan deze met beide communiceren zonder dat er enige vertaling hoeft plaats te vinden.

Samen met 6in4 tunneling (een implementatie van protocol-41) is Dual stack de oudste en meest ondersteunde transitietechniek bij de IETF (Internet Engineering Task Force). Het is de techniek die zowel de IETF als Cisco aanraden [6] om te gebruiken waar mogelijk op weg naar een IPv6 toekomst.
Als Cisco goldpartner heeft Simac na zorgvuldig beraad deze aanbeveling overgenomen als visie voor de lange termijn toekomst.

Dual stack is ook van toepassing op alle 3 de vraagstukken. Voor web services en werknemers betekent het, dat deze zowel op IPv4 als met IPv6 kunnen communiceren in beide richtingen. Voor IPv6 connectiviteit bied dual stack de mogelijkheid om zowel een IPv4 als IPv6 adres te krijgen over één internet verbinding, mitst de ISP beide kan leveren. De verwachting is dat de meeste ISP voor deze optie zullen kiezen
Om deze redenen zal deze techniek uitgebreid worden behandeld.

2.2 **Translatie technieken**

Een alternatieve aanpak voor dual stack is translatie. Translatie is een techniek waarbij IPv6 packet-headers worden omgezet in IPv4 packet-headers en visa versa. Vaak gecombineerd met porttranslatie om de verschillende lopende verbindingen van elkaar te kunnen onderscheiden.
Het vertalen van de headers en ICMP is vastgelegd in RFC6145 [7].
Het format voor het omzetten van de adressen is vastgelegd in RFC6052 [8].

Een overzicht van de toepasbaarheid van translatie is te vinden in RFC6144 [9].
In hoofdstuk 2 van deze RFC staan verscheidene scenario's beschreven, waarvan er 2 relevant zijn voor dit onderzoek:
Scenario 3 (hoofdstuk 2.3) is van toepassing op onderzoeksvraag 1 (web services).
Dit scenario beschrijft het IPv6 internet dat verbinding maakt met een IPv4 netwerk.
Scenario 4 (hoofdstuk 2.4) is van toepassing op onderzoeksvraag 2 (werknemers)
In dit scenario wordt beschreven hoe een IPv4 netwerk verbinding maakt met het IPv6 internet, waarbij gelijk moet worden opgemerkt dat dit scenario moeilijk te bewerkstelligen is voor translatietechnieken.

2.2.1 NA(P)T-PT

toepassing	NA(P)T-PT
Webservers IPv6→IPv4	
Werknemers IPv4→IPv6	
IPv6 connectiviteit	

NA(P)T-PT wordt beschreven in RFC 2766) [10] welke "Historic" is verklaard door RFC 4966 [11].
De Historic status betekend dat deze techniek niet meer wordt ontwikkeld, ondersteund, of aangeraden door het IETF.
Deze techniek bood in theorie een oplossing voor zowel scenario 3 (web services) als scenario 4 (werknemers) zoals beschreven in RFC6144 [9]. Maar uiteindelijk probeerde men met NAT-PT te veel zaken tegelijk op te lossen.
Zeker het gedeelte van IPv4 naar IPv6 (scenario 4/werknemers) was problematisch om meerdere redenen. De voornaamste hiervan is dat het ALG's en DNS translatie van praktisch al het verkeer vereist. Hierdoor bleek het een dure en weinig schaalbare oplossing. De Historic status alleen al is genoeg om deze techniek te diskwalificeren.

Het gedeelte van IPv6 naar IPv4 (scenario 3/webservices) was echter wel bruikbaar en is opnieuw uitgekomen als standaard in de vorm van NAT64 en DNS64.

2.2.2 NAT64

NAT64 wordt soms ook als xlate aangeduid.
De voorlopers van NAT64, NAT-PT en NAPT-PT zijn Historic verklaard (RFC 4966) [11]).
NAT64 is een flink vereenvoudigde variant van deze methodes met beperktere mogelijkheden.
Door het vereenvoudigde karakter van NAT64 heeft het echter een groot aantal van de zwaktes van zijn voorlopers niet. De Single-point-of-failure en de beperkte schaalbaarheids problemen van NA(P)T-PT zijn niet van toepassing op NAT64.
NAT64 is er in 2 vormen, stateless en stateful. Beide hebben hun eigen voor- en nadelen en toepassingsgebieden.

2.2.2.1 Nat64 Stateless (SIIT)

toepassing	Stateless NAT64
Webservers IPv6→IPv4	
Werknemers IPv4→IPv6	
IPv6 connectiviteit	

Stateless NAT64 wordt beschreven in RFC 6145 [7] en heeft de status van proposed standard.
In tegenstelling to andere vormen van stateless NAT is stateless NAT64 ook daadwerkelijk volledige stateless. Het is dus een heel schaalbare techniek die weinig overhead met zich mee brengt.
Maar stateless NAT64 kan alleen werken als deze de adressen van zowel source als destination zonder verdere informatie om kan zetten van IPv4 naar IPv6 en visa versa.
Dat betekend dat hij aan het IP adres moet kunnen zien hoe deze omgezet moet worden.
Het omzetten van een IPv4 adres naar IPv6 is altijd mogelijk en hier zijn verschillende manieren voor, maar andersom kan dat enkel als het IPv6 adressen aan speciale eisen voldoet. Zo'n IPv6 adres wordt een IPv4-translatable IPv6 adres genoemd en wordt beschreven in RFC6052 [8]. De Ipv6 adressen op internet voldoen niet aan deze eis, en daarom valt deze techniek af voor alle 3 de vraagstukken.
Deze techniek word daarom niet verder behandeld.

2.2.2.2 Nat64 Stateful

toepassing	Stateful NAT64
Webservers IPv6→IPv4	
Werknemers IPv4→IPv6	
IPv6 connectiviteit	

Stateful NAT64 wordt beschreven in RFC 6146 [12] en heeft de status van proposed standard.
Heel vergelijkbaar met NAT44. NAT44 laat meerdere IPv4 hosts één public IPv4 adres delen. NAT64 laat meerdere IPv6-only hosts één IPv4 adres delen. Samen met DNS64 geeft het meerdere IPv6-only hosts toegang tot het IPv4 internet met maar één IPv4 adres in gebruik.
Van uitgaande verbindingen wordt informatie bijgehouden op de NAT64 router zodat het terugkomende antwoord door de router naar de juiste host gestuurd kan worden. Hierdoor is stateful NAT64 niet gebonden aan de RFC6052 [8] adressen zoals Stateless NAT64 dat is.

In combinatie met port forwarding of static routing toepasbaar op vraagstuk één webservices. (DNS64 is hierbij niet nodig)

2.3 Proxy/ALG

toepassing	Proxy/ALG
Webservers IPv6→IPv4	
Werknemers IPv4→IPv6	
IPv6 connectiviteit	

Hoewel niet een officiële IETF transitie standaard als zodanig, is het toch een belangrijke variant om naar te kijken.
Dit is de enige transitie techniek die de mogelijkheid biedt IPv4-only host/servers met IPv6-only hosts/servers (en visa versa) te laten communiceren met protocollen die IP adressen embedden in de data, mitst de proxy server hier ondersteuning voor heeft.
Het nadeel is dat er per programma/protocol ondersteuning moet zijn in de Proxy server.

Ondanks dat proxies geen officiële IETF transitie techniek is, ligt er wel een specifieke RFC voor een FTP ALG met translatie mogelijkheid: RFC6384 [13].

2.4 Load balancers

Load balancers worden ook regelmatig aangedragen als techniek om IPv4 web services beschikbaar te maken op het IPv6 internet. Ze zijn niet als aparte techniek meegenomen in dit onderzoek omdat ze, afhankelijk van het type, nagenoeg hetzelfde doen als of NAT64 of reverse proxies.
Er zijn 2 type Load balancers, namelijk: de laag 4 balancers en de laag 7 balancers.

Laag 7 Load balancers doen nagenoeg het zelfde als reverse proxies.
De nadruk bij een reverse proxy ligt op het caches van data om de workload van een webserver te verminderen, waar een load balancer de connecties verdeeld over meerdere webservers en strikt genomen niet aan caching doet. Door de grote overeenkomsten zijn de functies van beiden vaak gecombineerd in één apparaat of softwarepakket.
Laag 7 load balancers kunnen ook adrestranslatie doen en hiervoor gelden precies dezelfde voor- en nadelen als voor de reverse proxyservers.
de laag 4 load balanceren zijn wat de IPv6 transitie betreft gelijk aan een NAT64 implementatie met ook hier precies dezelfde voor- en nadelen.

Cisco heeft recentelijk ondersteuning aangekondigd voor IPv4-IPv6 translatie (in beide richtingen) voor hun ACE systemen [14]. Op laag-4 worden alle protocollen ondersteund die geen IP adressen in de payload hebben en op laag 7 worden enkel HTTP en SSL(HTTPS) ondersteund.

2.5 Tunnels

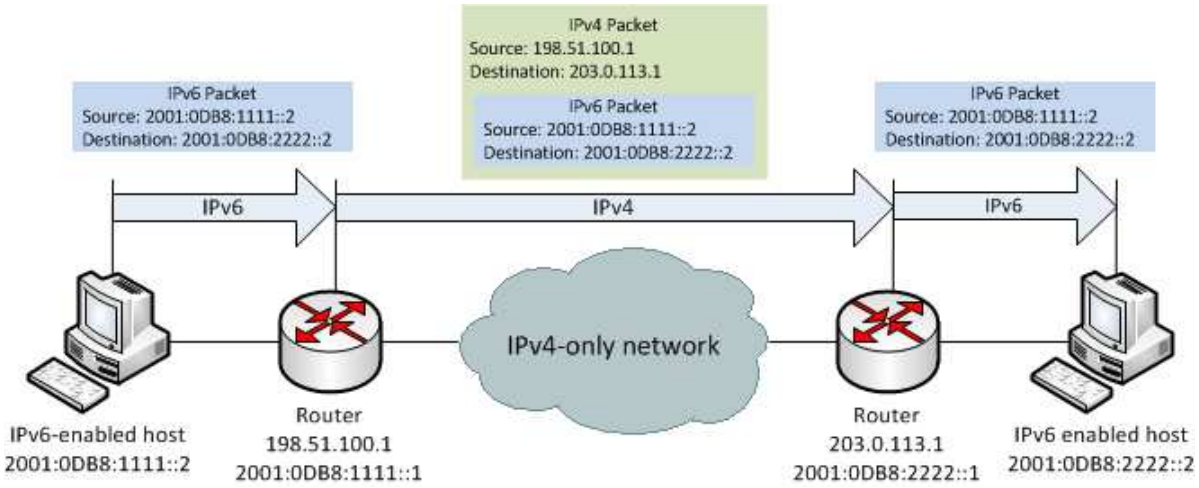
Hier worden een aantal tunnel technieken beschreven en hoe die van toepassing kunnen zijn op de 3 vraagstukken of waarom juist niet. Een tunnel kan zowel een oplossing zijn als enkel een ondersteuning van een andere techniek. In relatie met de vraagstukken zullen de tunneltechnieken worden gebruikt om IPv6 verkeer te transporteren over IPv4 netwerken/internet. Andersom is ook mogelijk maar is niet relevant voor dit onderzoek.

2.5.1 static tunnels

toepassing	Static Tunnels
Webservers IPv6→IPv4	
Werknemers IPv4→IPv6	
IPv6 connectiviteit	

Static of configured tunneling word beschreven in RFC4213 [5] en heeft de status van proposed standard.
Deze tunnels worden ook vaak 6in4 tunnels genoemd.
Techniek is van toepassing op alle drie de vraagstukken.
Tunnels met 2 vaste uiteinden gebaseerd op IP adres.
Static tunnels maken gebruik van protocol-41 ,waarin een IPv6 packet in een IPv4 packet word gestopt of andersom, wat encapsulation/encapsulatie wordt genoemd. Beide uiteinden van de tunnel moeten expliciet geconfigureerd worden.

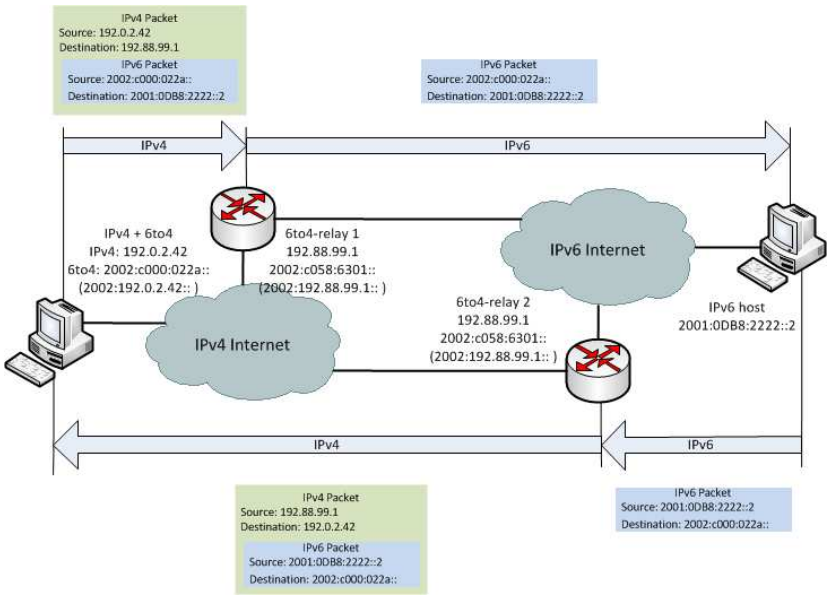
Bij de uitrol van dual stack kunnen deze tunnels gebruikt worden om een gefaseerde uitrol te ondersteunen door delen van het netwerk die men nog niet kan of wil dual stacken te overbruggen. Bij kleinere aantallen tunnels zijn static tunnels relatief snel op te zetten en geven duidelijke, overzichtelijke en voorspelbare resultaten. Hierdoor zijn voor deze tunnels ook heel specifieke regels aan te maken in access lists en firewall configuraties, waar bij andere tunnel-technieken vaak minder specifiek te werk kan worden gegaan. Dit maakt dat static tunnels tot de veiligere opties behoren wat tunneling betreft.
Om deze redenen zijn static tunnels in veel gevallen een goede keuze en worden daarom meegenomen in het onderzoek.
In combinatie met een tunnelbroker kunnen static tunnels worden gebruikt voor vraagstuk 3.



2.5.2 6to4

toepassing	6to4
Webservers IPv6→IPv4	
Werknemers IPv4→IPv6	
IPv6 connectiviteit	

6to4 wordt beschreven RFC 3056 [15] en heeft de status van proposed standard.
Een techniek die automatische tunneling (proto-41) gebruikt om sites die geen native IPv6 internet verbinding hebben toch toegang tot het IPv6 internet te geven, als zij tenminste een global IPv4 adres hebben.
Elke host met een global IPv4 adres kan zijn eigen 6to4 IPv6 adres maken door de 6to4 prefix (2002::/16) te koppelen aan het eigen IPv4 adres. Samen vormt dat een /48 prefix.
Voor 6to4 host naar 6to4 host communicatie wordt rechtstreeks getunneld naar het IPv4 adres dat in het IPv6 destination address zit verwerkt.
Voor 6to4 host naar het IPv6 internet wordt gebruikt gemaakt van 6to4 (border)routers (ook wel 6to4 relay's of relay servers genoemd). Deze zijn te vinden op internet en zijn te bereiken via de IPv4 anycast adres range 192.88.99.0/24. Zo wordt altijd de dichtstbijzijnde 6to4 router gebruikt om te zenden.
Om communicatie de andere kant op mogelijk te maken adverteert elke 6to4 router routing voor 2002::/16. Als de router een IPv6 packet binnen krijgt voor een 6to4 host zal deze het embedded IPv4 adres gebruiken om het IPv6 packet te encapsuleren en het over IPv4 naar de desbetreffend host te sturen.



Door de relatief kleine vaste prefix van /48 kan één 6to4 connectie worden gebruikt voor meerdere /64 subnetten en is daarom geschikt voor gebruik bij vraagstuk 3, internet connectiviteit.
Omdat alle gangbare werkstation besturingssystemen 6to4 tunnels ondersteunen zou 6to4 ook geschikt kunnen zijn voor vraagstuk 2 maar dit wordt sterk afgeraden.
Voor die toepassing zou elke werkstation op het netwerk een 6to4 eindpunt moeten zijn. Daarvoor moeten Protocol-41 verbindingen van en naar elke adres, binnen of buiten het netwerk, door de firewall gelaten worden. Vanuit veiligheidsoogpunt is dat niet te accepteren aangezien de inhoud van deze protocol-41 tunnels niet of nauwelijks te controleren is. Elk werkstation is dan rechtstreeks bereikbaar vanaf internet zonder de controle van de netwerk firewall. Een software firewall op elk werkstation is niet afdoende als firstline verdediging en bovendien arbeidsintensief in onderhoudt.
Het is sterk aan te bevelen om het 6to4 eind punt voor of op de firewall te houden zodat alle connecties die uit de 6to4 tunnel komen op de zelfde manier gecontroleerd en beveiligd kunnen worden als die van de reguliere internetverbinding.
Dat is de reden om deze techniek alleen aan te bevelen voor het bieden van IPv6 connectiviteit.

2.5.3 6RD

toepassing	6RD
Webservers IPv6→IPv4	
Werknemers IPv4→IPv6	
IPv6 connectiviteit	

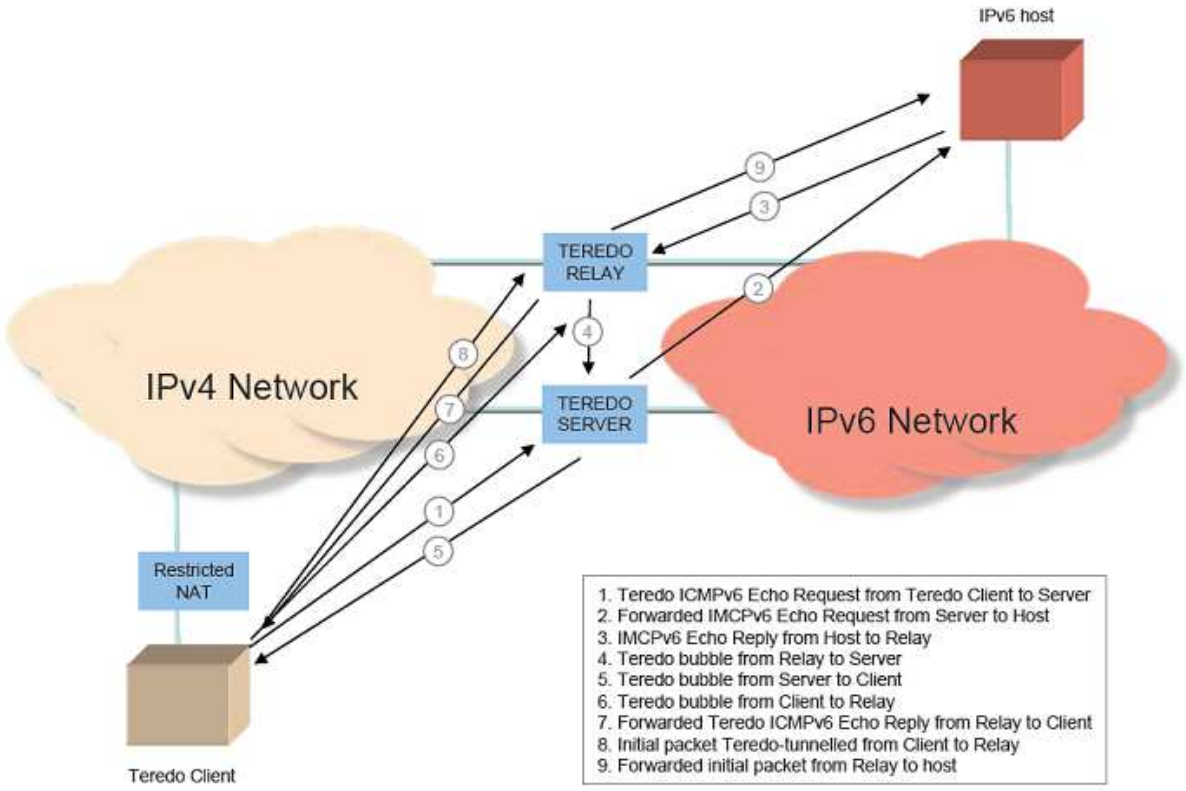
6RD wordt beschreven in RFC 5569 [16] en heeft de status van informational.
Eigenlijk is 6RD het zelfde als 6to4 maar zonder een aantal van zijn beperkingen in ruil voor een kleinere toepasbaarheid (6RD is gericht op een ISP's interne netwerk).
In 6RD wordt de relayserver (ook een 6RD gateway genoemd) echter binnen het eigen netwerk geplaatst zodat deze nu beheerbaar is. De kwaliteit van de geleverde verbinding is daarmee geheel onder de controle van netwerkbeheer en niet langer onbeheersbaar zoals bij 6to4. Ook vervalt de eis van een verplichte 2002:: prefix en de noodzaak om het hele IPv4 adres in het IPv6 adres te verwerken. Het is mogelijk voor een bedrijf om bijvoorbeeld zijn eigen IPv6 prefix (inclusief een eigen PI prefix) hiervoor te gebruiken. En door het deel van het IPv4 adres weg te laten dat voor alle hosts binnen het bedrijf geldt zijn er minder bits nodig om het IPv4 adres van de host in het IPv6 adres te verwerken, waardoor er meer ruimte over kan blijven voor subnetting.
Het en- en decapsuleren gebeurt bij een ISP uitrol in de modem/router die bij de klant staat. Om deze reden is er ook geen ondersteuning in Windows en OSX, zoals dat wel het geval is bij 6to4 (al is er wel een Linux implementatie). Bij een uitrol in het bedrijfsleven kan de default gateway/router van het netwerksegment deze taak overnemen.

Met 6RD kan IPv6 snel worden uitgerold voor grote groepen gebruikers, maar als IPv6 ook word gebruikt voor het interne netwerkverkeer zal dit ook allemaal via de 6RD gateway lopen. Het is duidelijk dat dit een potentiële bottleneck is. Puur naar vraag 2 kijkend kan 6RD een goede oplossing zijn, maar met een bredere blik kijkend naar een algehele IPv6 deployment is duidelijk dat 6RD gemakkelijk een bottleneck vormt bij gebruik in een bedrijfsnetwerk.
Het gebruik van 6RD voor bedrijfsnetwerken wordt daarom afgeraden.

2.5.4 Teredo

toepassing	Teredo
Webservers IPv6→IPv4	
Werknemers IPv4→IPv6	
IPv6 connectiviteit	

Teredo wordt beschreven in RFC 4380 [17] en heeft de status van proposed standard.
Teredo heeft in zijn opzet veel weg van 6to4 maar gebruikt UDP I.P.V. van protocol-41 en vereist geen public IPv4 adres, maar kan ook achter een NAT met een private IPv4 adres werken.
Teredo is ontwikkeld door Microsoft als laatste redmiddel om IPv6 connectiviteit te krijgen achter een NAT als andere methodes niet mogelijk zijn.
Om dit te bereiken zijn er naast de relay servers, vergelijkbaar met die van 6to4, ook Teredo servers nodig om de NAT piercing uit te voeren.
Een Teredo host heeft altijd een /128 IPv6 adres, omdat er naast de vaste Teredo prefix (2001:0000::/32) ook het public ipv4 adres van het netwerk, het IPv4 van de Teredo server en de gebruikte UDP port in het adres verwerkt moeten worden, samen met nog een aantal flags om het NAT type aan te duiden.



Hierdoor kan er dus niet meer dan 1 host zijn per Teredo tunnel eindpunt.
Dit maakt Teredo meteen ongeschikt voor vraagstuk drie, IPv6 connectiviteit.
Hoewel Teredo wel geschikt zou kunnen zijn voor vraagstuk twee, werknemers, betekent de /128 dat elke werknemer een Teredo eind punt moet zijn. Hierdoor zijn ze rechtstreeks bereikbaar

vanaf internet zonder de controle van de netwerk firewall, die de inhoud van het encapsulated packet niet of nauwelijks kan controleren. Deze firewall moet ook alle tunnels van en naar elke host, in beide richtingen, in alle gevallen doorlaten. Dit maakt Teredo onacceptabel op het gebied van veiligheid voor het werknemersvraagstuk.

Hoewel het kleinere hoeveelheid servers de veiligheidsproblemen van Teredo iets hanteerbaarder zou kunnen maken is ook het hosten van services via Teredo af te raden, gezien een eerder intern rapport van Simac. Onder andere omdat het IPv6 adres niet constant was en de gemaakte verbinding niet betrouwbaar was (packetloss).
Teredo is ontwikkeld als laatste redmiddel en zo moet het ook gezien worden. Het biedt geen structurele oplossingen.
Het gebruik van Teredo wordt daarom in alle gevallen sterk afgeraden.

2.5.5 ISATAP

toepassing	ISATAP
Webservers IPv6→IPv4	
Werknemers IPv4→IPv6	
IPv6 connectiviteit	

ISATAP wordt beschreven in RFC4214 [18] en heeft de status Experimental
ISATAP staat voor Intra-Site Automatic Tunnel Addressing Protocol. Het is een tunnelingprotocol om binnen een site een IPv6 netwerk te kunnen opzetten zonder de huidige IPv4 netwerkapparatuur aan te hoeven passen. Een toevoeging in de locale DNS servers en het neerzetten van een ISATAP router is genoeg om alle computers on site met elkaar te kunnen laten praten via IPv6. ISTATAP gebruikt een vaste prefix van fe80:0000:0000:0000:0200:5efe: (globaly unique) of fe80:0000:0000:0000:0000:5efe: (private)
Omdat deze prefix deel uitmaakt van de FE80:: /16 prefix zijn ISATAP adressen niet routeerbaar, wat internet connectiviteit uitsluit. Dit maakt deze techniek ongeschikt voor alle drie de vraagstukken. Deze techniek wordt daarom niet verder behandeld.

2.5.6 DS-lite

toepassing	DS-lite
Webservers IPv6→IPv4	
Werknemers IPv4→IPv6	
IPv6 connectiviteit	

DS-lite wordt beschreven in RFC6333 [19] en heeft de status van proposed standard.
DS-lite staat voor Dual stack light. Het is een techniek waarbij er een native IPv6 netwerk public IPv6 adressen en private IPv4 adressen uitdeelt aan de netwerkrouters. Al het IPv4 verkeer zal worden getunneld naar de een on-site CGN of NAT44 router over het IPv6-only netwerk.
Deze techniek is ontwikkeld voor zogenaamde “greenfield” situaties: Netwerken die enkel nog IPv6 gebruiken. Zelfs voor nieuw aan te leggen netwerken is het voorlopig echter nog niet verstandig om enkel IPv6 te gebruiken. IPv4 maakt naar alle waarschijnlijkheid nog een te groot deel van de communicatie uit die allemaal, zowel intern als extern, via de CGN moet lopen. Daarbij is de ervaring met het implementeren van IPv6 is voor de meeste bedrijven nog te gelimiteerd en het vertrouwen in de IPv6 implementaties is nog niet opgebouwd.
Deze techniek is dus niet geschikt voor gebruik bij het oplossen van de vraagstukken en wordt niet verder behandeld.

2.6 **Overzicht en conclusies**

Hieronder volgt een overzicht van de toepasbaarheid van elke techniek per onderzoeksvraag. Groen en oranje geven aan dat een techniek voor deze toepassing gebruikt kan worden. Maar oranje betekend ook dat er grote nadelen zijn aan het gebruik van deze techniek voor een bepaalde toepassing.
Rood geeft aan dat deze techniek in het geheel niet bruikbaar is voor een bepaalde toepassing.

Toepasbaarheid per vraagstuk:

toepassing	Dual stack	NAT-PT	Stateless NAT64	Stateful Nat64	Proxy/ALG	Static Tunnel	6to4	6RD	Teredo	ISATAP	DS-Lite
Webservers IPv6→IPv4											
Werknemers IPv4→IPv6											
IPv6 connectiviteit											

Legenda
Groen: toepasbaar
Oranje: toepasbaar maar afgeraden
Rood: niet toepasbaar/ niet ondersteund

Alle groen gemarkeerde technieken zijn toepasbaar op 1 of meer van de onderzoeksvragen zonder dat deze gelijk grote nadelen met zich mee brengen. Deze technieken zijn uitgekozen om verder te onderzoeken.
Een overzicht van alle afwegingen die gemaakt zijn per techniek staat in de tabel op de volgende pagina. De uitleg is op de pagina erna te vinden.

Techniek	IETF status	Adres/prefix ondersteuning	Alleen bedoeld voor IPv6-only netwerken	Schaalbaarheid/ bottleneck issues?	Beheersbaarheid	Structurele Beveiligingsissues
Dual stack	proposed standard	alle	nee	nee		nee
NAT-PT	Historic	alle	nee	ja	toekomstige support onzeker	nee
Stateless NAT64	proposed standard	Enkel IPv4-converted IPv6 adressen	nee	nee		nee
Stateful NAT64	proposed standard	alle	nee	nee		nee
Proxy/ALG	Geen/N.V.T.	alle	nee	nee		nee
Static tunnel	proposed standard	alle	nee	nee		nee
6to4	proposed standard	Vaste prefix	nee	nee	Niet alles is beheersbaar	Verminderde controle
6RD	Informational	Elke custom Prefix + (deel van) IPv4 adres	nee	ja		nee
Teredo	proposed standard	Vaste prefix en Enkel /128	nee	nee	Niet alles is beheersbaar. veel tunnel eindpunten.	Niet controleerbare tunnels door de firewall. veel tunnel eindpunten.
ISATAP	Experimental	Vaste prefix niet routeerbaar	nee	nee		Nee
Ds-Lite	proposed standard	IPv6 Alle, private IPv4	ja	ja		nee

Groen: goede ondersteuning/geen structurele issues
Orange: toepasbaar maar met, mogelijk aanzienlijke, nadelen.
Rood: Onoverkomelijk/inherent niet te accepteren nadeel

IEFT status
De Historic status betekend dat deze techniek is afgeraden door het IETF. Dat betekend dat zelfs als er ondersteuning is bij bijvoorbeeld Cisco op dit moment, die in de toekomst kan verdwijnen met nieuwe software versies of nieuwe hardware. Een investering in deze techniek is dus een groot risico.
De experimentele status van ISATAP hoeft geen probleem te zijn. Experimenteel kan veranderen in een opwaardering naar de standardstrack. Maar hij het ook evengoed niet halen. Een risico dus, maar zeker niet zo groot als die van een techniek die al Historic is.

Adres/prefix ondersteuning
Stateless NAT64 kan maar met één bepaald soort IPv6 adres om gaan. De adressen op internet voldoen niet aan deze norm waardoor stateless NAT64 niet bruikbaar is voor de vragen in dit onderzoek. ISATAP's vaste en niet routeerbare maakt het eveneens ongeschikt.
6to4 en Teredo hebben een vaste prefix en kunnen daarom niet gebruikt worden in combinatie met een PI adres range. Een aanzienlijk nadeel, maar het maakt de technieken niet onbruikbaar.
6RD kan wel gebruik maken van een PI adres range, maar een deel van de overgebleven sub-netting ruimte zal moeten worden gebruikt om een (deel van) het IPv4 adres in te verwerken. Iets om rekening mee te houden, maar dat maakt het niet onbruikbaar.
DS-lite werkt enkel met private IPv4 adressen. Opnieuw iets om rekening mee te houden.

Alleen bedoeld voor IPv6-only netwerken
DS-lite maakt gebruik van een IPv6 infrastructuur waar bovenop het IPv4 netwerk is gebouwd door middel van tunneling. Een IPv6 infrastructuur op dit moment, nu er nog weinig tot geen operationele ervaring is met IPv6 is niet te verantwoorden. Daarbij is er geen rechtstreekste overgang naar DS-lite mogelijk voor een bestaand IPv4 netwerk. Dit is de hoofdreden om Ds-lite niet aan te raden, en niet mee te nemen in het verdere onderzoek.

Schaalbaarheid/ bottleneck issues?
NAT-PT, 6RD en DS-lite gebruiken alle drie interne gateways waar een aanzienlijke deel, zo niet al het interne verkeer van het gehele netwerk doorheen moet. Dit is niet schaalbaar of kosten effectief te maken, en daarom vallen alle 3 deze technieken af voor de rest van dit onderzoek.

Beheersbaarheid
NAT-PT's historic status maakt dat de toekomstige support voor deze techniek erg onzeker is, en daarmee onbeheersbaar. Het afsluiten van SLA's met deze techniek in zich zal daarom moeilijk zijn en niet te garanderen. Daarom valt deze techniek ook op dit onderdeel af.
Teredo is afhankelijke van zowel een relay gateway, als een teredo server voor het maken van verbindingen, waarbij beide per host op internet kunnen verschillen. Geen van beide is dus te op enige manier te beheersen. Daarbij zorgt het /128 adres ervoor dat er te veel tunnel eindpunten zijn, die allemaal een risico vormen en daarom goed afgeschermde moeten worden. Dit is niet of nauwelijks kosten effectief en beheersbaar te implementeren. Daarom valt Teredo ook af op dit onderdeel.
6to4 maakt ook gebruik van relay servers op internet die niet beheersbaar zijn, maar heeft niet de andere nadelen van Teredo. De onbeheersbaarheid van 6to4 relay servers is zeker een nadeel, maar maakt de techniek nog niet geheel onbruikbaar.

Structurele Beveiligingsissues

Om Teredo te gebruiken moet de firewall zo zijn ingesteld dat deze protocol-41 (tunnel) connecties van en naar het netwerk van buitenaf door laat. De inhoudt van deze tunnels is niet of nauwelijks te controleren wat dus een enorm veiligheidsrisico vormt. Het vergroot de kans op succesvolle aanvallen enorm omdat er zo veel meer hosts zijn die rechtstreeks aangevallen kunnen worden.

6to4's relay servers geven de mogelijkheid tot man in het middel attacks. Je moet er op vertrouwen dat de ISP van diegenen waarmee verbinding wordt gemaakt een betrouwbare relay server heeft gekozen om 6to4 verkeer heen te leiden.

Conclusies

Voor Dual stack, stateful NAT64, proxy/ALG, en static tunnels zijn in dit vooronderzoek geen grote nadelen naar voren gekomen, en deze worden daarom allemaal meegenomen in het vervolgonderzoek.

6to4 heeft een aantal nadelen waar duidelijk rekening mee gehouden moet worden, maar geen ervan groot genoeg om de techniek af te keuren in het vooronderzoek. Ook deze techniek wordt mee genomen in het vervolgonderzoek.

3 Gekozen technieken

In dit hoofdstuk worden alle technieken uit het vorige hoofdstuk die toepasbaar en relevant waren uitgebreid in het algemeen beschreven.
Er wordt uitgelegd wat de voor- en nadelen van de techniek in het algemeen zijn en hoe die passen in een bredere uitrol van IPv6 binnen het bedrijfsnetwerk.
Later in het document zullen de technieken nog een keer specifiek beschreven worden voor de verschillende toepassingen en alle voor en nadelen worden opgesomd die betrekking hebben op die toepassing.

3.1 **Dual stack**

Dual stack word beschreven in RFC4213 [5]. De netwerk hardware heeft twee IP adressen, een IPv4 adres en een IPv6 adres. In de meeste gevallen hebben ze op dezelfde netwerk aansluiting. Met een dual stack host word een host bedoeld met een globaly unique public IPv6 adres en een globaly unique public IPv4 adres of een private IPv4 adres achter een NAT.
Hoewel het IPv6 adres ook NAT-ed zou kunnen zijn, is hier geen officiële standaard voor, enkel het experimentele NAT66 beschreven in RFC6296 [20].
NAT op IPv6 wordt vaak gezien als onnodig; er zijn immers genoeg IPv6 adressen; en ongewenst omdat het de end-to-end connectiviteit breekt. Dit laatste geldt niet in alle gevallen voor NAT66 omdat het enkel prefixtranslatie uitvoert. Er bestaat dus een één-op-één verhouding tussen interne en externe adressen. Echter, protocollen met embedded IP adressen in de payload zullen ook deze NAT translatie niet overleven zonder hulp van een ALG.
NAT66 is ontwikkeld om omnummering te voorkomen bij een providerwissel. Het heeft echter nog weinig bijval gevonden vanuit de industrie en ook andere technieken om het probleem van omnummering te voorkomen kunnen nog niet op grote steun rekenen of zijn nog in ontwikkeling.
De enige praktische oplossing op dit moment is PI address space. Zeker bij middel- en grote netwerken kunnen de kosten van een omnummering anders erg hoog zijn.
Deze netwerken zullen bij het uitrollen van dual stack zich dit goed moeten realiseren. Zolang er geen werkbare alternatieven zijn is PI een must voor elk netwerk van enige formaat.

Ondersteuning

Zoals gezegd: dual stack is de meest ondersteunde transitietechniek. Alle veel gebruikte besturingssystemen ondersteunen dual stack: Microsoft vanaf Windows XP SP2 (of SP1 + advanced networking pack) en Windows server 2003, Apple vanaf Mac OSX(10.2) en Linux vanaf kernel2.4.(2.6 of hoger is aangeraden)
Ook de meeste professionele netwerkapparatuur heeft al lange tijd ondersteuning voor dual stack IPv4/IPv6. Cisco biedt hier standaard ondersteuning voor op al zijn producten vanaf 2001 (let op: dit betekend echter nog geen feature-parity met IPv4.)
De bestaande netwerkinfrastructuur, servers en workstations zullen dus waarschijnlijk allemaal met dual stack om kunnen gaan met de juiste configuratie, al dan niet na een software/firmware update.
De binnen Simac veel gebruikte IOS12.4 heeft ondersteuning voor een groot aantal features in IPv6, maar niet voor alle.
Een overzicht van welke features precies in welke IOS versie worden ondersteund is te vinden op de Cisco Website [21].

Ook de software ondersteuning van dual stack is goed te noemen. Bestaande software die met zowel IPv4 als IPv6 om kan gaan zal IPv6 gaan gebruiken zodra een service daarop beschikbaar is en bestaande legacy IPv4-only software zal zonder verandering kunnen blijven functioneren.

Ook toekomstige software die mogelijk IPv6-only is zal geen moeite hebben om te functioneren in een dual stack omgeving.

Performance/Schaalbaarheid
Naast de brede ondersteuning heeft dual stack ook het voordeel dat het verwerken van IPv6 packets niet zorgt voor merkbare extra workload voor netwerkapparatuur en dat dual stack geen extra verkeer genereert.
Op deze vuistregel zijn drie uitzonderingen: Routing tables, Access lists en DNS. Routing tables omdat er nu óók voor IPv6 een routing table moet zijn naast die voor IPv4, die ook geheugen innemen. Het zelfde voor access lists. En DNS, zeker in het begin, omdat onder andere Windows IPv6 prefereert bij het aanvragen van een DNS record. Er word dus altijd eerst om een AAAA record gevraagd. En als die er niet is voor een domain moet er een tweede request gedaan worden, ditmaal voor een A record. Voor het overgrote deel van de domains zal dit op dit moment dus twee DNS aanvragen betekenen. Naarmate steeds meer content IPv6-enabled zal zijn zal deze extra DNS load weer verdwijnen.

Beheerbaarheid
Een van de grote nadelen van dual stack is de flink toegenomen configuratiedruk. Alle netwerk apparatuur zal geconfigureerd moeten worden voor zowel IPv6 als IPv4, wat veelal neer zal komen op dubbel uitvoeren. Routing, access lists, DNS en eventueel DHCP configuraties worden groter. Dat kost extra tijd om te configureren en daarmee extra geld.
De grotere hoeveelheid configuratie kan troubleshooting en beveiliging mogelijk moeilijker maakt. Echter is het configureren voor dual stack niet wezenlijk moeilijker of ingewikkelder dan het configureren van IPv4. De configuraties van IPv4 en IPv6 zullen veel overeenkomsten vertonen, als ze al niet ’n één-op-één kopie zijn, in het gunstigste geval.

Onder andere door deze complexiteit en het feit dat elke netwerkapparaat moet worden aangepast, is het niet verstandig, zo niet onmogelijk om een uitrol van dual stack in een keer te doen op een bestaand netwerk van enig formaat. Bij nieuwe netwerken kan dual stack vanaf het begin gelijk worden geïmplementeerd als hier de extra tijd voor wordt genomen. Bij bestaande netwerken kan dit echter bijna niet worden gedaan zonder dat de service er onder lijdt.
Een gefaseerde uitrol is daarom het meest gewenst.
De visie van Simac is om met een dual stack implementatie te beginnen aan de randen van het netwerk en dan naar binnen te werken en met het core-netwerk te eindigen. Zo kan de ervaring met IPv6 deployments groeien naarmate de impact van de changes stijgt.
Om de verschillende netwerksegmenten met elkaar te laten communiceren tot het core-netwerk dual stack is gemaakt, moet er gewerkt worden met tunnels. De verschillende tunnel technieken zijn beschreven in het vorige hoofdstuk.

Structureel oplossing
Als een bedrijf eenmaal dual stack heeft geïmplementeerd in het gehele netwerk is het echter volledige klaar voor de toekomst wat betreft IPv6. Als IPv4 in de toekomst niet meer relevant is kan het zonder verdere gevolgen uitgezet worden. Geen andere handelingen zijn daarvoor noodzakelijk. Alle andere transitietechnieken leunen in meer of mindere mate op het bestaan van een IPv4 netwerk/internet en die kunnen daarom dus niet zo maar worden uitgeschakeld.
De toekomstige stap naar IPv6-only is bij bestaande netwerken dus nagenoeg onmogelijk zonder een dual stack tussenstap als men onderbrekingen in de service tot een minimum wil beperken.

3.2 **Stateful NAT64**

Stateful NAT64 is in de eerste plaats ontwikkeld om "greenfield"(IPv6-only)sites toegang te geven tot het IPv4 internet of een IPv4 netwerk. Het maakt het mogelijk om met meerdere IPv6-only hosts één of een klein aantal public IPv4 adressen te delen. Dat gebeurt met behulp van DNS64. DNS64 zal voor elke domain request waarvoor geen AAAA record beschikbaar is een IPv6 adres fabriceren aan de hand van het IPv4 adres via een vooraf geconfigureerde methode (meestal een vast gekozen prefix). De NAT64 router herkent deze adressen en zal translatie toepassen op alle IPv6 adressen die aan de omzettingsmethode voldoen en ze naar het IPv4 internet/netwerk forwarden.
Deze toepassing voor IPv6-only sites valt echter buiten de scope van dit onderzoek.
Maar de mogelijkheden van stateful NAT64 om meerdere hosts met een IPv6 adres toegang te geven tot elk mogelijk IPv4 adres bied ook mogelijkheden om het IPv6 internet toegang te geven tot een IPv4-only bedrijfsnetwerk en dan in het bijzonder de publieke servers van het netwerk. Een NAT64 router wordt zo geconfigureerd dat hij verkeer, bestemd voor de webserver (meestal gefilterd op IPv6 adres.) forward naar het IPv4 adres van de webserver.

kosten
Het grootste voordeel van het gebruik van NAT64 is dat er nagenoeg niets in het bestaande netwerk aangepast hoeft te worden.
Voor het hosten van services is het aanpassen van de DNS records voor het domain (om AAAA records toe te voegen) en het instellen van de router waar de IPv6 internetverbinding is aangesloten, vaak al voldoende.
De enige eisen zijn, dat de gebruikte router NAT64 moet ondersteunen en dat er een bruikbare IPv6 verbinding is (native of anderzijds). Een IPv6 verbinding realiseren wordt later in dit document behandeld.

Ondersteuning
Cisco geeft op het moment van schrijven stateful NAT64 ondersteuning alleen op de ASR1000 routers vanaf Cisco IOS XE 3.4S en Cisco IOS XR 4.1.2 [22].

Een van de nadelen van NAT64 is dat Protocollen die IP adressen embedden in de data niet werken. Deze embedded adressen worden namelijk niet mee vertaald bij de translatie. FTP is het bekendste protocol met dit probleem, maar ook veel gebruikte protocollen als SIP hebben moeite met NAT.
Een Application layer gateway (ALG) bij de NAT64 zou hiervoor een oplossing kunnen bieden. Cisco biedt op moment van schrijven echter enkel ondersteuning voor FTP64 en enkel in IOS XE 3.4S en later [23].

Performance
Het doen van de translatie en het bijhouden van de states-table kost extra CPU en geheugen capaciteit op de router voor elke IPv6 verbinding. De hoeveelheid IPv6 verkeer zal nu nog niet zo groot zijn, waardoor dit nú nog geen groot probleem zal zijn. In de toekomst kan het IPv6 verkeer echter nog wel eens hard groeien omdat, onder andere Windows, een IPv6 verbinding verkiest boven een IPv4 als beiden beschikbaar zijn.

security

Servers gehost achter een stateful NAT (inclusief stateful NAT64) zijn ook vatbaarder voor (D)Dos aanvallen. Achter de NAT heeft elke packet hetzelfde source-adres, het zelfde destination address, en het zelfde destination portnummer. Enkel het source portnummer kan gebruikt worden om verbindingen van elkaar te onderscheiden. Er zijn echter maar een beperkt aantal portnummers beschikbaar, 64.000 ongeveer. Dat is de maximale hoeveelheid IPv6 verbindingen die de router tegelijk kan leveren per intern IPv4 adres. Hoe groter de interne IPv4 adrespool van de router hoe groter het aantal verbindingen dat ondersteunde wordt [12].
Logging van het IPv6 verkeer op de server is met NAT64 is ook lastiger. Een server zal nooit het IPv6 adres van de cliënt te zien krijgen. Om toch te kunnen herleiden waar een request vandaan kwam, zal de server het poortnummer en het precieze tijdstip moeten bewaren, en dat vergeleken met het log van states-table van de NAT64 router. De grote van dergelijke logfiles kan snel toenemen naarmate het IPv6 verkeer groeit.

Structureel Oplossing

Een ander veel gemaakt argument tegen het gebruik van NAT64 voor dit doel is niet zo zeer een argument tegen de techniek zelf, maar gaat over het effect van dergelijke technieken op het uitrollen van IPv6 wereldwijd, maar ook binnen een bedrijf.
Voor een IPv4 content provider is iets als NAT64 gemakkelijk om snel IPv6 connectiviteit te bieden, maar het limiteert heel sterk hun aanraking met IPv6 en biedt geen mogelijkheid om IPv4 uit te schakelen in de toekomst als deze niet meer gebruikt wordt. Een volledige overschakeling van IPv4-only naar IPv6-only is uitermate onwaarschijnlijk en onwenselijk. Er zal bij het gebruik van NAt64 alsnog een periode komen waarbij dual stack zal worden gebruikt. Ieder bedrijf met een IPv4 netwerk dat voor NAT64 kiest moet zich er dus bewust van zijn dat het enkel een tijdelijke oplossing is, een extra tussenstap op weg naar IPV6-only.

3.3 **Proxy/ALG**

Proxyservers zijn servers waar cliënts mee connecten waarna de proxy vervolgens de door de cliënt gevraagde informatie gaat ophalen. Waar alle andere technieken gebruik maken van één connectie, eventueel vertaald/aangepast, gebruikt een proxy er twee. Een proxy accepteert de connectie van de klant volledig, bekijkt de inhoud van het ontvangen packet en maakt vervolgens een nieuwe connectie aan naar de gevraagde server.

Voor dit rapport zijn er twee proxy vormen van belang. De standaard proxyserver (ook wel forward proxy geheten), die werknemers kunnen gebruiken om te browsen op het internet, is de meest voorkomende. Deze stelt bedrijven in staat om hun werknemers beter te beschermen en om strengere access lists te gebruiken zonder dat het de werknemer belemmerd bij het browsen op internet. Deze vorm van proxy is van belang voor het bieden van werknemer IPv6 connectiviteit.

De andere vorm die van belang is voor dit rapport is de reverse proxy. Deze doet eigenlijk precies hetzelfde, maar dan is deze verplaatst naar het netwerk van de webserver. Waar een forward proxy gebruikt word om een beperkt aantal gebruikers toegang te geven tot alle servers is de reverse proxy geconfigureerd om het hele internet toegang te geven tot één of een beperkt aantal servers.

Een proxy en een ALG zijn heel vergelijkbaar en doen nagenoeg het zelfde. Het verschil is dat een cliënt geconfigureerd moet worden om gebruik te maken van een proxy en dat deze zijn data rechtstreeks naar de proxy stuurt, waar een ALG de data onderschept zonder dat de cliënt hier iets van merkt.
Bij een reverse proxy ligt dit iets anders omdat de cliënt zelf niet geconfigureerd hoeft te worden om het te gebruiken. Het "configureren" van de cliënt bestaat hier uit het, in de DNS entry van het domain, verwijzen naar het IP adres(v4 of v6) van de proxyserver in plaats van het adres van de webserver.
Een ander verschil is dat de noodzaak om packets te onderscheppen betekent dat ALG's altijd te vinden moeten zijn in netwerkapparatuur als routers en firewalls, waar proxyservers meestal op een host/server staan (maar op netwerkapparatuur is ook mogelijk)
Een ALG wordt meestal gebruikt om een NAT router te ondersteuning bij protocollen die embedded IP adressen hebben. Bij IPv6 naar IPv4 translatie kan een AGL de NAT64 router ondersteunen voor protocollen waarbij dit nodig is bijvoorbeeld.

<u>Performance</u>
Van de drie gekozen technieken heeft de proxy de hoogste overhead per packet. Elk packet moet tot aan met laag 7 worden behandeld, waarna er vervolgens een nieuwe verbinding wordt opgezet om de aanvraag of de content door te sturen.

<u>Security</u>
Het voordeel van het gebruik van proxies is dat werknemers binnen het netwerk er door beschermd kunnen worden en dat webservers nooit rechtstreeks communiceren met cliënts op internet. Desgewenst kan ook veel gevraagde informatie lokaal gecached worden, waardoor deze sneller beschikbaar is bij de volgende aanvraag.

Struturele oplossing

Net als bij NAT64 biedt ook een proxy geen mogelijkheid om zonder extra stappen de overgang te maken naar een IPv6-only netwerk. De IPv6 connectiviteit van de web service en/of werknemers is gerealiseerd, maar de deployment van IPv6 blijft zeer beperkt en de benodigde kennis en ervaring met IPv6 wordt maar zeer beperkt opgedaan.
Wie de keuze voor een translating proxy maakt, moet zich er dus van bewust zijn dat het, net als bij NAT64, een tijdelijke maatregel is.

4 Webservers op IPv6

4.1 Dual stack

In dit hoofdstuk word specifiek gekeken naar de implementatie van dual stack bij webservers. Met dual stack webservers word bedoeld dat de server waar de webserver op draait dual stack is uitgevoerd, bereikbaar is vanaf zowel het IPv4 als het IPv6 internet en dat de gebruikte webserversoftware zo is geconfigureerd dat deze met zowel IPv4 als IPv6 connecties overweg kan.

Uitrol

De locatie van webservers aan de randen (edge) van het netwerk maakt deze een uitstekende kandidaat voor een eerste dual stack deployment in de praktijk, passend in Simac's visie voor IPv6 en de gekozen van-buiten-naar-binnen strategie.
Een dual stack deployment hier geeft bedrijven de kans om bekend te raken met IPv6 in een (voor de meeste bedrijven) low-impact omgeving waar eventuele kleine storingen niet meteen leiden tot extra kosten of omzetverlies.
Dit geeft beheerders de mogelijkheid om ervaring op te doen met het configureren van netwerk apparatuur voor IPv6 en dual stack en kan tegelijkertijd op de lange termijn stabiliteit van de IPv6 implementaties aantonen, voordat deze wordt uitgerold in meer een bedrijfskritische omgevingen.

In bedrijven waar webservers wel een kritisch onderdeel van de bedrijfsprocessen zijn kan het verstandiger zijn om eerst een ander, minder kritisch, netwerksegment te selecteren om met dual stack te beginnen. Zo kan de ervaring en kennis van IPv6 worden uitgebreid voordat deze bedrijfskritische onderdelen worden omgezet naar dual stack.

Ondersteuning

IPv6 ondersteuning is iets waar veel webserver softwareontwikkelaars al lange tijd serieus mee bezig zijn. De twee meest gebruikte webserversoftware, Apache en Microsoft IIS ondersteunen IPv6 al enige tijd. Apache al sinds versie 2.0 (april 2002) en IIS vanaf 6.0 (april 2003) gedeeltelijk en geheel vanaf 7.0 (februari 2008)
Simac gebruikt nagenoeg exclusief IIS voor web services bij haar klanten. De diversiteit van de klanten van Simac betekend dat IIS 6.0 nog voorkomt.
De restricties van IIS6.0 bij het gebruik van IPv6 zijn daarom relevant om te bekijken [24].

Een aantal van de missende features zijn enkel onhandig, maar een aantal andere kunnen voor problemen zorgen:

- Er kan maar één SSL site zijn per server
- Reverse DNS lookups werken niet voor IPv6
- Alle sites op de IIS server zullen allemaal reageren op IPv6 requests, het is niet mogelijk om IPv6 te enabelen voor individuele sites op dezelfde server
- De afwezigheid van IP restricties kan ook een probleem zijn, maar is iets dat binnen Simac meestal door het netwerk wordt afgehandeld.

Het belangrijkste gemis is misschien wel het feit dat enkel het WWW gedeelte van IIS IPv6 ondersteund. FTP, SMTP en NNTP zijn niet IPv6 enabled. Binnen Simac wordt de FTP server van IIS soms gebruikt, al is dat meestal kleinschalig gebruik. De grotere FTP servers zijn over het algemeen Linux based.
De SMTP functionaliteit van IIS6.0 wordt gebruikt door exchange 2003, die ook nog bij enkele klanten te vinden is.

IIS6.0 word standaard bij Windows server 2003 meegeleverd. Server 2003 komt nog regelmatig voor in het klantenbestand van Simac, maar er vind een verschuiving plaats naar server 2008. Windows server 2008 word standaard geleverd met IIS 7.0 en deze biedt gelijke functionaliteit in IPv4 en IPv6. Met de juiste configuratie is dual stack voor servers met IIS7.0 dus geen enkel probleem.

Hier een overzicht van alle voor webservers relevante voor- en nadelen van dual stack op een rij:

Voordelen

- In lijn met het globale IPv6 migratieplan (zoals beschreven in RFC5211 [25]).
- Geen extra hardware vereist in praktisch alle gevallen.
- Bijna alle bestaande netwerkapparatuur ondersteunt al dual stack of doet dat na een software update.
- IPv6 is goed ondersteund door veel webserversoftware.
- Weinig tot geen extra workload op netwerkapparatuur in vergelijking met het huidige IPv4 netwerk (DNS, access-lists en routing tables mogelijke uitzondering).
- Webservers in de edge van het netwerk mogelijk goede kandidaat voor eerste uitrol IPv6.
- Uitfaseren IPv4 eenvoudig als de tijd daar is.
- Niet tijdelijk van aard.

Nadelen

- Vergroot configuratiedruk op netwerkapparatuur (extra kosten); bijna alles moet dubbel worden geconfigureerd, éénmaal voor IPv4 en éénmaal voor IPv6.
- Vergroot “surface area” waarop aanvallen uitgevoerd zouden kunnen worden.
- Potentieel grote impact op veel ICT hardware en software door configuratieverandering. Uitgebreid testen noodzakelijk (kosten).
- IIS 6.0 IPv6-ondersteuning onvolledig.
- Herconfiguratie van webserver noodzakelijk om IPv6 te ondersteunen.
- Zonder eigen provider independent (PI) IPv6 prefix is omnummering noodzakelijk bij het wisselen van provider.

4.2 **Stateful Nat64**

Het hosten van web services met NAT64 is niet veel anders dan het hosten van andere services achter NAT64. Verbind de router met het IPv6 internet (rechtstreeks of met static tunnel bijvoorbeeld), zorg voor een via IPv6 bereikbare DNS server, voeg de juiste AAAA records toe aan het domain en stel de router in.
Zolang de website zelf geen verwijzingen naar IPv4 adressen heeft (iets dat sterk wordt afgeraden), is de website nu online op IPv6. De gebruikte webserversoftware is niet van belang en hier hoeft ook niets aan geconfigureerd te worden.
De Security en performance issues zijn exact het zelfde zoals beschreven in hoofdstuk 3.2

Uitrol

Om deze redenen is NAT64 een relatief eenvoudige drop-in oplossing om snel en eenvoudig een website op het IPv6 internet te krijgen.
Een eventuele omnummering met NAT64 blijft beperkt tot de static routing en de DNS entries voor de website. Als een bedrijf nog geen PI address space heeft, maar er wel een noodzaak is om snel de website op IPv6 beschikbaar te hebben, kan NAT64 een goede maar tijdelijke oplossing zijn. Voor http verkeer is geen ALG nodig. Maar als de gebruikte server nog meer services bied (zoals een FTP server bijvoorbeeld) dan kan deze wel nodig zijn om ook deze services op IPv6 aan te bieden.

Structurele oplossing

Ook voor web services geldt dat NAT64 geen structurele oplossing is. Het is een tijdelijke maatregelen op weg naar dual stack en IPv6 die zowel kan helpen als kan hinderen. Netwerk-technisch is de uitrol van NAT64 voor webservers geen belemmering voor de uitrol van dual stack, maar bedrijfspolitiek gezien kan het de noodzaak voor dual stack wel verkleinen, wat de uitrol van dual stack kan vertragen terwijl het opdoen van ervaring met IPv6 en dual stack, ook met NAT64, noodzakelijk is voor de toekomst.

Hier de voor web services relevante voor en nadelen van stateful NAT64 op een rij:

Voordelen

- IPv6 deployment blijft beperkt tot de randen van het netwerk.
- Kan bestaande hardware gebruiken (Enkel de router heeft mogelijk een hard- of software update nodig).
- Bestaande IPv4 infrastructuur kan verder bijna geheel met rust gelaten worden (met de mogelijke uitzondering van on-site DNS afhankelijk van SOA en NS records voor domain).
- Relatief lage investering in tijd en materiaal.
- Drop-in oplossing, snel en relatief eenvoudig op te zetten.

Nadelen

- Vergroot workload voor router die translatie doen.
- Dual stack nog steeds noodzakelijk voor de toekomst,
- Wordt niet gezien als langer termijn oplossing(onder andere door Cisco) misschien van toepassing op toekomstige ondersteuning.
- Zonder ALG enkel geschikt voor applicaties die geen IP/port informatie in hun protocols mee sturen.
- Logging ingewikkelder
- Vatbaar voor (D)DOS, elke adres in de interne pool kan ongeveer 64,000 connecties aan, daarna zijn de portnummers op.
- Vervolg investering dual stack blijft noodzakelijk

4.3 **(Reverse) Proxy**

Voor het aanbieden van web services op IPv6 met een IPv4 webserver kan een reverse proxy worden gebruikt.
Een van buitenaf op IPv6 bereikbare proxyserver vertaalt al het binnenkomende http verkeer naar IPv4 en stuur dit door naar een of meer servers.

NAT64 en een reverse proxy voor adres-translatie doen bijna het zelfde op iets andere plekken in het netwerk. Ze delen daarom een groot aantal van de voordelen en nadelen met elkaar.
Net als NAT64 is een reverse proxy daarom een relatief low-impact manier om de huidige IPv4-only servers beschikbaar te maken via IPv6.

Performance

Het grootste verschil zijn de benodigde hardware requirements en de load per connectie.
Voor een reverse proxy is in veel gevallen een hostserver nodig waar de proxy op draait. De load op zo'n server zal per verbinding hoger zijn dan bij NAT64. NAT64 hoeft enkel de IP en TCP/UDP headers aan te passen en door te sturen. Een proxy zal echter een packet helemaal tot en met de applicatielaag moet verwerken, waarna er vervolgens(als de gevraagde content niet lokaal gecached is) een nieuwe verbinding opgezet moet worden naar de benodigde server om de gevraagde data op te halen.

Ondersteuning

Een ander verschil met NAT64 zijn de protocollen die door een reverse proxy worden ondersteund. Als de proxysoftware de applicatie ondersteund dan kan ook software die normaal niet door een NAT heen werkt, wel werken met een reverse proxy. Active FTP is hier een voorbeeld van. Maar er moet wel specifieke ondersteuning per programma/protocol zijn bij de proxy server.
Ook logging is minder een probleem dan bij NAT64 omdat de proxyserver zowel het IP van cliënt te zien krijgt en weet welke informatie de cliënt aanvroeg.

Uitrol

Om een reverse proxy te gebruiken moet er een (virtuele) server komen, waar de proxyserver op gaat draaien, of moet er een dedicatie proxyserver hardware komen.
De proxyserver dient toegang te hebben tot het IPv4 netwerk en bereikbaar te zijn vanaf het IPv6 internet, en de gebruikte proxy software moet IPv6 naar IPv4 en visa versa translatie toestaat. De rest van het bestaande netwerk kan met rust geladen worden.
Ook het configureren en onderhouden zullen, enigszins afhankelijke van de hoeveelheid IPv6 verkeer, geen grote kostenposten zijn voor een bedrijf.
Afhankelijk van de SOA en NS records van het domain kan het zijn dat eventuele on-site DNS servers aangepast moeten worden en dual stack gemaakt.

Hier de voor web services relevante voor- en nadelen van reverse proxies op een rij:

Voordelen

- Drop-in oplossing
- IPv6 deployment blijft beperkt tot de randen van het netwerk
- Bestaande IPv4 infrastructuur kan verder bijna geheel met rust gelaten worden (met de mogelijke uitzondering van de on-site DNS afhankelijk van SOA en NS records voor domain)
- Relatief lage investering in tijd en materiaal
- Bruikbaar voor meer type protocollen dan NAT64, zolang er ondersteuning is vanuit de proxyserver software.

Nadelen

- Extra server vereist waar de proxy op draait (of huidige dual stack maken).
- Workload voor proxy hoger dan bij NAT64
- Geen rechtstreekse mogelijkheid om IPv4 uit te kunnen faseren.
- Word niet gezien als lange termijnoplossing (onder andere door Cisco), misschien van toepassing op toekomstige ondersteuning.
- Performance problemen mogelijk naar maten IPv6 verkeer groeit.
- Vervolg investering dual stack nog steeds noodzakelijk

4.4 **Aanbevelingen.**

Algemeen

Er is maar één lange termijnoplossing voor web services en dat is dual stack. Het is de techniek met de laagste overhead per connectie, de breedste en meeste complete ondersteuning en biedt de beste ondersteuning voor een internetwereld die steeds meer IPv6 zal gaan gebruiken. Het is ook de enige waarbij IPv4 op den duur uitgefaseerd zou kunnen gaan worden (hoe ver weg dat nu ook nog is).
Het is echter ook de techniek die het meeste tijd kost om te implementeren, de techniek die de meeste aanpassingen vereist aan de configuratie van het netwerk. Een netwerk brede, gefaseerde uitrol van dual stack kan lange tijd in beslag nemen, zeker als de interrupties tot een minimum beperkt moeten blijven. Zelfs voor er begonnen kan worden met een dual stack implementatie moeten veel dingen al geregeld en gecontroleerd zijn: native IPv6 connectie of alternatieve, PI address space, DNS, inventarisatie van benodigde features voor IPv6 en de ondersteuning in de huidige hardware vanaf welke software versie ect.
Het is dus aan te raden hier vroeg mee te beginnen, ruim voor de onvermijdelijke noodzaak zich aan dient.
Simac's visie hierop maakt dat webservers, door hun positie aan de rand van het netwerk, een goede kandidaat zijn om te starten met een dergelijke uitrol, en van daaruit de dual stack implementatie uit te breiden naar de rest van het netwerk, eventueel ondersteund met static tunnels.

Maar dat is het ideaalbeeld. Wat nu, als er ineens haast is bij een IPv6 implementatie van de web servers? Dan komen de andere technieken tot hun recht. Zowel NAT64 als een reverse proxy zijn zonder veel aanpassingen te implementeren en bieden beide genoeg functionaliteit om te gebruiken als tijdelijke oplossing.
Kijk dan om te beginnen naar de bestaande hardware en wat deze ondersteunen. Staat er een router met NAT64 ondersteuning? Een reverse proxy met IPv6 support of zijn er load balancers in gebruik die een IPv6/IPv4 vertaling kunnen doet? Als de benodigde hardware voor een bepaalde techniek aanwezig is en zolang de benodigde features ondersteund zijn, is er voor een dergelijke tijdelijke (en het is belangrijk om te realiseren dat dit tijdelijk is) weinig tot geen reden om voor een andere techniek te kiezen.

Is er nog geen bestaande mogelijk om IP translatie te doen op het bestaande netwerk, dan zijn de aanschaf en onderhoudskosten waarschijnlijk de belangrijkste reden om voor de een of de andere techniek te kiezen.
Voor nieuw aan te leggen netwerken zal ook dual stack het doel zijn. Maar of dit gelijk vanaf het begin af aan helemaal wordt doorgevoerd zal liggen aan de hoeveelheid IPv6 kennis die is opgedaan. Ligt er een concrete IPv6 vraag, voer die gelijk in dual stack uit. Voor de rest, volg het Simac plan, van buiten naar binnen, en voer dit net zo ver door als de kennis en ervaring op dat moment toelaat. Maar ook met de overige delen van het netwerk moet vanaf het begin af aan al rekening gehouden worden met IPv6. Het streven moet zijn om geen nieuwe hardware of software in te zetten waarvoor nog geen IPv6 support is (of die niet op zijn minst in de planning staat). Dit laatste geldt ook voor uitbreidingen en vervangingen aan bestaande netwerken.

Een aantal recente IPv6 Cisco presentaties eindigen met de woorden:
"Dual stack where you can, tunnel where you must, translate when you have a gun to your head."
En dat is ook de samenvatting van deze aanbeveling.

Kosten

Als de benodigde hardware IPv6 ondersteund in het edge netwerk, dan hoeven de kosten voor een dual-stack implementatie daar niet hoog uit te vallen. Maar een precisie inschatting maken is moeilijk vanwege de grote variatie aan mogelijke situaties. Als er voldoende ondersteuning is voor IPv6 in het bestaand netwerk, eventueel na een software update dan kan dual stack enkel voor de web servers in 10-20 manuur rond zijn. Echter moet er dan al een hoop voorbereidend werk zijn gedaan, zoals een IPv6 verbinding en PI space geregeld, een nummering plan zijn opgesteld en een inventarisatie gedaan van de benodigde en beschikbare security features van de bestaande netwerk hardware.
En schatting van 25% van de tijd die het kosten om het originele netwerk segment te plannen en configureren is een redelijke, misschien wat conservatieve, schatting.

Een kosten vergelijking maken tussen de 2 tijdelijke oplossingen is iets gemakkelijker, en minder variabel.
Het goedkoopste zou een translating proxy software packet zijn op een virtuele server. De web gateway software van Mcafee kan hiervoor gebruikt worden en heeft ondersteuning voor IPv6 van en naar IPv4 translaties met HTTP en HTTPS.
Deze software kost $57,12(€44,27) per jaar per node vanaf 11 nodes tot $21,78 (€16,88) per jaar per node vanaf 501 nodes.
De kosten voor het draaien van deze software in een VM omgeving zijn voornamelijk manuren. Een minimum installatie hiervan, zonder papier werk, kost naar schatting 8 manuur, een recent praktijk voorbeeld kosten 21,15 uur. Omgerekend in euro's (83 euro per uur) komt dat uit op respectievelijk 664 euro en 1.755,45)
Voor klanten zonder VM omgeving is het ook mogelijk om deze software op een blade te draaien.

Blue Coat ProxySG Virtual Appliance kan een alternatief zijn voor het McAfee software packet en biedt een alternatief licentie model, met eenmalige kosten van $2.700,- vanaf 10 gebruikers tot $14.000,- voor 300 gebruikers. Gezien de tijdelijkheid van de proxy oplossing voor de vraagstelling beidt dit echter geen kosten voordelen.

Een andere optie is de Mcafee web gateway Appliance. Deze gebruikt dezelfde software als de hierboven beschreven oplossingen maar nu met dedicated hardware van Mcafee, en is te krijgen in 4 verschillende uitvoeringen.
Vanaf $1.695,75 (€1.314,33) tot aan met $17.846,- (€13 832) aanschaf + 1 jaar onderhoudt contract. daarna tussen de $399(€312) en $4,199(€3.283) per jaar aan onderhoud en updates.

Een alternatief voor de McAfee web gateway is de Blue coat Proxy SG, maar deze begint zo'n $4.500,- hoger voor de zelfde hoeveelheid gebruikers en biedt, puur naar deze toepassing gekeken, geen extra voordelen.

De Laatste optie is de Cisco ASR-1000. Deze router heeft ondersteuning voor stateful NAT64 maar is op dit moment de enige router van Cisco die dit ondersteunt. De ASR-1000 een van de duurdere modellen. Hij kost €26.065,- voor aanschaf + 1 jaar onderhoudscontract. Vervolgens €2.795,- per jaar onderhoud.
Tot de ondersteuning van Stateful NAT64 ook voor de lagere ASR modellen beschikbaar komt zal NAT64 dus geen aantrekkelijke optie zijn om aan te schaffen als er geen bestaande mogelijkheid tot translatie is.

	Aanschaf/installatie	Onderhoud/licentie kosten per jaar	Protocol ondersteuning IPv6<-->IPv4	
McAfee Web Gateway(VM)	8 manuur minimaal (€664,-)	€20,04 tot 52.55 per node + kosten VM omgeving	HTTP/HTTPS	
McAfee Web Gateway appliance	€1.560,- tot €16.416,- aanschaf + 10 manuur minimaal (€830,-)	€312 tot €3.283	HTTP/HTTPS	
Cisco ASR-1000	€26.065,- 6 manuur minimaal (€498,-)	€2.795,-	HTTP/HTTPS FTP	

(dollar euro omrekening gedaan met koers op 17-1-2012)

DNS

DNS is een belangrijk punt in elke IPv6 transitie. En zeker bij web services is het belangrijk om te controleren of de huidige DNS structuur IPv6 ondersteund.
Elk domein heeft op dit moment een A record met het IPv4 adres van de webserver erin. IPv6 gebruikt in plaats van A records AAAA records (uitgesproken quad-a).
Voor het hosten van web services op IPv6 zullen de bestaande IPv4 DNS entries aangevuld moeten worden met deze AAAA records.
Dual stack hosts kunnen zonder problemen AAAA records aanvragen bij IPv4-only DNS server, zolang de server AAAA records ondersteund. Maar voor IPv6-only hosts om verbinding te maken met de web services is het noodzakelijk dat (een deel van) de DNS servers voor het domein bereikbaar zijn via IPv6.
Worden de DNS server van een derde partij (hosting provider/register ect) gebruikt voor het domain, controleer dan of deze IPv6 ondersteunen op hun DNS. Worden er on-site DNS servers gebruikt voor het externe domain, dan zullen die dual stack gemaakt moeten worden of er moeten extra IPv6 enabled servers worden bijgezet.

PI address space

Regel dit voor de uitrol van dual stack.
Voor kleinere bedrijfjes is het misschien nog te doen is om een omnummering uit te voeren bij een providerwissel, voor middel- en grote bedrijven is het niet te accepteren. Voor de uitrol van dual stack van start gaat, is het belangrijk om PI address space te krijgen, zeker zolang er nog geen andere oplossingen zijn in de markt voor multihoming en prefix translatie/aanpassing.

Wordt er nog gebruik gemaakt van NAT64, reverse proxy of een load balancer dan is PI strikt genomen nog niet noodzakelijk en kunnen PA adres gebruikt worden. Als de PI address space is aangevraagd kan de dual stack implementatie van start gaan met de nieuwe adressen terwijl de translating- of proxyoplossingen gewoon door blijven werken met de PA adressen.
Als de uitrol van dual stack is voltooid voor het edge netwerk dan hoeft enkel de DNS record aangepast te worden zodat deze verwijst naar het nieuwe PI IPv6 adres van de webserver. Als de DNS aanpassing kans heeft gehad om zich te verspreiden kan de oude oplossing offline gehaald worden.

Webserver software
De meeste web-server software heeft al geruime tijd IPv6 ondersteuning, al dan niet gedeeltelijk. Voor Simac is vooral IIS van belang. IIS 7 heeft voor IPv6 volledige feature parity met IPv4 en IPv6 kan hier zonder problemen op enabled worden.
IIS6 IPv6 ondersteuning is er wel, maar wel beperkt [24]. Inventariseer of IIS6 alles ondersteunt, dat nodig is voor het huidige gebruik of dat wat er is voldoende is om aan de vraag naar IPv6 te voldoen. Met een upgrade naar Windows server 2008 of later (en daarmee IIS7 of later) kunnen de andere features alsnog ook op IPv6 enabled worden.
Maar let hierbij wel op, het gemis van bijvoorbeeld IPv6 FTP functionaliteit in IIS6 kan problemen geven voor dual stack hosts die willen verbinden naar de FTP server via de domein naam. De dual stack host zal eerst een AAAA record aanvragen, er een terug krijgen en dan proberen te verbinden met het IPv6 adres van de server, die op IPv6 niet kan antwoorden voor FTP. Een oplossing hiervoor zou kunnen zijn een subdomein (ftp.voorbeeld.nl) met enkel de A record.

Security
Beveiliging is een belangrijk aspect bij alles dat met networking te maken heeft, en de IPv6 transitie is daarin geen uitzondering. Een dual stack implementatie kan gezien worden als het hebben van 2 aparte netwerken, en beiden moeten even goed beschermde worden. Alle beveiligingsmaatregelen en best practice die gelden voor IPv4 zijn nog steeds van kracht bij IPv6.

Er komen echter ook een aantal issues bij:
Net als rogue DHCP servers bij IPv4 (en IPv6) kunnen er ook rogue routers zijn die reageren op een "router solicitation multicast request" van een host die gebruik maakt van SLAAC. Deze rogue router kan vervolgens al het verkeer van deze hosts bekijken en manipuleren voor het door te sturen naar de eigenlijke router van het netwerk of naar buiten te tunnelen. De publiekelijke Servers, inclusief de web-servers hebben nagenoeg altijd vaste IP adressen waardoor dit minder een issue is voor web-services. Een uitgebreidere beschrijving van dit probleem is te vinden in hoofdstuk 5.3, de aanbevelingen voor werknemers IPv6 connectiviteit.

Een ander gevaar dat nieuw is met IPv6 is de route header type 0 (RH0)
Met deze extension header is het mogelijk om 1 or meer tussenstation op te geven voor een packet. Op deze manier kan de route van het packet worden beïnvloed.
Er zijn echter een aantal Security issues met deze RH0 en ze zijn gemakkelijk uit te buiten voor DoS aanvallen.
Door packets bijvoorbeeld routeren via een publiekelijke server op het netwerk zou het mogelijk kunnen zijn om de rest van het bedrijfsnetwerk te bereiken als verkeer van die server meer wordt vertrouwt als verkeer van buitenaf.
Ook een DoS aanval kan hiermee worden versterkt. Door een packet te maken dat meerdere keren tussen twee hosts heen en weer wordt gestuurd wordt er op die twee hosts veel meer netwerk verkeer gegenereerd als dat het kosten om dat ene packet te uploaden. [26]
Daarnaast zijn er ook een aantal oudere versies van IOS die kunnen crashen door een speciaal ontworpen RH0 packet (met name 12.2 t/m12.4 versies). [27] [28]

Sinds Cisco IOS 12.2(15)T is het mogelijk om route header type 0 uit te schakelen.
Met oudere versies is het enkel mogelijk om route headers in het geheel uit te zetten, inclusief type 1 en 2. Type 2 wordt gebruikt voor mobile IP, wat een techniek is die in de toekomst steeds vaker gebruikt lijkt te gaan worden.

RFC5095 raad aan om Route headers type 0 niet meer te gebruiken en niet meer te implementeren [29] maar oudere versies van software en firmware hebben hier nog steeds ondersteuning voor.

Het voornaamste probleem met IPv6 is niet de techniek zelf, maar de volwassenheid van de implementaties op dit moment.
Het komt nog regelmatig voor dat bepaalde securityfeatures nog niet geïmplementeerd zijn in IPv6, zelfs in de laatste versie van de software.
Het is dus zaak om goed te inventariseren wat er wordt gebruikt voor IPv4 en wat er daarvan mist aan ondersteuning in IPv6.
Ga na of deze missende features op een andere manier zijn op te lossen, of maar het kan niet zo zijn dat er op Ipv6 minder beveiliging word geboden dan op Ipv4. Ook al is nog maar een (klein) deel van het netwerk Ipv6 enabled, het is mogelijk om via een Ipv6 lek verder het Ipv4 netwerk op te komen door middel van een dual stack host bijvoorbeeld.

5 Werknemers IPv6 connectiviteit

5.1 **Dual stack**

Met dual stack voor werknemers wordt bedoeld dat de werkstations van de werknemers beschikken over zowel een IPv4 als een IPv6 adres, met internet connectiviteit op beide.

Vanuit de werknemer gezien biedt Dual stack de meeste voordelen.
Het biedt de grootste flexibiliteit in ondersteunde programma's/protocollen. Er zijn geen extra ALG's nodig, proxies zijn optioneel, en er hoeft geen extra werk gedaan te worden zoals translatie. De enige limitatie is dat IPv4-only programma's niet kunnen communiceren met IPv6-only servers en andersom zonder extra maatregelen.
Ook de ondersteuning onder besturingssystemen is goed en zou geen problemen mogen opleveren. Alle workstations met Vista of Windows 7 zullen, als dit niet eerder is uitgezet, meteen gebruik maken van IPv6 zodra dit beschikbaar is. Voor XP is er ondersteuning voor IPv6 vanaf servicepack 2, maar moet dit wel specifiek worden geïnstalleerd. Ook Mac OS X heeft vanaf versie 10.2 (Jaguar) net als Vista en Windows 7 standaard zijn IPv6 ondersteuning enabled. Eerdere versies hadden nog geen IPv6 ondersteuning. (Apple's Bonjour heeft IPv6 ondersteuning vanaf versie 10.3). Eventuele Linuxworkstations zullen, als ze een 2.6 of hoger kernel hebben naar alle waarschijnlijkheid ook IPv6 ondersteunen out of de box, maar dit varieert per Linuxdistributie. Er zijn versies van de kernel 2.4 en zelfs 2.2 met IPv6 ondersteuning, maar deze worden niet meer bijgewerkt naar de laatste versies van de RFC's en het word daarom aangeraden om minimaal kernel 2.6 of hoger te gebruiken.

Vanuit het Netwerk gezien is Dual stack wat performance betreft de techniek met de laagste impact, maar net als bij webservers is het wat configuratiechanges betreft de meeste intensieve. Een gefaseerde uitrol is hier extra belangrijk vanwege het grotere bereik van IPv6. Meer netwerken en netwerkapparatuur zal aangepast moeten worden om IPv6 connectiviteit aan alle werknemers te bieden. Dit betekent meer kans op configuratiefouten en daardoor storingen. Een gefaseerde aanpak verkleint de kans óp en de impact ván dergelijke fouten en storingen.
Er kan per netwerksegment een static tunnel worden gebruikt om de router van elk segment apart met de IPv6 internet verbinding te verbinden. Hierdoor kan eenvoudig elk netwerk segment één voor één worden overgezet op dual stack, wat de kans op storing en de impact hiervan verkleint.

De router kan vervolgens worden ingesteld om met of SLAAC of DHCPv6 IP adressen uit te gaan delen en andere noodzakelijke informatie zoals de IPv6 adressen van de default IPv6 gateway de adressen voor de DNS servers (die niet noodzakelijkerwijs IPv6 hoeven te zijn).

Als werknemers nu met IPv4 verplicht zijn om bijvoorbeeld een proxy server te gebruiken zal deze eerste dual stack gemaakt moeten worden en moeten worden geconfigureerd zodat deze IPv6 connecties kan accepteren en kan maken. Het is belangrijk om van te voren te controleren of de gebruikte proxyserver überhaupt IPv6 ondersteuning heeft en welke protocollen deze over IPv6 ondersteunt (dat aantal ligt meestal veel lager dan bij IPv4) hoewel HTTP en HTTPS meestal goed ondersteund zijn.

Nog even de voor werknemer connectiviteit relevante voor- en nadelen van dual stack op een rij:

Voordelen
- In lijn met globale IPv6 migratieplan (zoals beschreven in RFC5211 [25]).
- In lijn met de visie van Simac voor de toekomst.
- Geen tot weinig extra hardware nodig.
- Ondersteunt alle type connecties en software
- Veel bestaande netwerk apparatuur ondersteunt al dual stack of doet dat na een software update [26].
- weinig tot geen extra workload op netwerkapparatuur ivm huidige IPv4 netwerk (DNS, access lists en routing tables mogelijke uitzondering).
- Migratie naar IPv6-only eenvoudig.
- Gefaseerd uitrollen mogelijk (in combinatie met tunneling)
- Van permanente aard

Nadelen
- Gefaseerde uitrol enkel mogelijk na upgraden core-netwerk of door gebruik te maken van tijdelijke configuraties zoals interne tunnels.
- Vergroot configuratiedruk netwerkapparatuur (extra kosten); bijna alles moet dubbel worden geconfigureerd, éénmaal voor IPv4 en éénmaal voor IPv6.
- IPv4-only programma’s kunnen niet met IPv6 communiceren zonder extra tussenstap.
- Zonder provider independent (PI) IPv6 range kan omnummering noodzakelijk zijn bij het wisselen van provider.

5.2 **Proxy**

Voor nagenoeg alle netwerk (laag 4) technieken is het onmogelijk om een IPv4-only host connectie te laten maken met het IPv6 internet. Het is voor een IPv4-only host onmogelijk om duidelijk te maken naar welk IPv6 adres hij wil verbinden zonder gebruik te maken van hoger gelegen technieken, meestal DNS. NAT-PT is de enige, mislukte, poging tot nu toe om dit te doen (en ook die maakte gebruik van DNS).
In tegenstelling tot de nadere technieken werkt een proxyserver op laag 7. In plaats van dat een host een packet stuurt met een IP adres als destination, stuurt hij een domain naam of URL naar de proxyserver. De proxyserver gaat vervolgens kijken welk IP hier bij hoort, maakt dan een verbinding aan, haalt de informatie op en stuurt die door naar de host. Als de proxy server zowel IPv4 als IPv6 servers kan benaderen, maakt het voor de host niet uit welk IP versie word gebruikt door de servers (een gebruiker op een IPv4-only host zou zelfs een IPv6 adres in bijvoorbeeld zijn browser in kunnen vullen).
Hierdoor lijkt een Proxyserver de ideale manier om werknemers snel en in een low-impact manier van IPv6 connectiviteit te voorzien.
Er zijn echter een aantal nadelen aan deze techniek. Ten eerste moet, in tegenstelling tot bij een reverse proxy, het programma op de host ondersteuning bieden voor proxyservers. Hoewel veel programma's dit wel doen, geldt dit niet voor alle programma's. Ten 2de moet de proxyserver het programma of protocol ondersteunen. Voor bekende protocollen als HTTP, FTP, telnet en RDP zal dit geen problemen opleveren, maar bij minder bekend software of customsoftware zou dit een probleem kunnen zijn.

Van de proxyservers op dit moment in gebruik binnen Simac en haar klantenbestand (Microsoft ISA/TMG, eSafe en McAfee webgateway (voorheen webwasher) heeft alleen de McAfee ondersteuning voor IPv6. Microsoft geeft aan geen plannen voor IPv6 te hebben, waar op de eSafe website wordt het woord "IPv6" geen enkel keer wordt genoemd.
Helaas geeft McAfee geen overzicht welke protocollen op IPv6 worden ondersteund. Maar HTTP en HTTPS en FTP worden wel expliciet genoemd als zijnde ondersteund, evenals ondersteuning voor IPv4 hosts naar IPv6 server verbindingen.

Een andere optie is de McAfee Firewall enterprise. Deze next generation (laag 7) firewall gedraagt zich op veel punten als een proxy server en heeft een uitgebreide IPv6 ondersteuning (hoewel nog geen volledige featureparity met IPv4). Deze firewall wordt door Simac al bij enkele klanten geplaatst (vaak ter vervanging van de tweede lijn ASA servers) en biedt ook ondersteuning voor IPv4 naar IPv6 verbindingen maar op dit moment enkel voor http(s) verkeer en alleen als de host deze firewall als proxy server instelt. [27]

Voordelen

- IPv6 wijzigingen blijven beperkt tot de rand van het netwerk.
- Kan mogelijk gebruik maken van bestaande proxy servers/hardware, zonder (significante) extra load toe te voegen.
- Gefaseerd uitrollen mogelijk, maar enkel met 2de proxyserver.
- De McAfee next gen firewall ondersteund deze techniek.

Nadelen

- Enkel geschikt voor verbindingen/programma's die proxies ondersteunen, en die ondersteunde worden door de proxy.
- Een tijdelijke oplossing, geen rechtstreekse migratie naar IPv6-only mogelijk.
- Geen rechtstreekse uitfasering van IPv4 mogelijk.
- Word niet ondersteunde door alle proxysoftware.

5.3 **Aanbevelingen**

Algemeen

Zoals al eerder aangegeven, een IPv4 naar IPv6 connectie is een lastige opdracht voor translatie technieken, waardoor er ook geen werkbare implementatie van is op laag-4. Hierdoor zijn er eigenlijk maar 2 opties: een eigen IPv6 adres door middel van dual stack of een forward proxy.

Proxies zijn snel op te zetten en bieden genoeg IPv6 functionaliteit om bij IPv6-only webcontent (http en http's) te komen. Maar hoewel er daarnaast misschien nog een aantal protocollen ondersteunt worden door bepaalde proxysoftware, is de hoeveelheid protocollen waarvoor er IPv4 naar IPv6 connectie ondersteuning is, erg gelimiteerd op dit moment. Daarnaast moet ook de software zelf proxies ondersteunen.
Is er een acute vraag naar IPv6 connectiviteit voor http(s) dan zijn proxies een goede, maar tijdelijke, optie.

Voor de lange termijn bieden ze echter niet genoeg protocolondersteuning en flexibiliteit. Zodra IPv6 functionaliteit vereist wordt voor meer protocollen, voor minder bekende programma's, programma's zonder proxy ondersteuning of custom software, dan kan de proxy niet meer aan deze vraag voldoen. De enige optie dan is om dual stack toe te passen.

DNS

Voor werknemer connectiviteit is het niet noodzakelijk dat de DNS server bereikbaar is op IPv6 om AAAA-records te kunnen leveren, zolang de gebruikte DNS software maar AAAA records ondersteunt. Microsoft ondersteunt dit vanaf Windows server 2000, BIND vanaf 8.4.1
Iets om in het achterhoofd te houden is, dat Windows XP, zelfs met SP3, helemaal geen DNS records via IPv6 kan aanvragen, dit gebeurt altijd via IPv4, ook als het om AAAA records gaat.

Nog iets om rekening mee te houden is, dat IPv6, door het langere adres, ervoor zorgt dat sommige DNS responses groter zijn dan de 576byte(512bytes in het datagram), die van oudsher werden toegestaan over UDP voor DNS. Om dit (en andere problemen, met name DNSSEC) op te lossen is al tijden geleden de, in RFC2671 [28] beschreven, EDNS0 ontwikkeld. Deze standaard word ondersteund door de DNS server van Windows server 2003 en hoger, en ook in BIND vanaf versie 8.3.
Echter sommige, en dan met name oudere, securityoplossingen, blokkeren standaard UDP packets groter dan 576bytes op port 53, inclusief oudere versies van Cisco IOS.
Vanaf Cisco ASA software versie 8.2.2 is er een functie die automatische de benodigde lengte kan bepalen aan de hand van de DNS configuratie, maar deze moet wel nog handmatig enabled worden. In oudere versies van IOS moet de maximum lengte handmatig worden bepaald en ingesteld. [29]
Om IPv6 DNS volledig te kunnen ondersteunen moet de maximum packet grote omhoog naar 1280bytes (gelijk aan de nieuwe minimum MTU van IPv6). Voor DNSSEC moet deze 4000Bytes zijn.

PI address space

De impact van omnummering op het netwerk bij een dual stack implementatie voor werknemers is nog groter als die voor web services, omdat het om veel meer netwerksegmenten gaat.
Tot er werkbare alternatieven zijn voor omnummering en multihoming is het dus van essentieel belang voor een middel- tot groot bedrijf, om zijn eigen IPv6 address space te realiseren.
Voor het gebruik van de forward proxy is PI nog niet noodzakelijk door de kleine impact op het netwerk.

Nummering
Maak voor de uitrol van dual stack een nieuw nummering plan.
Het eenvoudigste is, om dit te baseren op het IPv4 plan, maar dit is niet aangeraden. Het IPv4 plan is meestal in de eerste plaats opgesteld om zo efficiënt mogelijk om te gaan met de beschikbare adressen, niet om herkenbaar, eenvoudig of gemakkelijk beheerbaar te zijn. Met IPv6 vervalt de noodzaak om efficiënt met de ruimte om te gaan in zijn geheel. Maak daarom een nieuwe plan dat beter aansluit bij de organisatie en veel meer mogelijkheden voor groei overlaat. Voor tips en richtlijnen hiervoor kan verwezen worden naar het rapport "IPv6-nummerplan opstellen" [30] gemaakt door surfnet. Het is ook te vinden op de Simac SharePoint omgeving.

Let wel, dit rapport heeft het ook over point-to-point verbindingen en dat het soms handiger kan zijn om hiervoor een /127 te gebruiken ipv een /64, maar met als opmerking dat dit tegen de IPv6 standaard is.
Recent, in april 2011, is echter RFC6164 [31] gepubliceerd, met de status "proposed standard", waarin het gebruik van /127 juist word aangeraden voor point-to-point verbindingen, waardoor het argument tegen het gebruik van /127 vervalt.

Kosten
de totale kosten voor een dual stack implementatie zijn bij werknemers een stuk hoger als bij web services omdat er meer netwerk apparatuur bij betrokken is en meer hosts, waarvan allemaal de configuratie moet worden aangepast. Ook is het werknemer netwerk vaak strenger beveiligde, waardoor het vaker voor zal komen dat bepaalde benodigde security features nog niet voor handen zijn op IPv6. Daar omheen plannen en werken kost weer extra tijd.
De schatting per netwerk segment is echter ongeveer het zelfde. Ongeveer 25% van de tijd die het kosten om het IPv4 netwerk te plannen en implementeren. Maar dit is een ruwe schatten, heel afhankelijke van de situatie.

Ook de kosten voor de forward proxy zijn het zelfde als die voor de reverse proxy zoals genoemd in hoofdstuk 4.4

	Aanschaf/installatie	Onderhoud/licentie kosten per jaar
McAfee Web Gateway(VM)	8 manuur minimaal (€664,-)	€20,04 tot 52.55 per node + kosten VM omgeving
McAfee Web Gateway appliance	€1.560,- tot €16.416,- aanschaf + 10 manuur minimaal (€830,-)	€312 tot €3.283

Security
Ook bij werknemer IPv6 connectiviteit is beveiliging is een belangrijk aspect van de IPv6 transitie. Een dual stack implementatie kan gezien worden als het hebben van 2 aparte netwerken, en beiden moeten even goed beschermde worden. Alle beveiligingsmaatregelen en best practice die gelden voor IPv4 zijn ook van kracht bij IPv6.

Het voornaamste voordeel van IPv6 op security gebied is dat IPsec standaard ondersteund moet worden. Het opzetten van beveiligde verbindingen kan daarom gemakkelijker en sneller gebeuren. IPsec werkt voor alle type IP verbindingen omdat het op laag 3 werkt.
Het is echter niet te doen om alle IP packets te versleutelen. Er komt nog aardig wat overhead bij IPsec kijken, meer als bij bijvoorbeeld SSL.

Veel verkeer zal dus onversleuteld blijven, en ook door middel van versleuteld verkeer kan een kwaadwillende schade aanrichten.
IPsec is dus een mooie toevoegingen, maar geen vervanging van de security best practice zoals die al toegepast worden bij IPv4. Alle bestaande security principes en bedreigingen zijn met IPv6 net zo geldig en actueel als bij IPv4.

IPv6 brengt ook een aantal nieuwe bedreigingen met zich mee:
Net als rogue DHCP servers bij IPv4 (en IPv6) kunnen er ook rogue routers zijn die reageren op een "router solicitation multicast request" van een host met SLAAC. Deze rogue router kan vervolgens nagenoeg al het verkeer van deze hosts bekijken en manipuleren voor het door te sturen naar de eigenlijke router van het netwerk. Op de host is hier niks van te merken maar de rogue router is in een perfecte situatie om een man-in-the-middel attack uit te voeren.
En let op: dit geld ook voor het IPv4 verkeer. De meeste hosts zullen IPv6 kiezen boven IPv4. Met wat traffic manipulatie en een DNS translatie kan deze rogue router het doen voorkomen alsof elk domein een IPv6 adres heeft, en zullen de hosts dus altijd het IPv6 netwerk verkiezen boven het IPv4 netwerk, waardoor de rogue router nagenoeg AL het verkeer van alle hosts die hij heeft kunnen manipuleren te zien krijgt. Dit gevaar bestaat ook voor IPv4-only netwerken waarop de hosts wel IPv6 enabled hebben staan (wat de default instelling is in bijvoorbeeld windows) en tunnels naar buiten toe zijn toegestaan. [32]

Een ander vaak gehoord securityissues is de afwezigheid van NAT in IPv6. Elk werkstation is daardoor rechtstreeks vanaf het internet te benaderen, wat sommigen als onveilig ervaren. Echter moderne netwerkbeveiligingsapparatuur gaan allemaal vanuit het principe van "block-all-unless" en zijn daarmee net zo veilig als NAT zou zijn, maar wel veel flexibeler. De afwezigheid van NAT brengt dus geen extra gevaren met zich mee.

6 Native IPv6 verbinding

Met een native IPv6 verbinding wordt bedoeld dat de provider een verbinding levert, waarover een PA of PI IPv6 prefix wordt ondersteund en die connectiviteit levert naar het IPv6 internet. In veel gevallen zal dit neer komen op een verbinding waarover zowel IPv4 als IPv6 wordt geleverd. Dit laatste voorkomt, dat bedrijven extra internet verbinding aan moeten leggen, enkel om IPv6 verbinding te krijgen en die redundant uit te voeren. Dat zou de kosten van een IPv6 implementatie duurder maken dan noodzakelijk.

Een aantal zakelijke providers levert nu al IPv6 verbindingen. Een aantal levert IPv6 aan al hun klanten zonder extra kosten, sommigen alleen op aanvraag, en anderen vragen hier extra voor. Weer andere leveren nu nog geen native IPv6 verbindingen, maar eigenlijk allemaal hebben ze hier wel plannen voor. Het jaar 2012 lijkt voor de meeste hiervan het aangewezen jaar om IPv6 te gaan leveren.

zakelijke providers met native IPv6 verbinding
BIT
Interoute
Luna
RoutIT
XS4ALL
Claranet
Signet
Eurofiber (signet biedt IPv6 aan over het eurofiber netwerk)
surfnet
Edutel (onsbrabantnet gaat in 2012 IPv6 aan bieden en maakt gebruik van het edutelnetwerk)

Plannen van andere grote providers:
UPC: 2012
Ziggo: eind 2012
KPN: voor het einde van 2012
BBned: geen IPv6 plannen kunnen vinden, ook niet van BBned eigenaar Tiscali. (ipv6 over ATM verbinding wel mogelijk)

6.1 **Alternatieven**

Het is niet altijd mogelijk om een native IPv6 verbinding te realiseren. Gelukkig zijn er op internet een paar alternatieve technieken beschikbaar waardoor toch IPv6 connectiviteit gerealiseerd kan worden.
Eigenlijk al deze technieken maken gebruik van tunnels om IPv6 in IPv4 verkeer te encapsuleren (6in4). Maar er zijn veel verschillende technieken om dergelijke tunnels te configureren.

6.1.1 Static Tunnels

Een handmatig geconfigureerde tunnel, die een tunnel op zet naar een zogenaamde tunnelbroker. De tunnel moet aan beide einden ervan worden geconfigureerd, er kan dus niet zomaar verbinding gemaakt worden naar een tunnelbroker. Dit moet vooraf worden afgesproken, meestal door een simpele registratie.
Er zijn verschillende tunnelbrokers voor de particuliere markt die gratis hun diensten aanbieden. Deze voldoen echter meestal niet aan de eisen van de zakelijke markt, bijvoorbeeld op het gebied van betrouwbaarheid en bandbreedte. Inmiddels beginnen sommigen van deze tunnelbrokers (met name HE.net) echter ook zakelijke diensten aan te bieden. Voor deze tunnels moet betaald worden, maar in ruil hiervoor kunnen SLA's afgesloten worden over de uptime en bandbreedte.

Waar je bij de consumententunnels altijd een IPv6 range krijgt toegewezen, wordt bij zakelijke tunnels in sommige gevallen ook ondersteuning geboden voor een eigen PI IPv6 range.
Dit heeft als voordeel dat er geen omnummering hoeft plaat te vinden als er in de toekomst wordt overgegaan op een native verbinding.
De tunnel van HE.net kost 500 dollar per maand en biedt 1Gbps aan bandbreedte en ondersteunt zowel IPv4 als IPv6. BGP is vereist en PI address space is ondersteund. [32]

Voordelen
- Verkeerrouting is duidelijk.
- Zakelijke tunnel is betrouwbaar.
- Mogelijk om eigen IP range te gebruiken, omnummeren bij overgang naar native niet persé noodzakelijk.
- Hosting van services door tunnel mogelijk.
- SLA's mogelijk bij zakelijke tunnels.

Nadelen
- Zakelijke tunnel kost geld (maar is goedkoper dan een extra lijn aan laten leggen.)
- (iets) Hogere latency/meer hops dan een native verbinding.

6.1.2 6to4

RFC3056 [15]
Zoals eerder beschreven stelt 6to4 een netwerk in staat om met één public IPv4 adres verbinding te maken met het IPv6 internet door het gebruik van relays.
Iedere IPv4 hosts met een public adres die hier gebruik van wil maken kan een IPv6 /48 prefix genereren aan de hand van zijn IPv4 adres. Dit adres begint met 2002: gevolgd door het IPv4 adres omgezet in hexadecimale.

Voor consumenten is dit een vrij aantrekkelijke techniek. Hij is eenvoudig op te zetten en werkt in de meeste gevallen goed genoeg. En voor bedrijven betekent de korte /48 prefix dat er genoeg ruimte is voor subnetting. Maar voor bedrijven kleven er echter grote nadelen aan 6to4. Want hoewel er over de 6to4 relays van de eigen ISP, verantwoordelijk voor de upstream, mogelijk afspraken gemaakt kunnen worden over uptime en bandbreedte geld dat niet voor de relays verantwoordelijk voor de downstream.
En als de huidige ISP('s) geen eigen relayservers hebben kan het zelfs lastig zijn om te achterhalen welke relayserver er gebruikt word om het upstream verkeer af te handelen.

Ook de vaste prefix is niet ideaal. De prefix is niet lang en even lang als de meeste PI prefix's zouden zijn, waardoor in de meeste gevallen enkel de prefix veranderd hoeft. Maar zelfs de prefix veranderen is op dit moment niet gemakkelijk. Er zijn nog geen manieren om dit netwerkbreed in een keer uit te rollen. De keuze voor 6to4 betekend dus gegarandeerd omnummeren bij een overgang naar een native verbinding.

Voordelen

- Hosting mogelijk met vast IPv4 adres: IPv6 adres gerelateerd aan IPv4 adres en daarom stabiel.
- altijd te gebruiken mitst er minimaal één public IP adres is.
- Gratis.
- Korte /48 prefix, zeker 16bit ruimte voor subnetting beschikbaar.

Nadelen

- Relayservers kwaliteit mogelijk niet gegarandeerd, upstream ISP afhankelijk, downstream relay verschilt per host, en is daarom nooit gegarandeerd.
- Niet altijd duidelijk bij welke relayserver je pakketten uitkomen.
- Vaste prefix. Omnummering noodzakelijk als er een native IPv6 verbinding beschikbaar komt.
- Hogere latency/meer hops dan een native verbinding.

6.2 **Aanbevelingen**

Een native IPv6 verbinding is in alle gevallen de beste oplossing. Het heeft de hoogste betrouwbaarheid, laagste latency en een voorspelbare bandbreedte, maar is niet altijd meteen mogelijk.
Steeds meer providers bieden IPv6 aan op hun netwerk of zijn van plan om dat binnenkort te doen. Het jaar 2012 lijkt voor de grote spelers in de markt het aangewezen jaar om IPv6 aan de klant te gaan leveren. In veruit de meeste gevallen worden hiervoor geen extra kosten in rekening gebracht.

Het verstandigste is om IPv6 bij de bestaande providers te betrekken. Speciaal voor IPv6 een extra internet verbinding aanleggen is in de meeste gevallen niet aantrekkelijk vanwege de extra kosten, terwijl de huidige providers misschien het jaar erna ook IPv6 aanbieden. Maar wat te doen in de tussentijd?

Om deze periode te overbruggen is een zakelijke tunnelprovider de beste optie. Deze biedt veel van de voordelen van een native verbinding, (betrouwbaar, gegarandeerde snelheid en PI address space ondersteuning) maar zonder de hoge startkosten of een langlopend contract. Ze zijn snel te verkrijgen en op te zetten en er is dus ook snel weer vanaf te komen als er geen noodzaak meer voor is.
De bescheiden maandelijkse kosten zijn goed op te brengen voor iets dat in de meeste gevallen één, misschien twee jaar gebruikt zal worden.
En als het tunneleindpunt wordt behandeld zoals elke internetverbinding wordt behandeld zijn er geen extra security issues verbonden aan het gebruik van de tunnel.

6to4, het andere alternatief, is gratis, snel op te zetten en is voor consumentenmarkt redelijk betrouwbaar gebleken, maar biedt simpelweg niet genoeg zekerheid voor de zakelijke markt.
In een productieomgeving wordt het gebruik hiervan daarom ook sterk afgeraden. In een testlab omgeving zou het goed dienst kunnen doen, maar als men serieus met IPv6 aan de slag wil gaan is, als een native verbinding niet mogelijk is, de (zakelijk) tunnel een beter alternatief.

Bibliografie

[1] INTEC Inc. IPv4 Exhaustion Counter. [Online]. http://inetcore.com/project/ipv4ec/index_en.html

[2] RIPE. (2009, Sep.) RIPE NCC - IPv6 Provider Independent (PI) Assignments. [Online]. http://www.ripe.net/ripe/docs/ripe-481#_8._IPv6_Provider

[3] University of Oregon. (2011, Nov.) http://routeviews.org/ University of Oregon Route Views Project. [Online]. http://archive.routeviews.org/route-views6/bgpdata/2011.11/RIBS/rib.20111101.0000.bz2

[4] Public. (2011, Oct.) Comparison_of_IPv6_support_by_major_transit_providers. [Online]. http://en.wikipedia.org/wiki/Comparison_of_IPv6_support_by_major_transit_providers

[5] IETF. (2005, Oct.) RFC4213 Basic Transition Mechanisms for IPv6 Hosts and Routers. [Online]. http://tools.ietf.org/html/rfc4213

[6] CIsco. (2011, May) What Enterprises Should Do About IPv6 In 2011. [Online]. http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6553/whitepaper_c11-586154.html

[7] IETF. (2011, Apr.) RFC6145 IP/ICMP Translation Algorithm. [Online]. http://tools.ietf.org/html/rfc6145

[8] IETF. (2010, Oct.) RFC6052 IPv6 Addressing of IPv4/IPv6 Translators. [Online]. http://tools.ietf.org/html/rfc6052

[9] IETF. (2011, Apr.) RFC6144 Framework for IPv4/IPv6 Translation. [Online]. http://tools.ietf.org/html/rfc6144

[10] IETF. (2000, Feb.) RFC2766 Network Address Translation - Protocol Translation (NAT-PT). [Online]. http://tools.ietf.org/html/rfc2766

[11] IETF. (2007, July) RFC4966 Reasons to Move the Network Address Translator - Protocol Translator. [Online]. http://tools.ietf.org/html/rfc4966

[12] IETF. (2011, Apr.) RFC6146 http://tools.ietf.org/html/rfc6146. [Online]. http://tools.ietf.org/html/rfc6146

[13] IETF. (2011, Oct.) RFC6384 An FTP Application Layer Gateway (ALG) for IPv6-to-IPv4 Translation. [Online]. http://tools.ietf.org/html/rfc6384

[14] Cisco. (2011, Oct.) Release Note vA5(1.x), Cisco ACE Application Control Engine Module. [Online]. http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/ace/vA5_1_x/release/note/ACE_mod_rn_A51x.html

[15] IETF. (2001, Feb.) RFC3056 Connection of IPv6 Domains via IPv4 Clouds. [Online]. http://tools.ietf.org/html/rfc3056

[16] IETF. (2010, Apr.) RFC5569 IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) Protocol Specification. [Online]. http://tools.ietf.org/html/rfc5569

[17] IETF. (2006, Feb.) RFC4380 Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs). [Online]. http://tools.ietf.org/html/rfc4380

[18] IETF. (2006, Oct.) RFC4214 Intra-Site Automatic Tunnel Addressing Protocol (ISATAP). [Online]. http://tools.ietf.org/html/rfc4214

[19] IETF. (2011, Aug.) RFC6333 Dual stack Lite Broadband Deployments Following IPv4 Exhaustion. [Online]. http://tools.ietf.org/html/rfc6333

[20] IETF. (2011, June) RFC6296 IPv6-to-IPv6 Network Prefix Translation. [Online]. http://tools.ietf.org/html/rfc6296

[21] Cisco. (2011, Oct.) Start Here: Cisco IOS Software Release Specifics for IPv6 Features. [Online]. http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-roadmap.html

[22] Cisco. (2011, June) NAT64 Technology: Connecting IPv6 and IPv4 Networks. [Online]. http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6553/white_paper_c11-676278.html

[23] Cisco. (2011, Dec.) Stateful Network Address Translation 64. [Online]. http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_nat/configuration/xe-3s/iadnat-stateful-nat64.pdf

[24] Microsoft. IPv6 and IIS 6.0. [Online]. http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/4c7c6bce-213a-4125-bc36-2202e3b4c8c8.mspx?mfr=true

[25] IETF. (2008, July) RFC5211 An Internet Transition Plan. [Online]. http://tools.ietf.org/html/rfc5211

[26] The IPv6 Forum. (2011, Dec.) The IPv6 Forum. [Online]. https://www.ipv6ready.org/db/index.php/public/search/?do=1&lim=25&p=0

[27] McAfee, "McAfee Firewall Enterprise 8.1.x Product Guide," McAfee, 2011.

[28] IETF. (1999, Aug.) RFC2671 Extension Mechanisms for DNS (EDNS0). [Online]. http://tools.ietf.org/html/rfc2671

[29] Cisco. Cisco - DNSSEC. [Online]. http://www.cisco.com/web/about/security/intelligence/dnssec.html

[30] surfnet. (2010, Feb.) surfnet.nl IPv6 nummerplan v10. [Online]. http://www.surfnet.nl/Documents/handleiding_201002_IPv6_nummerplan_v10.pdf

[31] IETF. (2011, Apr.) RFC6164 Using 127-Bit IPv6 Prefixes on Inter-Router Links. [Online]. http://tools.ietf.org/html/rfc6164

[32] Alec Waters. (2011, Apr.) SLAAC Attack – 0day Windows Network Interception Configuration Vulnerability. [Online]. http://resources.infosecinstitute.com/slaac-attack/

[33] EON. Hurricane Electric to Offer Premium Tunnel Broker Service. [Online]. http://eon.businesswire.com/news/eon/20110606006365/en/IPv6/World-IPv6-Day/IPv6-Transition

[34] (1998, Dec.) RFC2460 Internet Protocol, Version 6 (IPv6) Specification. [Online]. http://tools.ietf.org/html/rfc2460