FS-20150610.03A

Anna van Buerenplein 1
2595 DA Den Haag
Postbus 96800
2509 JE Den Haag

www.tno.nl

T +31 88 866 90 00

TNO-rapport

TNO 2015 10435 | Eindrapport v1.0

Overheidsbrede beleidskaders voor IPv6-nummerplannen

Datum	3 april 2015
Auteur(s)	Arjen Holtzer, Otto Baijer, Annelieke van der Giessen, Bart Gijsen (TNO) Piet Hein Minnecré, Rob Meijer (PBLQ)
Exemplaarnummer	
Oplage	
Aantal pagina's	65 (incl. bijlagen)
Aantal bijlagen	1
Opdrachtgever	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Directoraat-generaal Bestuur en Koninkrijksrelaties, Directie Burgerschap en Informatiebeleid
Projectnaam	Overheidsbrede beleidskaders voor IPv6-nummerplannen
Projectnummer	060.12424

Dit onderzoek is uitgevoerd in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. De verantwoordelijkheid voor de inhoud van het onderzoek berust bij de auteurs. De inhoud vormt niet per definitie een weergave van het standpunt van de Minister van Binnenlandse Zaken en Koninkrijksrelaties.

FS-20150610.03A

Bestuurlijke samenvatting

Titel :	Overheidsbrede beleidskaders voor IPv6-nummerplannen
Auteur(s) :	Arjen Holtzer, Otto Baijer, Annelieke van der Giessen, Bart Gijsen (TNO) Piet Hein Minnecré, Rob Meijer (PBLQ)
Datum :	3 april 2015
Opdrachtnr. :	060.12424
Rapportnr. :	TNO 2015 10435

Strategische relevantie onderzoek overheidsbreed IPv6-nummerplankader

Invoering van een overheidsbreed IPv6-nummerplankader biedt kansen voor een overzichtelijke en veilige inrichting van ICT bij de Nederlandse overheid. Het kan een instrument zijn om strategische doelstellingen van de overheid op het gebied van leveranciersonafhankelijkheid en communicatie over besloten netwerken te ondersteunen. Enkele voordelen kunnen op korte termijn worden gehaald. Het nu al werken volgens een IPv6-nummerplankader maakt het eenvoudiger om toekomstige strategische keuzes door te voeren, waarmee risico's op fouten en migratiekosten in de toekomst kunnen worden voorkomen.

Aanleiding en vraagstelling

Deze samenvatting beschrijft op hoofdlijnen de resultaten van het onderzoek dat TNO heeft uitgevoerd in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties getiteld: *"De Nederlandse overheid ook de komende decennia bereikbaar: IPv6-nummerplan Nederlandse Overheid".*

De aanleiding voor dit onderzoek is de introductie van Internet Protocol versie 6 (IPv6) in ICT-netwerken en –diensten van de Nederlandse overheid. De overheid heeft het belang van deze invoering onderschreven onder meer door opname van deze standaard op de pas-toe-en-leg-uit-lijst van open standaarden[1] van het Forum Standaardisatie en de doelstellingen in de Digitale Agenda[2].

IPv6 wordt op dit moment wereldwijd uitgerold om de groei van internet de komende decennia aan te kunnen. Om te kunnen communiceren beschikken alle apparaten, zoals PC's, servers en routers, in een ICT-netwerk over een Internet Protocol (IP) adres. IP versie 6 is de opvolger van IP versie 4 dat sinds de jaren '80 wordt gebruikt in (inter)netwerken.

Sommige overheidsonderdelen zijn al begonnen met de introductie van IPv6 en het zal de komende jaren steeds verder worden ingevoerd in de ICT-omgeving van de overheid. Een essentieel onderdeel bij de introductie van IPv6 is het opstellen van

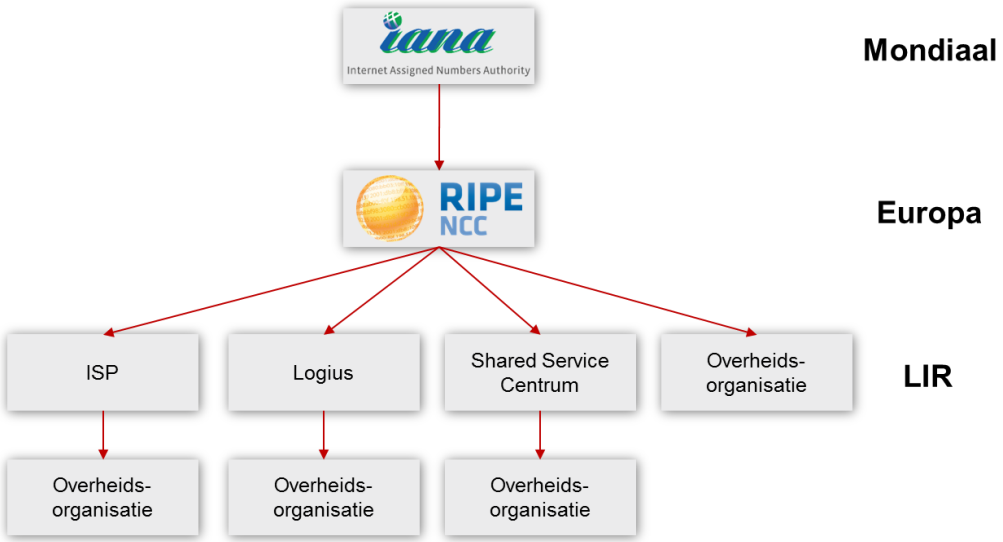
[1] https://www.forumstandaardisatie.nl/open-standaarden/voor-overheden/pas-toe-of-leg-uit-regime/
[2] http://www.rijksoverheid.nl/documenten-en-publicaties/notas/2011/05/17/digitale-agenda-nl-ict-voor-innovatie-en-economische-groei.html

een IPv6-nummerplan, waarin afspraken over het gebruik van IPv6-adresblokken staan. Voor het Rijk bestaat al een gecoördineerd IPv6-nummerplanbeleid.

De invoering van IPv6 biedt de kans om via gemeenschappelijke afspraken over IPv6-nummerplannen – een “IPv6-nummerplankader” – bij te dragen aan een voor de overheid zo overzichtelijk, veilig en voordelig mogelijke invoering van IPv6. De hoofdvraag die dit onderzoek beantwoord is:

“In hoeverre en onder welke voorwaarden kunnen gezamenlijke afspraken aangaande IPv6-nummerplannen tussen overheidsorganisaties voor de Nederlandse Overheid leiden tot kansen voor leveranciersonafhankelijkheid, informatieveiligheid, financieel voordeel en eventuele overige baten, rekening houdend met het organisatorische en bestuurlijke landschap?”

De IPv6-adressen die door overheden worden gebruikt maken onderdeel uit van een wereldwijd georganiseerd uitgifteproces. De figuur geeft dit mondiale, hiërarchisch georganiseerde IP-adresuitgifteproces en hoe overheidsorganisaties daar een plaats in kunnen hebben weer.



Beantwoording van de onderzoeksvragen

Uit het onderzoek komt naar voren dat een beperkte set afspraken een bijdrage kan leveren aan leveranciersonafhankelijkheid, informatieveiligheid en efficiënt beheer van de ICT-infrastructuur van de overheid. Dit kan worden bereikt door het in gebruik nemen van overheidseigen IPv6-adressen. Met overheidseigen adressen kan de overheid zelf haar IPv6-adressen op internet beter beschermen tegen misbruik, kunnen omnummerkosten bij een leverancierswissel worden voorkomen en wordt het mogelijk om overheden redundant via verschillende internetproviders aan te sluiten. Het gebruik van één overheidsadresblok maakt adressen herkenbaarder en eenvoudiger te registreren wat kan helpen bij detectie van misbruik en het maken van onderscheid tussen overheidsverkeer en niet-overheidsverkeer. De mate waarin een overheidsbreed IPv6-nummerplankader deze voordelen biedt hangt samen met de mate waarin de Nederlandse overheid in het algemeen haar ICT in eigen hand wenst te houden en welke aspecten zij aan leveranciers wil overlaten. In bijvoorbeeld Duitsland speelt communicatie over

besloten netwerken en de beheercomplexiteit die dit met zich meebrengt een belangrijke rol in hun keuze om te werken met een overheidsbreed IPv6-nummerplan.

Voorkeursinrichting overheidsbreed IPv6-nummerplankader
Deze aanbevelingen dienen als startpunt voor een definitieve vaststelling van een overheidsbreed IPv6-nummerplankader, waarbij het van belang is dit gezamenlijk met (technische) stakeholders van decentrale overheden op te stellen. Daarnaast bevelen we aan om discussies aangaande de technische implementatie van een overheidsbreed IPv6-nummerplan die spelen in onder meer Duitsland en Spanje te volgen, omdat ook daar nog niet alles is uitgekristalliseerd, en aansluiting te zoeken bij meer strategische discussies binnen de Nederlandse overheid over het gebruik van besloten netwerken en leveranciersonafhankelijkheid in het kader van informatiebeveiliging. De toegevoegde waarde van een IPv6-nummerplankader neemt sterk toe wanneer het ingezet wordt in combinatie met overige maatregelen gericht op het realiseren van dergelijke strategische doelen.

In de kern behelst het nummerplankader het gebruik van overheidseigen IPv6-adresblokken. Dit wordt gefaciliteerd door centraal één overheids-IPv6-blok aan te vragen door een centrale overheids-Local Internet Registry (LIR), waarvoor Logius op dit moment de meest voor de handliggende partij lijkt. De centrale LIR hanteert de standaardvoorschriften voor adresuitgifte aan overheidsorganisaties. Verder dienen afspraken te worden gemaakt voor overheidskoppelingen en dient iedere overheidsorganisatie over een IPv6-nummerplan te beschikken.

Het verdient de aanbeveling het kader onderdeel te maken van de Generieke Digitale Infrastructuur (GDI) van de overheid en daarmee onderhavig te maken aan de daarvoor geldende governancestructuur, omdat er sprake is van overheidsbrede afspraken. De financiering van het kader kan structureel worden geregeld door het mee te nemen in de financiering van de GDI.

We bevelen aan om de toepassing van het IPv6-nummerplankader gelijk te laten lopen met momenten waarop overheidsorganisaties IPv6 introduceren in bepaalde netwerken of diensten, bijvoorbeeld bij aanbestedingen op het gebied van ICT. Deze invoering is van belang, omdat in de praktijk eventuele nieuwe aandachtspunten aan het licht kunnen komen die tot een bijstelling of concretere invulling van het kader kunnen leiden.

Tot slot helpt de invoering van dit IPv6-nummerplankader overheden om na te denken over de invoering van IPv6 en de wijze waarop ze dit doen door aandacht te vestigen op het onderwerp. Bij sommige overheden zal kennis over de invoering van IPv6 in huis aanwezig zijn, maar voor andere overheden kan de invoering een uitdaging vormen. Overweeg daarom om ook andere taken ter ondersteuning van overheden bij de invoering van IPv6 bij de centrale beheerder te beleggen
.

Versiegeschiedenis

Versie	Datum	Omschrijving
v0.7	23 februari 2015	Pre-conceptversie ter review aan BZK en SURFnet. TNO-interne review door Frits Klok.
v0.9	6 maart 2015	Conceptversie ter review aan de volledige begeleidingscommissie en ter inzage aan alle geraadpleegde stakeholders. TNO-interne review op §4.2 door Sander Degen.
v1.0	3 april 2015	Eindversie

FS-20150610.03A

Inhoudsopgave

Bijlage(n)

A Rekenvoorbeeld omnummerimpact Nederlandse overheid

Versiegeschiedenis **5**

Inhoudsopgave **6**

1 Inleiding **8**
1.1 Doelstelling en onderzoeksvragen 8
1.2 Definitie IPv6-nummerplan en IPv6-nummerplankaders en scoping 9
1.3 Werkwijze 9
1.4 Betrokken partijen 10
1.5 Leeswijzer 11

2 Over IPv6-nummerplannen **12**
2.1 Het gebruik van IP-nummerplannen 12
2.2 De introductie van IPv6 en relevante IPv6-eigenschappen voor nummerplannen 12
2.3 De relatie met besloten netwerken 15
2.4 Vanwaar de interesse voor IPv6-adresplannen bij overheden in het algemeen 16
2.5 IP-adresuitgifteproces 17

3 Wensen en randvoorwaarden overheidsbreed IPv6-nummerplankader **20**
3.1 Leveranciersonafhankelijkheid 20
3.2 Informatieveiligheid 21
3.3 Financieel voordeel 21
3.4 Randvoorwaarden en overige baten 22
3.5 Conclusies 23

4 Analyse **24**
4.1 Leveranciersonafhankelijkheid 24
4.1.1 Analyse 24
4.1.2 Conclusie 30
4.2 Informatieveiligheid 31
4.2.1 Analyse 31
4.2.2 Conclusie 37
4.3 Financieel voordeel 37
4.3.1 Analyse 37
4.3.2 Conclusie 41
4.4 Overige baten en randvoorwaarden 42
4.4.1 Toekomstvastheid 42
4.4.2 Bestuurlijke autonomie 43
4.4.3 Overige technische aandachtspunten van het gebruik van een overheidsprefix 43
4.5 Conclusie 47

5 Elementen IPv6-nummerplankader NL overheden **49**
5.1 Element 1: Eigendom van door de overheid gebruikte IPv6-adressen 50

5.1.1 Toelichting element 1 50
5.1.2 Voorkeursinrichting element 1 50
5.2 Element 2: Herkomst van gebruikte IPv6-adressen (LIR-schap) 51
5.2.1 Toelichting element 2 51
5.2.2 Voorkeursinrichting element 2 51
5.3 Element 3: IPv6 uitgiftebeleid binnen de overheid 53
5.3.1 Toelichting element 3 53
5.3.2 Voorkeursinrichting element 3 53
5.4 Element 4: Zonering binnen overheidsorganisaties 53
5.4.1 Toelichting element 4 53
5.4.2 Voorkeursinrichting element 4 54
5.5 Element 5: Overige afspraken over IPv6-nummerplannen 54
5.5.1 Toelichting element 5 54
5.5.2 Voorkeursinrichting element 5 54
5.6 Besturing, uitvoering en financiering van het IPv6-nummerplankader 55
5.6.1 Governance van het IPv6-nummerplankader 55
5.6.2 Uitvoering van het IPv6-nummerplankader 57
5.6.3 Financiering van het IPv6-nummerplankader 58

6 Conclusies en aanbevelingen 59

7 Ondertekening 62

1 Inleiding

In november 2014 heeft de Nederlandse overheid aan TNO de opdracht gegeven om het onderzoek *"De Nederlandse overheid ook de komende decennia bereikbaar: IPv6-nummerplan Nederlandse Overheid"* uit te voeren.

Dit rapport beschrijft de werkwijze en resultaten van dit onderzoek.

1.1 Doelstelling en onderzoeksvragen

Het doel van dit onderzoek is om nadere duidelijkheid te geven in hoeverre en onder welke voorwaarden overheidsbrede afspraken aangaande IPv6-nummerplannen kunnen leiden tot meer control, autonomie[3] en kansen op het gebied van leveranciersonafhankelijkheid, informatieveiligheid en financieel voordeel.

De hoofdvraag die de overheid heeft gesteld voor dit onderzoek is tijdens het begin van project met de opdrachtgever geherformuleerd als volgt:

"In hoeverre en onder welke voorwaarden kan IPv6-nummerplanbeleid voor de Nederlandse Overheid tot kansen voor leveranciersonafhankelijkheid, informatieveiligheid, financieel voordeel en eventuele overige baten leiden, rekening houdend met het organisatorische en bestuurlijke landschap."

Hierbij heeft de overheid de volgende deelvragen gesteld:

1. In hoeverre en onder welke voorwaarden is te verwachten dat een IPv6-nummerplankader voor de hele Nederlandse Overheid tot kansen voor leveranciersonafhankelijkheid, informatieveiligheid, financieel voordeel en overige baten zal leiden?
2. Op welke wijze kan een overheidsbreed IPv6-nummerplankader bestuurlijk ingericht worden, mede in relatie tot de Generieke Digitale Infrastructuur[4]?
3. Op welke wijze kan een overheidsbreed IPv6-nummerplankader het beste ingericht worden?
4. Op welke wijze kan het registratieproces en administratieve inrichting gezien de autonomie van de overheden en hun decentrale karakter het beste georganiseerd worden?
5. Op welke wijze kan het nummerplankader het beste op strategisch, tactisch en operationeel niveau onderhouden worden?
6. Op welke wijze kan de inbedding en implementatie bij alle relevante organisaties georganiseerd worden?
7. Welke wijze van financiering is gezien de voorgaande vragen het meest geëigend?

[3] De term 'control' is in overleg met de opdrachtgever niet meer als apart criterium in dit onderzoek opgenomen maar meegenomen als onderdeel van de aspecten leveranciersonafhankelijkheid, informatieveiligheid en financieel voordeel. De term 'autonomie' wordt in dit onderzoek alleen gebruikt in de zin van bestuurlijke autonomie.

[4] De Generieke Digitale Infrastructuur van de overheid (GDI) bestaat uit standaarden, producten en voorzieningen die gezamenlijk worden gebruikt door alle overheden, vele publieke organisaties en in een aantal gevallen door private partijen, zie http://www.digicommissaris.nl/thema/generieke-digitale-infrastructuur-gdi.

1.2 Definitie IPv6-nummerplan en IPv6-nummerplankaders en scoping

In dit onderzoek maken we onderscheid tussen IPv6-nummeradministraties, IPv6-nummerplannen en IPv6-nummerplankaders.

IPv6-nummeradministratie: een overzicht van specifieke IPv6-adressen of IP-blokken die zijn toegewezen aan een bepaald apparaat, netwerk, dienst, of organisatie, zoals typisch wordt bijgehouden in een spread-sheetdocument of een IP Address Management systeem (IPAM).

IPv6-nummerplan: de manier waarop een individuele overheid omgaat met zijn adresblokken op het gebied van adresuitgifte, -aanvraag, -registratie, voorschriften betreffende de indeling van het adresblok en de governance op deze aspecten.

IPv6-nummerplankader: een set van afspraken tussen overheden aangaande IPv6-nummerplannen over één of meer van de aspecten adresuitgifte, -toewijzing, -aanvraag, -registratie, voorschriften betreffende de indeling van het adresblok en de governance van deze afspraken. Het IPv6-nummerplankader valt onder algemeen ICT-beleid binnen de overheid.

Dit onderzoek richt zich op de kansen die een overheidsbreed IPv6-nummerplankader met zich meebrengt. Er wordt geen onderzoek uitgevoerd aangaande IPv6-nummerplannen en nummeradministraties.

In dit rapport is gekozen om de term ‘nummerplan’ te gebruiken en niet de term ‘adresplan’. Hier is voor gekozen, omdat de overheid deze term ook gebruikt in haar onderzoeksvragen en deze term bijvoorbeeld ook door SURFnet en in verschillende technische standaarden (“renumbering”) wordt gebruikt. Er wordt in dit rapport gesproken over ‘IP-adressen’ en niet over ‘IP-nummers’.

1.3 Werkwijze

Dit onderzoek bestaat uit de volgende stappen:

- Het opstellen van beoordelingscriteria en verwachte voordelen van overheidsbreed IPv6-nummerplanbeleid;
- Het formuleren van de elementen van het IPv6-nummerplankader. Een element bevat een bepaalde keuze over een gezamenlijke afspraak tussen overheden.
- Analyse van de beoogde voordelen en de gevolgen daarvan voor de keuze per element van het IPv6-nummerplankader.
- Het beantwoorden van de hoofdvraag op basis van de analyse en het formuleren van aanbevelingen.

Voor dit onderzoek is gebruik gemaakt van relevante openbare documentatie, overheidsinterne documentatie en interviews met verschillende stakeholders, onder andere ervaringsdeskundigen op het gebied van IPv6-nummerplannen bij overheidsorganisaties in binnen –en buitenland, (de)centrale overheden in Nederland en leveranciers.

Verder is er in het onderzoek een belangrijke rol weggelegd voor de begeleidingscommissie, die bestaat uit vertegenwoordigers van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (DGBK en DGOBR), Logius, KING, IPO, UvW, de Manifestgroep en SURFnet en is weergegeven in Tabel 1. De begeleidingscommissie is tijdens dit onderzoek meerdere keren bijeen geweest en heeft een belangrijke rol gehad bij het vaststellen van de criteria die gehanteerd zijn bij de beoordeling van de verschillende oplossingsrichtingen. Daarnaast zijn de elementen van het IPv6-nummerplankader, de analyse en adviezen uitgebreid bij de begeleidingscommissie getoetst.

Tabel 1: Leden van de begeleidingscommissie

Naam	**Organisatie**
Arjan de Jong, Michelle van Dijk	Ministerie van BZK DGBK/B&I
Leon Paul de Rouw, Edgar Heijmans	Ministerie van BZK DGOBR
	Ministerie van BZK DGBK
Bart Knubben	Ministerie van BZK Bureau Forum Standaardisatie
Cees vd Poel, Glenn Lutke Schipholt	Ministerie van BZK Logius
Michel Voorsluijs	Manifestgroep / Belastingdienst
Arianne de Man	IPO
John-Paul Kloosterman	Provincie Fryslân
Ruud van der Lee	Provincie Noord-Brabant
André Batenburg	Provincie Zuid-Holland
Marianne Krug	UvW
Anita van Nieuwenborg, Theo Peters	VNG/KING
Rogier Spoor	SURFnet

1.4 Betrokken partijen

Tijdens dit onderzoek zijn naast de leden van de begeleidingscommissie verschillende stakeholders en experts binnen en buiten de Nederlandse overheid geraadpleegd. De volledige lijst is weergegeven in Tabel 2.

Tabel 2: Lijst van geraadpleegde stakeholders en experts tijdens het onderzoek

Naam	**Organisatie**
Michiel Ettema	Gemeente Alkmaar
John Dautzenberg	Gemeente Heerlen
Gabor Verputten	Hoogheemraadschap Hollands Noorderkwartier
Jan de Groot	Provincie Overijssel (SSC Zwolle)
Michiel Oosterwijk	NCSC
Bert de Krijger, Jaco de Vries, Christian Oomen	British Telecom
Gert Jan van der Leer	Centric
Pieter Bas Nederkoorn, Jan Lammerts	KPN Lokale Overheid
Martin Krengel	Citkomm, Duitsland
Bart Hanssens	FedICT, België
Constanze Bürger, Tahar Schaa	Ministerie van Binnenlandse Zaken, Duitsland
Carlos Gomez Munoz	Ministerie van Financiën, Spanje

1.5 Leeswijzer

Dit rapport is als volgt opgebouwd:

- In Hoofdstuk 2 worden de achtergrond en context van het onderzoek geschetst aangaande IP-nummerplannen en IPv6 in het algemeen en bij overheden.
- Vervolgens worden in Hoofdstuk 3 de verwachte voordelen van een overheidsbreed IPv6-nummerplankader geschetst, met daarbij de belangrijkste criteria die moeten worden meegenomen bij het opstellen van een dergelijk kader.
- In Hoofdstuk 4 volgt de analyse aangaande de potentiële voordelen en onder welke omstandigheden deze al dan niet realiseerbaar zijn. In overleg met de opdrachtgever is er voor gekozen om deze analyse vrij uitgebreid in het rapport op te nemen.
- In Hoofdstuk 5 wordt het IPv6-nummerplankader zelf geïntroduceerd en worden de keuzes met argumentatie voor een voorkeursinrichting gegeven op basis van de analyse in Hoofdstuk 4.
- In Hoofdstuk 6 staan de conclusies, de beantwoording van de onderzoeksvragen en de handelingsperspectieven voor de overheid op basis hiervan.

2 Over IPv6-nummerplannen

Dit hoofdstuk beschrijft de achtergrond van IP-nummerplannen op basis van literatuur en bestaande ervaringen met IPv6-nummerplannen bij overheidsorganisaties.

2.1 Het gebruik van IP-nummerplannen

Om te kunnen communiceren hebben apparaten, zoals PC's, servers en routers, in een ICT-netwerk allemaal een Internet Protocol (IP) adres. Om een dergelijk netwerk efficiënt te kunnen beheren is het noodzakelijk inzicht te hebben in welk apparaat van welk IP-adres gebruik maakt. In geval van netwerkproblemen kan het IP-adres bijvoorbeeld worden gebruikt om te kijken of een apparaat nog bereikbaar is. Ook kunnen op basis van IP-adressen bepaalde beveiligingsmaatregelen worden getroffen, bijvoorbeeld met firewalls, om ervoor te zorgen dat niet-bevoegden niet zomaar alle apparaten in het netwerk kunnen benaderen.

Bij een zeer eenvoudig netwerk, bijvoorbeeld een thuisnetwerk, is het niet nodig om een IP-nummerplan op te stellen, omdat de eigenaar de adressen makkelijk kan onthouden, of omdat de instellingen op een standaardmanier door de internetprovider zijn geconfigureerd. Als een netwerk wat groter wordt, of als er belangrijke diensten in draaien wordt het al snel belangrijk voor beheerders om over een overzicht te beschikken van welke apparaten van welk IP-adres gebruik maken.

Daarnaast zijn nummerplannen in netwerken ondersteunend aan de netwerkarchitectuur. Door structuur aan te brengen in de adressering van apparaten, kan netwerkbeheer efficiënter worden uitgevoerd. Bijvoorbeeld: het toevoegen van een nieuw apparaat kan eenvoudiger gaan als daar in het nummerplan ruimte voor is opgenomen.

Nederlandse overheidsorganisaties maken ook gebruik van IP-nummerplannen. Sterker nog, als het goed is bestaat er voor iedere overheidsorganisatie met een ICT-infrastructuur een IP-nummerplan. Het gaat hierbij dan in de meeste gevallen om IPv4-nummerplannen en in slechts in enkele gevallen om IPv6-nummerplannen, omdat veel organisaties hier nog niet mee aan de slag zijn. Wat betreft de huidige IP-nummerplannen bestaan er geen overheidsbrede afspraken.

2.2 De introductie van IPv6 en relevante IPv6-eigenschappen voor nummerplannen

Omdat IPv4 met ca. 4 miljard beschikbare IP-adressen onvoldoende ruimte heeft om de groei van internet te kunnen ondersteunen is in de jaren '90 van de vorige eeuw IPv6 ontwikkeld. Dit protocol beschikt over 10^38 unieke IP-adressen en kan daarmee als opvolger van IPv4 de sterke groei van het aantal apparaten dat op internet wordt aangesloten voor de komende decennia aan. Deze groei wordt

vooral veroorzaakt door het toenemende aantal mobiele apparaten, 'machine-to-machine'-toepassingen en het *Internet of Things*[5].

De uitrol van IPv6 wereldwijd en in onze buurlanden neemt gestaag toe, bijvoorbeeld 35% van de internetgebruikers in België, 17% in Duitsland en ruim 2% in Nederland[6]. Daarnaast maken sommige applicaties verplicht gebruik van IPv6, bijvoorbeeld Microsofttoepassingen[7], waardoor IPv6 al op netwerken gebruikt wordt zonder dat de beheerder van dat netwerk IPv6 bewust heeft geïntroduceerd.

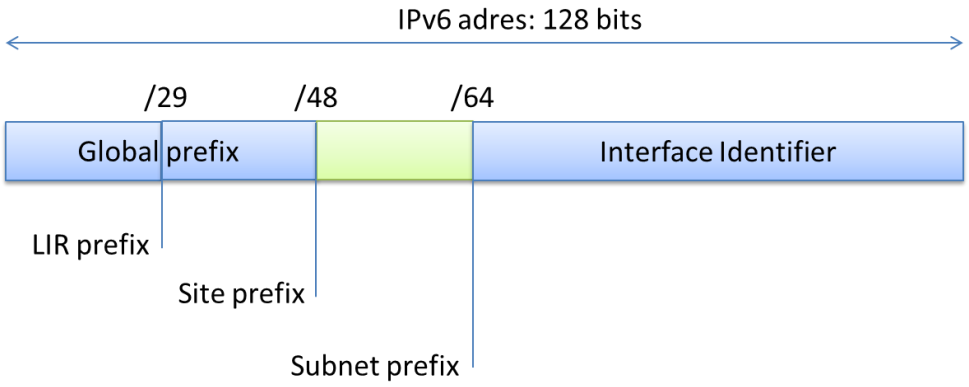
Tijdens de overgangsperiode van IPv4 naar IPv6 worden de twee protocollen naast elkaar gebruikt. Omdat deze overgangsperiode lang zal duren, wordt in veel gevallen gesproken over de introductie van IPv6 naast IPv4, in plaats van een migratie van IPv4 naar IPv6. In de praktijk betekent dit dat een overheidsorganisatie twee netwerken moet inrichten, beheren en beveiligen: de IPv4-omgeving en de IPv6-omgeving. Overigens kan dit in veel gevallen op dezelfde fysieke apparatuur worden gerealiseerd: een laptop, server of router kan tegelijkertijd van zowel IPv4 als IPv6 gebruikmaken. Hiervoor wordt de term *dual-stack* gebruikt. Daarnaast kan een organisatie er voor kiezen om op bepaalde plekken in het interne bedrijfsnetwerk, bijvoorbeeld voor werkplekken, maar één internetprotocol te gebruiken: ofwel IPv4 ofwel IPv6.

Een IPv6-nummerplan leidt tot een IPv6-nummeradministratie die niets anders is dan een overzicht van apparaten en netwerken en hun bijbehorende IPv6-adres of prefix. Een organisatie zal dus in de praktijk beschikken over twee nummerplannen: één voor IPv4 en één voor IPv6.

IPv4 en IPv6 hebben veel overeenkomsten. Er zijn echter ook enkele verschillen, die het opstellen van een IPv6-nummerplan net iets anders maken dan het opstellen van een IPv4-nummerplan.

Figuur 1 toont de structuur van een IPv6-adres. Een IPv6-adres bestaat uit 128 bits en heeft twee delen, te weten een prefix-deel (de eerste 64 bits) en een interface identifier (de laatste 64 bits). De interface identifier wordt gebruikt ter identificatie van een specifiek apparaat binnen een subnet. Het prefixdeel is opgesplitst in verschillende niveaus. De subnet-prefix identificeert een lokaal netwerk, de site-prefix identificeert bijvoorbeeld het netwerk van een organisatie en de LIR-prefix[8] identificeert het adresblok dat een LIR ter beschikking heeft om uit te delen aan andere organisaties, bijvoorbeeld klanten in geval de LIR een internetprovider is.

[5] Een voorgestelde ontwikkeling van het internet, waarbij allerhande voorwerpen zijn verbonden met het netwerk en gegevens kunnen uitwisselen. Voorbeelden hiervan zijn sensoren voor infrastructuurbewaking, vuilniscontainers of verkeerslichten.
[6] Volgens http://labs.apnic.net/ipv6-measurement, per 4 maart 2014
[7] Vanaf Windows Vista stelt Microsoft het gebruik van IPv6 verplicht en raadt af om IPv6 uit te zetten, omdat sommige Windowscomponenten dan mogelijk niet functioneren. Bron: http://support.microsoft.com/kb/929852/en-us
[8] LIR staat voor Local Internet Registry. Deze term wordt verder toegelicht in Paragraaf 2.5.



Figuur 1: Structuur van een IPv6-adres.

Deze structuur is iets anders dan voor IPv4, hetgeen de invloed heeft op nummerplannen.

Ieder IPv6-subnet is even groot
IPv6 werkt met een vaste subnet-omvang, namelijk 64 bits. Dit betekent dat ieder subnet in een IPv6-netwerk per definitie een prefix heeft van 64 bits en in theorie 2 tot de macht 64 apparaten in het subnet van adressen kan voorzien. Dit is anders dan in IPv4, waar subnetomvang wisselend kan zijn, binnen de 32 bits die IPv4 biedt.

Een IPv6-subnet is vele malen groter dan een IPv4-subnet
In een IPv6-subnet van 64 bits (/64) kan een enorm aantal apparaten van een uniek IP-adres worden voorzien, terwijl dit bij IPv4 beperkt is. Als in IPv4 bijvoorbeeld een /24 als subnet-omvang wordt gekozen dan kunnen hierbinnen 256 apparaten worden aangesloten. Als er meer apparaten moeten worden aangesloten, dan zal de subnet-omvang moeten worden aangepast, hetgeen meestal omnummeringen op andere plaatsen in het netwerk zal vergen. Een andere optie is om te gaan werken met adresvertaling, ofwel Network Address Translation (NAT).

NAT is als oplossing bedacht toen schaarste ontstond op publieke IP-adressen. NAT zorgt ervoor dat er meerdere private adressen achter één publiek adres worden geplaatst[9]. Een “vertaler” zet de privé adressen om naar een IP-adres dat op het publieke internet uniek herkenbaar is. Het nadeel van deze oplossing is dat deze vertalingen, maar ook de specifieke applicaties (poorten) moeten worden bijgehouden. Verder maakt het end-to-end communicatie en security moeilijker omdat aan de publieke kant niet bekend is welk device er precies is aangesloten (alleen het publieke IP-adres is bekend).

Bij IPv6 heeft het toevoegen van apparaten binnen een subnet geen impact op het nummerplan, omdat het enerzijds veel groter is en anderzijds een vaste omvang heeft. Het leidt daarom niet tot de noodzaak van een andere subnetindeling die de IPv6-adressen van apparaten in andere netwerken beïnvloedt. Bovendien is vanwege de grote adresruimte NAT bij IPv6 niet nodig.

[9] RFC1918

Er is meer ruimte voor het kiezen van netwerkprefixes
De omvang van IPv6-adresblokken die worden uitgedeeld aan organisaties is afhankelijk van het aantal apparaten dat door die organisatie is of wordt aangesloten. De standaard-omvang voor een gemiddelde locatie is /48, maar indien nodig kan een groter blok worden aangevraagd. Een /48 betekent dat 16 bits beschikbaar zijn om binnen die organisatie of locatie subnetten te maken, in totaal 65536 subnetten (het groene deel in Figuur 1). Omdat de subnetomvang vast staat (/64) kunnen deze subnetten volgens een bepaalde structuur worden ingedeeld, zodat netwerkbeheer overzichtelijk blijft. Hierbij is het van belang om de structuur (of: zonering) zo te kiezen, dat dit toekomstvast is, zodat veranderingen in het netwerk of de organisatie niet snel zullen leiden tot aanpassingen van de subnetindeling. Het opstellen van een IPv6-nummerplan binnen een enkele organisatie wordt nader beschreven in de handleiding[10] die SURFnet heeft gepubliceerd aangaande het opstellen van IPv6-nummerplannen.

De IPv6-adresruimte is vele malen groter
IPv4-adressen aanvragen bij RIPE NCC is nog maar in zeer beperkt mate mogelijk[11], omdat vrijwel alle IPv4-adressen al aan organisaties zijn toegewezen (al dan niet in gebruik). Wat betreft IPv6 is wereldwijd nog ruimte genoeg, en kun je als organisatie veel meer vanuit toekomstvastheid (lees: ruimte) denken, in plaats vanuit schaarste. Er is altijd de mogelijkheid om meer adressen aan te vragen bij RIPE NCC, mits je als organisatie voldoet aan de zogenaamde HD-ratio[12]. Deze ratio geeft aan dat een bepaald percentage van de toegewezen IPv6-prefixes daadwerkelijk in gebruik moet zijn binnen de organisatie voordat je nieuwe IPv6-adressen toegewezen kunt krijgen.

Beheer van twee nummerplannen
Een laatste aandachtspunt is dat sommige organisaties ervoor kiezen om het IPv6-nummerplan niet al te veel te laten afwijken van het IPv4-nummerplan, omdat beheerders anders voor twee netwerken met een andere netwerkstructuur moeten werken, hetgeen de kans op beheerfouten vergroot.[13]

2.3 De relatie met besloten netwerken

Niet alle apparaten en netwerken communiceren via Internet. Binnen de overheid wordt ook veelvuldig intern gecommuniceerd en gebruik gemaakt van diensten die niet via het internet bereikbaar zijn, denk daarbij bijvoorbeeld aan de diensten van basisregistraties.

In de analyse zullen we zien dat de mate waarin communicatie plaats vindt via een besloten overheidsnetwerk, van invloed is op de vraag of enerzijds (gezamenlijke) overheids-IPv6-adresblokken meerwaarde bieden en anderzijds of dit in de praktijk ook kan worden afgedwongen of gestimuleerd bij decentrale overheden.

---

[10] "Een IPv6-nummerplan opstellen: handleiding", SURFnet whitepaper, versie 2, 18 september 2013,
https://www.surf.nl/binaries/content/assets/surf/nl/kennisbank/2013/rapport_201309_IPv6_numplan_NL.pdf
[11] "RIPE-634: IPv4 Address Allocation and Assignment Policies for the RIPE NCC Service Region", maart 2015, https://www.ripe.net/ripe/docs/ripe-634
[12] "RIPE-641: IPv6 Address Allocation and Assignment Policy", maart 2015, https://www.ripe.net/ripe/docs/ripe-641
[13] GEN6 Deliverable 3.6, http://www.gen6-project.eu

2.4 Vanwaar de interesse voor IPv6-adresplannen bij overheden in het algemeen

Omdat verschillende Nederlandse overheidsorganisaties zich bezig houden met IPv6, de één in een wat verder stadium dan de ander[14], hebben ook verschillende overheidsorganisaties nagedacht over een IPv6-nummerplan voor hun organisatie. Op Rijksbreed niveau heeft Logius hier onderzoek naar gedaan en vanuit BZK is het onderzoek dat voor u ligt, aangaande overheidsbreed beleid, geïnitieerd.

Ook in het buitenland bestaat interesse voor overheidsbreed beleid op het gebied van IPv6-nummerplannen. In Europa loopt Duitsland voorop als het gaat om overheidsbrede afspraken aangaande IPv6. In Duitsland heeft men al in 2007 besloten dat men centraal IPv6-adresruimte ging aanvragen voor alle overheidsorganisaties in Duitsland. In 2009 is dit IPv6-adresblok daadwerkelijk toegewezen aan een centrale entiteit[15]. In navolging van Duitsland is ook Spanje[16] aan de slag gegaan met het voeren van nationaal IPv6-nummerplanbeleid en ook in Zwitserland[17] worden de mogelijkheden onderzocht. Deze landen gebruiken hierbij de aanpak van Duitsland als voorbeeld.

De interesse voor overheidsbreed IPv6-nummerplanbeleid volgt in Duitsland uit een breder strategisch doel om voor overheidscommunicatie minder afhankelijk te worden van leveranciers en met elkaar te communiceren over besloten netwerken. De introductie van IPv6 zien zij als een kans om negatieve ervaringen die zijn ontstaan bij IPv4, dat zonder enige coördinatie is ingevoerd, voor IPv6-netwerken te voorkómen. Deze ervaringen relateren aan beveiligingsincidenten, zoals het kapen van IP-reeksen van de overheid, hoge beheerlast bij het wijzigen van IP-configuraties, bijvoorbeeld ten gevolge van overstappen naar andere leveranciers of het samenvoegen en koppelen van overheidsnetwerken. Voor één van deelnemende gemeentelijke datacentra in Duitsland is met name het communiceren over besloten overheidsnetwerken een grote drijfveer voor het hebben van een centraal overheids-IPv6-adresblok, omdat hiermee routering op het besloten netwerk veilig en beheersbaar kan worden gehouden. In Spanje zijn overheidsorganisaties vanwege informatiebeveiligingsredenen verplicht om te koppelen met een besloten overheidsnetwerk. Dit betekent dat de introductie van IPv6 op dat besloten netwerk alle overheidsorganisaties raakt en dat er op nationaal niveau afspraken over moeten worden gemaakt.

De problemen met IPv4 zijn het gevolg van onder meer een gebrek aan overzichtelijkheid in welke systemen welke adressen gebruiken, het meervoudig in gebruik zijn van dezelfde IPv4-adressen op verschillende plaatsen binnen de

[14] IPv6-onderzoek onder Nederlandse overheden, “Marktrapportage Elektronische Communicatie Eerste halfjaar 2013”, TNO 2013 R12099

[15] Deutschland-Online Infrastruktur – IPv6 Reference Manual, T. Schaa, januari 2011, http://www.bva.bund.de/DE/Organisation/Abteilungen/Abteilung_BIT/Leistungen/IT_Beratungsleistungen/IPv6/best_practice/ipv6migrationsleitfaden/download/IPv6_Referenzhandbuch_2011_Version_KW45.html

[16] Dit hebben zij voor een groot deel uitgevoerd in het Europese project GEN6, http://www.gen6-project.eu

[17] Dit werd door Duitsland aangegeven in het interview dat in het kader van dit onderzoek is gehouden in februari 2015.

overheid en het niet hanteren van best-practices en standaarden voor de inrichting van IPv4-netwerken. In Nederland bestaan vergelijkbare ervaringen.[18]

Omdat IPv6 nog beperkt wordt gebruikt door overheden, ziet de overheid een kans door nu richtlijnen op te stellen, waarmee dergelijke problemen in de toekomst voor IPv6-netwerken en -diensten bij de overheid zoveel mogelijk worden voorkomen.

2.5 IP-adresuitgifteproces

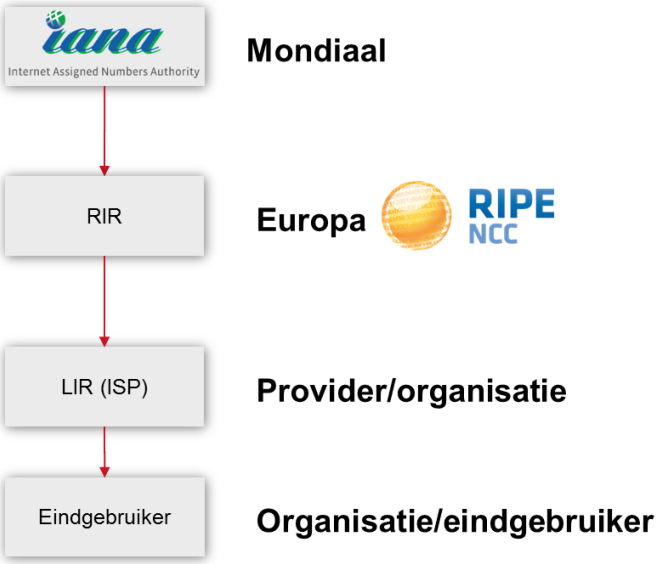
Communicatie via IP vereist dat systemen op Internet gebruik maken van IP-adressen die mondiaal uniek zijn. Om de uitgifte van IP-adressen te coördineren zijn vijf Regional Internet Registries (RIR) opgericht[19]. De RIR's staan onder toezicht van IANA (Internet Assigned Numbers Authority). Figuur 2 laat het bedieningsgebied van de vijf RIR's zien. In Europa worden IP-adressen uitgedeeld door RIPE NCC. De regels die hierbij worden gehanteerd worden opgesteld door de leden van RIPE[20].

Figuur 2: Overzicht van de vijf Regional Internet Registries (RIR) en het gebied dat zij bedienen[21].

RIPE NCC kent adresblokken toe aan haar leden, die adressen kunnen aanvragen en daarmee LIR (Local Internet Registries) worden. Een LIR is vaak een Internet Service Provider (ISP), maar kan ook een ander type bedrijf of een overheidsorganisatie zijn. Een LIR deelt IP adresreeksen uit aan eindgebruikers, die de adressen op individuele apparaten configureren. In sommige gevallen

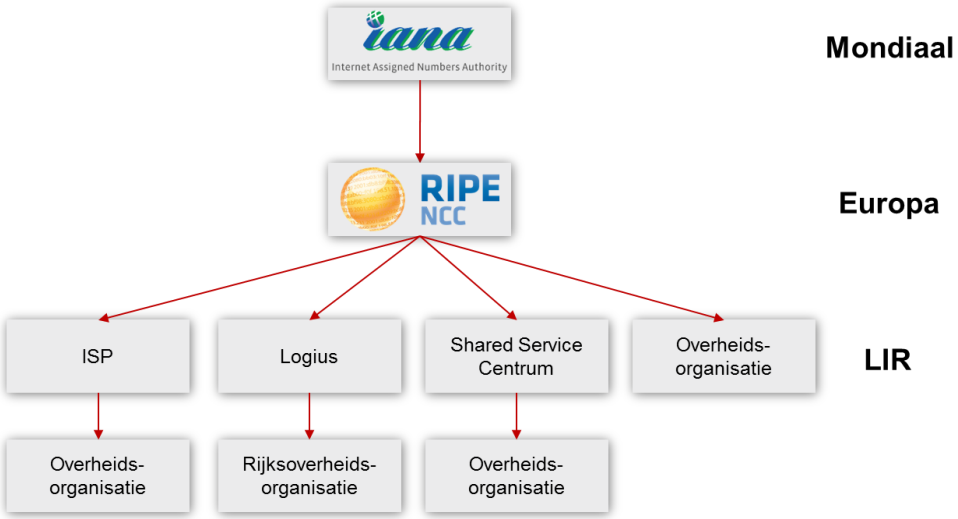
[18] Logius heeft aangegeven dat zij omnummeren onwenselijk vinden. Daarnaast gaven ook geraadpleegde leveranciers aan specifieke gevallen te kunnen benoemen waarbij dit problemen heeft gegeven. Zogaf één van hen aan dat gemeentes in sommige gevallen hun eigen conventies gebruiken, die in een enkel geval soms zelfs tegen de internationale afspraken over internetkoppelingen ingaan. Bijvoorbeeld het gebruik van-IP adressen, die door RIPE NCC aan een andere organisatie zijn toegekend.
[19] "The Internet Numbers Registry System", IETF RFC7020, R. Housley et al., August 2013, http://tools.ietf.org/html/rfc7020
[20] RIPE Policy Development, https://www.ripe.net/ripe/policies
[21] The Internet Registry System, bron: www.ripe.net,

bestaat er nog een tussenlaag (sub-LIR). Figuur 3 toont deze hiërarchische wijze van IP-adresuitgifte.



Figuur 3: IP adresuitgifte hiërarchie, van mondiaal niveau tot eindgebruikers in Europa. Een LIR is vaak een ISP, maar een organisatie kan ook zelf als LIR IP-adressen aanvragen, zonder dat ze daarvoor zelf ISP hoeft te zijn.

Nederlandse overheidsorganisaties kunnen op verschillende manieren hun IPv6-adressen krijgen uitgedeeld, zoals is weergegeven in Figuur 4. Hierin is te zien dat overheidsorganisaties hun IP adressen van een ISP kunnen krijgen, van een andere overheidsorganisatie die LIR is (bijvoorbeeld een ministerie of uitvoeringsorganisatie bij Logius, of een gemeente via een shared service centrum (SSC)), of dat zij zelf als LIR direct IP-adressen aanvragen bij RIPE NCC.



Figuur 4: Verschillende typen LIR-organisaties waarvandaan een overheidsorganisatie haar IP adressen toegewezen kan krijgen.

Het is essentieel op te merken dat de LIR-organisatie waarvandaan een overheidsorganisatie haar IP adressen ontvangt, niet altijd de organisatie hoeft te zijn die ook de verbinding naar internet voor de betreffende overheidsorganisatie levert. Zo kan een overheidsorganisatie die zelf LIR is gebruik maken van een externe ISP om de internetverbinding te realiseren.

3 Wensen en randvoorwaarden overheidsbreed IPv6-nummerplankader

In de onderzoeksvragen, zoals beschreven in Paragraaf 1.1, is vanuit het Ministerie van BZK aangeven dat overheidsbreed IPv6-beleid mogelijk kan leiden tot potentiële voordelen op het gebied van leveranciersonafhankelijkheid, informatiebeveiliging, financiën en mogelijke overige baten. Bij aanvang van het project zijn deze door de overheid beoogde voordelen door het onderzoeksteam nader uitgewerkt tot een set criteria en randvoorwaarden, waarvan de prioriteit is vastgesteld[22] tijdens de eerste workshop van het onderzoek op 9 december 2014 met de vertegenwoordigers in de begeleidingscommissie. Tijdens deze workshop heeft de begeleidingscommissie de gelegenheid gehad om nieuwe wensen en criteria aan te dragen.

De criteria en randvoorwaarden worden meegenomen in de analyse in Hoofdstuk 4 en het IPv6-nummerplankader in Hoofdstuk 5. In dit hoofdstuk worden de wensen, criteria en hun belang beschreven per categorie: leveranciersonafhankelijkheid (Paragraaf 3.1), informatieveiligheid (Paragraaf 3.2), financieel voordeel (Paragraaf 3.3) en overige baten en randvoorwaarden (Paragraaf 3.4). Daarbij wordt het belang dat de begeleidingscommissie aan deze onderwerpen hecht weergegeven.

3.1 Leveranciersonafhankelijkheid

Leveranciersonafhankelijkheid wordt door de begeleidingscommissie gezien als een belangrijke drijfveer voor het opstellen van een overheidsbreed IPv6-nummerplankader. De begeleidingscommissie acht de volgende aspecten van groot belang als het gaat om het verhogen van deze leveranciersonafhankelijkheid[23]:

- Alle overheidsdiensten maken gebruik van IPv6-adressen die ‘eigendom’[24] van de overheid zijn.
- Bij het overstappen naar een andere leverancier moet omnummeren (zoveel mogelijk) voorkomen worden.

Het idee daarbij is dat het moeten omnummeren van IPv6-adressen bij een leveranciersoverstap een drempel opwerpt voor overheidsorganisaties om over te stappen naar een andere leverancier.

Daarbij zijn ook enkele belangrijke voorwaarden genoemd:

- Van alle IPv6-configuraties van overheidsdiensten en -netwerken, ook die door leveranciers worden geleverd, moet bij voorkeur toetsbaar zijn of wordt voldaan

[22] De criteria en randvoorwaarden konden door de leden van de begeleidingscommissie worden geclassificeerd als *randvoorwaarde*, *heel erg belangrijk*, *belangrijk*, *niet belangrijk*, *weet niet* of *geen mening*.

[23] Het betreft hier leveranciers van ICT-diensten aan de overheid, waar IP-adressen onderdeel van uitmaken.

[24] Hier wordt mee bedoeld dat de betreffende IPv6 adressen onderdeel uitmaken van een adresblok dat door RIPE NCC is toegewezen aan een LIR binnen de overheid. Volgens het beleid van RIPE NCC worden IP-adressen nooit officieel eigendom van een LIR.

aan het afgesproken IPv6-nummerplankader. Bijvoorbeeld het nagaan of overheidsadressen daadwerkelijk gebruikt door een bepaalde leverancier.
- De eisen die vanuit het nummerplanbeleid worden gesteld aan netwerken en diensten worden door (zo goed als) alle marktpartijen ondersteund.

Deze laatste voorwaarde richt zich op het aspect dat een zo groot mogelijk leveranciersaanbod bijdraagt aan leveranciersonafhankelijkheid. Ook bij invoering van een overheidsbreed IPv6-nummerplankader is de wens dat het aanbod van leveranciers voor overheidsorganisaties voldoende groot is.

3.2 Informatieveiligheid

De begeleidingscommissie heeft aangegeven dat zij bij het maken van afspraken tussen overheden aangaande IPv6-nummerplannen kansen ziet op het gebied van informatieveiligheid van overheidsorganisaties.

Hierbij wordt belang toegekend aan de volgende aspecten:

- Monitoring en configuratie ten bate van informatiebeveiliging wordt bevorderd als inzichtelijk is welke IPv6-adressen waar binnen de overheid in gebruik zijn. Niet-toegestane verkeerstromen kunnen eenvoudiger worden gedetecteerd en er kan mogelijk sneller worden gereageerd op incidenten. Een overheidsbreed IPv6-nummerplankader kan hier mogelijk aan bijdragen.
- Het opstellen van voorschriften voor individuele overheden aangaande het reserveren van adresreeksen voor beveiliging (zonering) binnen het aan die overheid toegewezen adresblok kan veiliger koppelen van diverse overheidsnetwerken mogelijk maken.

Naast voordelen van gezamenlijke afstemming van IPv6-nummerplannen binnen de overheid, zijn er ook enkele erg belangrijk geachte beveiligingsaspecten benoemd op het niveau van individuele IPv6-nummerplannen van overheidsorganisaties:

- Beveiligingsrisico's zijn lager, want door het voorkomen van omnummeracties is er een kleinere kans op configuratiefouten tijdens deze acties.
- IPv6-nummerplannen zouden zo moeten worden ingericht dat het toevoegen van een nieuw apparaat (PC, server, router) mogelijk is zonder aanpassingen in de actieve IPv6-gerelateerde beveiligingsconfiguratie.

Daarnaast wordt meer algemeen opgemerkt dat het hebben van een IPv6-nummerplan op zichzelf voor iedere overheidsorganisatie een belangrijk instrument is om een ICT-omgeving beheerbaar en veilig in te richten.

3.3 Financieel voordeel

De opdrachtgever vraagt zich af of er, door gezamenlijke afspraken te maken of gezamenlijk bepaalde activiteiten op te pakken, mogelijk financiële voordelen te behalen zijn voor de overheid. De begeleidingscommissie heeft aangegeven dat zij dit belangrijk vindt, maar veel minder belangrijk dan het vergroten van leveranciersonafhankelijkheid en het bijdragen aan informatieveiligheid.

Kansen voor eventueel financieel voordeel zouden kunnen liggen op de volgende punten:

- Een gezamenlijk lidmaatschap bij RIPE NCC brengt minder jaarlijkse lidmaatschapskosten met zich mee dan vele lidmaatschappen bij RIPE NCC van individuele overheden.
- Mensinzet ten bate van onderhoud en uitvoering van gezamenlijk IPv6-nummerplanbeleid, onder andere beheer van adressen en het op peil krijgen en houden van kennis van personeel aangaande IPv6-nummerplannen, zou minder kosten met zich mee brengen als bepaalde aspecten gezamenlijk worden opgepakt of als er richtlijnen zouden bestaan.

Naast kostenvoordelen heeft de begeleidingscommissie aangegeven dat zij de eenmalige kosten ten aanzien van de introductie van het IPv6-nummerplanbeleid, zoals opleidingskosten, aanschaf IP-adresmanagementsystemen en de kosten voor omnummeren van partijen die al een IPv6-nummerplan hadden, een zeer belangrijk aspect vinden, omdat zij hier de hoogste extra kosten verwachten, mocht er een overheidsbreed IPv6-nummerplankader worden opgesteld.

Eventuele overige extra kosten, bijvoorbeeld vanwege het risico dat leveranciers vanwege het IPv6-nummerplankader hun kosten voor het conformeren eraan zullen doorberekenen, worden laag ingeschat door de begeleidingscommissie.

3.4 Randvoorwaarden en overige baten

Naast bovenstaande categorieën van potentiële voordelen zijn tijdens het onderzoek nog enkele andere mogelijke baten en randvoorwaarden naar voren gekomen die in deze paragraaf worden genoemd:

- Het behoud van de autonomie van overheidsorganisaties ten aanzien van beslissingen over hun ICT-bedrijfsvoering.
- De begeleidingscommissie heeft de voorkeur om geen omvangrijke toetsingsprocedures of strikte handhaving in te richten voor een nummerplankader.
- De positionering van het IPv6-nummerplankader in de algemene ICT-bedrijfsvoering en -inrichting binnen de overheid. Specifiek moet het kader aansluiten bij de doelstellingen van de Digicommissaris en de Generieke Digitale Infrastructuur (GDI)[25].

Omdat IPv6 bij veel overheden nog niet is geïntroduceerd is er voor het grootste deel een green-field-situatie aangaande IPv6-nummerplannen bij de overheid. Deze situatie is een kans die de overheid kan benutten om ICT-netwerken toekomstvast in te richten. Hierbij hecht de begeleidingscommissie belang aan de volgende punten:

- Een bestuurlijke aanpassing (zoals een gemeentelijke herindeling), het ontstaan van nieuwe Shared Service Centra, en het aansluiten van grote hoeveelheden sensoren en andere apparaten (voor bijvoorbeeld *Internet of Things*-toepassingen), moeten een zo beperkt mogelijke impact hebben op het

[25] Generieke Digitale Infrastructuur van de overheid, http://www.digicommissaris.nl/thema/generieke-digitale-infrastructuur-gdi

overheidsbreed IPv6-nummerplankader en de IPv6-nummerplannen van individuele overheidsorganisaties.
- Het IPv6-nummerplankader moet eraan bijdragen dat IPv6-adressen niet dubbel in gebruik zijn binnen de overheid om het koppelen en samenvoegen van netwerken niet complexer dan nodig te maken.

Nederlandse overheidsorganisaties kennen een grote autonomie. Zij zijn zelf verantwoordelijk voor bijvoorbeeld aanbestedingen, contracten met leveranciers, en de inrichting van hun ICT-omgeving. De begeleidingscommissie acht het van zeer groot belang dat de afspraken in een overheidsbreed IPv6-nummerplankader de bestuurlijke autonomie van overheden niet beperken maar juist ondersteunen. Ten opzichte van de andere criteria benoemd in dit hoofdstuk werd aan dit criterium unaniem het meest belang gehecht door de leden van de begeleidingscommissie.

3.5 Conclusies

Uit de prioritering door de begeleidingscommissie blijkt dat men bestuurlijke autonomie het belangrijkste criterium vindt. Aan deze randvoorwaarde moet absoluut voldaan worden als een overheidsbreed IPv6-nummerplankader wordt opgesteld. Een overheidsbreed IPv6-nummerplankader moet juist ondersteunend zijn voor overheidsorganisaties.

Ook is als randvoorwaarde aangegeven dat elke overheidsorganisatie in ieder geval een IPv6-nummerplan dient te hebben[26], onder andere als instrument voor informatieveiligheid.

Daarnaast wordt door de deelnemers veel belang gehecht aan leveranciersonafhankelijkheid. Met name het niet meer hoeven omnummeren en het daaraan gerelateerd gebruik van overheids-IPv6-adressen in overheidsdiensten werd door een paar leden van de begeleidingscommissie als bijna randvoorwaardelijk beoordeeld.

Op het gebied van beveiliging wordt belang gehecht aan overzichtelijkheid van adressen voor monitoring. Dit wordt echter vooral als ‘kritiek’ beoordeeld en niet als randvoorwaarde.

Van belang wordt ook gezien dat het IPv6-nummerplankader toekomstvast is ten aanzien van bestuurlijke veranderingen. Daarbij wordt gedacht aan het ontstaan van shared service centers of in mindere mate eventuele bestuurlijke herindelingen van departementen of overheden. Bestuurlijke of organisatorische veranderingen moeten zo min mogelijk impact hebben op de IPv6-nummerplannen van de betreffende organisaties.

[26] Voor kleinere, individuele overheidsorganisaties volstaat ook dat er een andere overheidsorganisatie is die over een IPv6-nummerplan beschikt dat alle IPv6-adressen van de betreffende organisatie afdekt. Die andere overheidsorganisatie kan bijvoorbeeld een Shared Service Centrum zijn of een centrale LIR, zolang het IPv6-nummerplan maar alle IPv6-adressen omvat.

4 Analyse

Dit hoofdstuk beschrijft de analyse ter beantwoording van de hoofdonderzoeksvraag:

In hoeverre en onder welke voorwaarden is te verwachten dat een IPv6-nummerplan voor de hele Nederlandse Overheid tot kansen voor leveranciersonafhankelijkheid, informatieveiligheid, financieel voordeel en overige baten zal leiden?

Dit hoofdstuk beschrijft de analyse per onderwerp waaruit volgt in hoeverre en onder welke omstandigheden een gezamenlijk nummerplankader daar aan kan bijdragen:

- leveranciersonafhankelijkheid (Paragraaf 4.1);
- informatieveiligheid (Paragraaf 4.2);
- financieel voordeel (Paragraaf 4.3);
- overige baten en randvoorwaarden (Paragraaf 4.4).

4.1 Leveranciersonafhankelijkheid

4.1.1 Analyse

Uit de workshops met de begeleidingscommissie en gesprekken met de geraadpleegde stakeholders blijkt dat leveranciersonafhankelijkheid raakt aan twee aspecten:

- enerzijds relateert dit aan het eenvoudig kunnen overstappen van de ene naar de andere leverancier (voorkomen van vendor-lock-in);
- anderzijds kan een overheid vanwege informatieveiligheidsredenen onafhankelijk van een leverancier willen zijn.

Het eerste punt wordt in deze paragraaf verder uitgewerkt. Het tweede aspect wordt beschouwd in Paragraaf 4.2 als onderdeel van de analyse met betrekking tot informatieveiligheid.

Bij leveranciersonafhankelijkheid is de kern dat overheidsorganisaties zo eenvoudig mogelijk willen en kunnen overstappen naar een andere leverancier voor hun diensten en verbindingen, bijvoorbeeld omdat een andere leverancier een beter passend pakket aanbiedt of betere kwaliteit levert. Om een dergelijke overstap niet te hinderen is het van belang dat overstappen zo min mogelijk extra kosten met zich meebrengt, maar ook zo weinig mogelijk werk oplevert voor de overheidsorganisatie. Leveranciersonafhankelijkheid hangt samen met verschillende zaken zoals contractuele afspraken die er bestaan tussen overheid en leverancier, het aanbod in de markt en de prijs van verschillende leveranciers.

Een aspect dat kosten en mogelijk extra werk kan opleveren is het herconfigureren, of *omnummeren*, van IP-adressen op het moment dat van leverancier wordt veranderd en dit gepaard gaat met het overstappen naar een andere IP-adresreeks, die bij de nieuwe leverancier hoort. Deze situatie is weergegeven in Figuur 5. Dit omnummeren geldt zowel voor IPv4 als voor IPv6. Een IPv6-

nummerplankader zou kunnen bijdragen aan leveranciersonafhankelijkheid als dankzij het kader het omnummeren van IPv6-adressen eenvoudiger wordt of kan worden voorkomen.

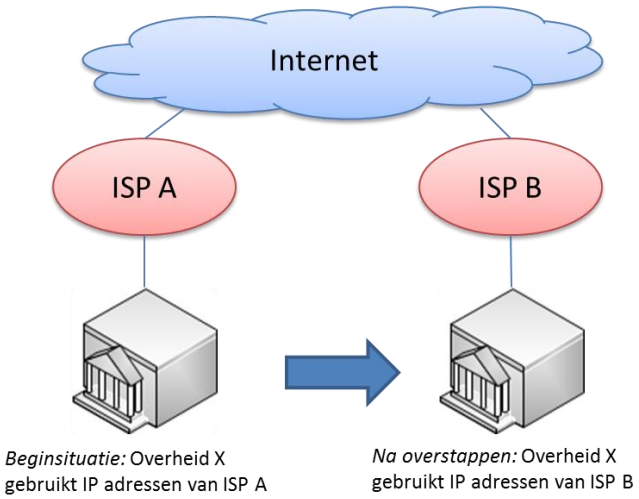
Een ander aspect dat naar voren kwam in de analyse[27] is het feit dat een overheidsorganisatie die vanwege beschikbaarheid aangesloten wil worden via twee leveranciers (dual-homed), dit het beste kan doen als de organisatie over eigen IP-adressen beschikt, die dan door beide internetproviders bereikbaar worden gemaakt. Immers, leveranciers staan over het algemeen niet toe dat hun IP-reeksen door andere ISP's op internet geadverteerd worden. Met dual-homing wordt een overheidsorganisatie onafhankelijker van één enkele leverancier als het gaat om beschikbaarheid van haar internetverbinding. Bijvoorbeeld in geval er een Denial of Service (DOS) aanval wordt uitgevoerd op één van de internetverbindingen van een dienst, dan kan de dienst via de andere verbinding bereikbaar blijven.

> Het aansluiten van een overheidsorganisatie op Internet via twee of meerdere internetproviders vereist dat de overheidsorganisatie beschikt over eigen IP-adressen.

De hypothese van leveranciersonafhankelijkheid wat betreft omnummeren kan worden aangescherpt tot de volgende twee uitspraken, waarbij we het gebruik van IPv6-adressen van de leverancier vergelijken met het gebruik van eigen IPv6-adressen van de overheid:

- "Omnummeren werpt een drempel op voor overheden om over te stappen naar een andere leverancier."
- "Als ik mijn eigen IPv6-adressen gebruik, dan hoef ik niet meer om te nummeren als gevolg van een wisseling van leverancier."

[27] Dit werd aangegeven/bevestigd door BT en SURFnet.



Figuur 5: Overheid X gebruikt IP-adressen van leverancier A en stapt over naar leverancier B. Nu moeten overheid X de IP-adressen op al haar apparaten vervangen door de adressen van Leverancier B.

Er zijn verschillende aanleidingen waardoor het herconfigureren van IP-adressen op apparaten nodig is:

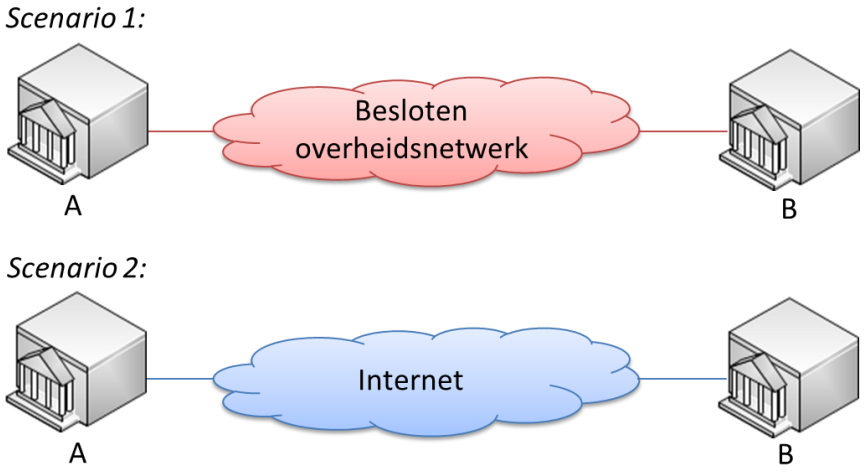
1. De netwerkprefix die in het netwerk wordt gebruikt verandert.
2. De subnetindeling, die in het netwerk van toepassing is, verandert.

Een wijziging in de subnetindeling kan worden veroorzaakt door een wijziging in het nummerplan van een organisatie. Stel dat een subnet is toegewezen aan een deelorganisatie en die deelorganisatie verdwijnt, wordt opgesplitst of samengevoegd, dan kan dit aanleiding zijn om de subnetindeling aan te passen, hetgeen leidt tot het moeten herconfigureren van IP-adressen. Een andere reden waardoor de subnetindeling kan wijzigen is dat er meer apparaten moeten worden aangesloten dan dat er ruimte is in het subnet. In dat geval moet een subnet groter gemaakt worden. Dit laatste speelt alleen in IPv4-netwerken en niet meer bij IPv6, omdat daar voldoende ruimte in een subnet beschikbaar is en ieder subnet bovendien een vaste omvang heeft (/64).

> Binnen een organisatie kan omnummeren van IPv6-adressen worden beperkt door de subnetindeling zo te kiezen dat deze zo veel mogelijk onafhankelijk is van veranderlijke zaken, zoals organisatorische wijzigingen.

Een wijziging in de netwerkprefix wordt in de regel veroorzaakt door een leverancierswissel waarbij in de overheidsorganisatie voor de geleverde dienst gebruik gemaakt wordt van IP-adressen van de leverancier. Om een indruk te krijgen van de omvang van dergelijke omnummeracties beschrijven we hier verschillende situaties en de bijbehorende omnummeractiviteiten. Deze situaties beschrijven we aan de hand van twee scenario's, die zijn weergegeven in Figuur 6:

1. Twee overheidslocaties die zijn verbonden via een besloten netwerk;
2. Twee overheidslocaties die zijn verbonden via internet.



Figuur 6: De twee scenario's aan de hand waarvan verschillende omnummersituaties worden beschreven. Een 'overheidslocatie' (A en B) kan op verschillende manieren worden ingevuld. Het kan bijvoorbeeld een datacenter zijn, maar ook een kantoornetwerk.

De scenario's beschouwen we hier vanuit een client-server perspectief: overheidslocatie A zet een communicatiesessie op naar overheidslocatie B, bijvoorbeeld om bepaalde gegevens uit een overheidsregistratiesysteem op te halen. Locatie A en locatie B gebruiken een andere niet-overlappende IP-netwerkprefix. We beschrijven voor deze scenario's de omnummeractiviteiten die moeten plaatsvinden als B (de server-zijde) van IP-netwerkprefix wisselt en als A (de client-zijde) van IP-netwerkprefix wisselt. De acties zijn weergegeven in een overzicht in Tabel 3. Merk op dat de rollen van A en B ook omgedraaid kunnen zijn. RFC4192[28] en RFC5889[29] beschrijven uitgebreider de stappen en uitdagingen die komen kijken bij het omnummeren van een IPv6-gebaseerde ICT-omgeving van een organisatie.

De redenen waarom client (A) en server (B) van netwerkprefix kunnen wisselen zijn:

- Services worden op een andere plek (andere leverancier) gehost of dienstleverancier wisselt van connectiviteitprovider (bijvoorbeeld de Basisregistratie Personen (BPR) wordt door een andere leverancier gehost);
- De connectivityprovider naar internet wijzigt (bijvoorbeeld overstappen van Tele2 naar KPN);
- De connectivityprovider richting het besloten netwerk wijzigt (bijvoorbeeld overstappen van of naar GEMNET).

[28] "RFC4192 - Procedures for Renumbering an IPv6 Network without a Flag Day", F. Baker et al, september 2005, IETF, https://tools.ietf.org/html/rfc4192

[29] "RFC5889 - Renumbering Still Needs Work", B. Carpenter et al., mei 2010, IETF, https://tools.ietf.org/html/rfc5887

Tabel 3: Overzicht van benodigde omnummeractiviteiten bij een leveranciersoverstap die een netwerkprefixwijziging vereist.

	Benodigde omnummeractiviteiten indien:	
	Client (A) verandert netwerkprefix	**Server (B) verandert netwerkprefix**
Scenario 1: A communiceert met B via besloten overheidsnetwerk	• B moet alle toegangsregels (firewall, filters) op basis van de adressen van A aanpassen. • Routes en toegangsregels naar A in het besloten netwerk moeten worden aangepast. • A moet de IP-adressen op alle besloten-netwerkgerichte apparaten in haar eigen netwerk aanpassen.	• Nieuw adres moet voor A zichtbaar worden in de besloten DNS.[30] • A moet eventuele hardgecodeerde IP-adressen van B in haar systemen wijzigen. • Routes en toegangsregels naar B in het besloten netwerk moeten worden aangepast. • B moet de IP-adressen op alle apparaten in het eigen netwerk aanpassen.
Scenario 2: A communiceert met B via Internet	• B moet toegangsregels op basis van de adressen van A aanpassen. • A moet de IP-adressen op alle internet-gerichte apparaten in haar eigen netwerk aanpassen.	• Nieuw adres moet voor A zichtbaar worden in de Internet DNS. • A moet eventuele hardgecodeerde IP-adressen van B in haar systemen wijzigen. • B moet de IP-adressen op alle apparaten in het eigen netwerk aanpassen.

De benodigde acties die zijn genoemd in Tabel 3 schalen met het aantal verbindingen dat tussen overheidslocaties bestaat en het aantal plekken waar IP-adressen of -prefixen worden gebruikt in de dienst- of netwerkconfiguratie. Stel dat er tien diensten zijn die toegangsregels op basis van de IP-prefix van overheid X instellen, dan moeten al die tien diensten hun configuratie aanpassen indien overheid X andere IP-adressen gaat gebruiken.

[30] (Web)servers worden in de regel bekendgemaakt op een netwerk via een naam (URL), die gebruikt kan worden door gebruikers of systemen om een server of dienst aan te duiden (bijvoorbeeld www.rijksoverheid..nl). Om de server te kunnen bereiken wordt een IP-adres gekoppeld aan deze naam in het Domain Name System (DNS), zodat de systemen daadwerkelijk via IP kunnen communiceren. Voor diensten die over een besloten netwerk worden benaderd kan worden gekozen een DNS in te richten die alleen op het besloten netwerk beschikbaar is.

Omnummeren van diensten en netwerken waarvoor door veel andere overheden/diensten filter-regels of verwijzingen naar IP-adressen zijn opgenomen, introduceren grote omnummer-impact.

Het hebben van een eigen overheidsprefix en het gebruik hiervan in alle netwerken en diensten leidt er toe dat de hierbovengenoemde omnummeractiviteiten niet meer hoeven worden uitgevoerd ten gevolge van een leverancierswissel. Immers, overheidslocatie A en B veranderen nooit van adressen.

Kostenmodel voor omnummeren als gevolg van een leverancierswissel
In deze paragraaf introduceren we een kostenmodel om inzichtelijk te maken in hoeverre omnummerkosten een *overstapdrempel* vormen.

Vanuit kostenperspectief zal een individuele overheidsorganisatie overstappen naar een andere leverancier als deze een financieel interessanter aanbod doet dan de huidige leverancier. De kosten voor de impact van de overstap mogen niet zo hoog zijn dat het kostenvoordeel verdwijnt. Omnummerkosten houden, bij gelijkblijvend niveau van dienstverlening van de nieuwe leverancier ten opzichte van de huidige, een leveranciersoverstap tegen, indien:

$$K_{aanbod\_huidige\_leverancier} < \left(K_{aanbod\_nieuwe\_leverancier} + K_{omnummeren} + K_{overstap\_overig}\right) \quad (1)$$

waarbij K de kosten zijn en < kleiner dan betekent.

Hierbij kijkt een organisatie alleen naar haar eigen kosten. Echter, omnummeren kan ook impact hebben op andere organisaties, zoals beschreven staat in Tabel 3, en die worden hierin niet meegenomen. Als dit wel wordt meegenomen, dan kost een leverancierswissel geld indien:

$$K_{aanbod\_huidige\_leverancier} < K_{aanbod\_nieuwe\_leverancier} + \sum_{n=1}^{N} K_{omnummeren,n} + K_{overstap\_overig} \quad (2)$$

waarbij K de kosten zijn en N het aantal overheidsorganisaties is dat omnummeracties moet uitvoeren vanwege die leverancierswissel en het sigma-teken de sommatie voorstelt van deze kosten over alle N organisaties. Echter, de kosten die door anderen worden gemaakt zijn voor een individuele organisatie meestal slecht zichtbaar. Merk hierbij op dat je dit aan alle partijen die een koppeling hebben moet gaan uitleggen[31].

[31] Ervaring Logius: het imago van een dienst kan achteruit gaan als gebruikers regelmatig moeten omnummeren, bijvoorbeeld vanwege een leveranciersoverstap van die dienst.

Niet hoeven omnummeren bij een leverancierswissel levert een kostenvoordeel op. Er spelen echter nog andere afwegingen die een rol bij een mogelijke leveranciersoverstap.

Meerdere geraadpleegde stakeholders (Logius, Centric, Spanje, Duitsland, SSC Zwolle, BT en Heerlen) zien in meer of mindere mate het voordeel van niet hoeven omnummeren en het hebben van eigen IP-adressen ten bate van leveranciersonafhankelijkheid.

Eén of meerdere overheidsadresblokken
Maakt het dan nog uit of er één groot overheidsadresblok wordt gebruikt, of dat iedere overheidsorganisatie zelf een eigen adresblok heeft, of een tussenvariant hiervan, bijvoorbeeld een blok per overheidssector? Zolang de netwerkprefix maar gelijk blijft hoeft er niet te worden omgenummerd vanwege een leveranciersoverstap, ongeacht of deze prefixen uit één groot blok komen of niet.

Het gebruik van een eigen overheidsnetwerkprefix kan omnummeractiviteiten ten gevolge van een leverancierswissel voorkomen. Het maakt hierbij niet of deze netwerkprefixes uit één groot overheidsadresblok komen of uit meerdere kleine blokken. Andere aanleidingen voor omnummeren zullen blijven bestaan.

Hierbij dient te worden opgemerkt dat iedere overheidsprefix die wordt gebruik voor koppelingen tussen overheden en/of overheidsdiensten in de netwerkconfiguratie moet worden opgenomen. Dit betekent dat het aantal regels in routetabellen en firewalls toeneemt naarmate er meer verschillende (kleinere) overheidsprefixen in gebruik zijn. Hierbij wordt aangenomen dat een aaneengesloten adresblok zoveel mogelijk geaggregeerd wordt.

Het gebruik van meerdere overheidsadresblokken leidt tot toename van het aantal regels in routers en firewalls op verbindingen tussen overheden, wat het beheer ervan minder overzichtelijk maakt.

4.1.2 Conclusie

Een IPv6-nummerplankader kan in de eerste plaats bijdragen aan het vergroten van leveranciersonafhankelijkheid door de drempel te verlagen voor een leverancierswissel in situaties waarbij, zonder kader, het omnummeren van IPv6-adressen kostbaar zou zijn geweest. Dit geld met name voor diensten en koppelingen waar veel overheidsorganisaties bij betrokken zijn. Door het in beheer

hebben van eigen IPv6-adressen kan de noodzaak voor omnummeren vanwege een leverancierswissel worden voorkomen.

In de praktijk spelen bij een leveranciersoverstap ook andere zaken een rol. Zo werpt bijvoorbeeld het omnummeren van IPv4 bij een leverancierswissel op dit moment een veel grotere drempel op, omdat IPv6 nog maar beperkt in gebruik is. Verder speelt mee hoe zwaar de redenen om over te stappen naar een andere leverancier wegen ten opzichte van de omnummerkosten. Een overheidsbreed IPv6-nummerplankader verandert daar niets in.

In de tweede plaats kan leveranciersonafhankelijkheid worden vergroot, omdat het in eigen beheer hebben van IP adressen het mogelijk maakt om via meerdere internetproviders aangesloten te worden op internet (dual homed). Een netwerk of dienst wordt vaak dual-homed aangesloten om de beschikbaarheid te verhogen, om bereikbaarheid te behouden ingeval van een technische storing of een cyberaanval.

4.2 Informatieveiligheid

4.2.1 Analyse

IP-adressen kunnen worden toegepast om te kunnen bepalen waar een apparaat zich op een netwerk bevindt. Daarnaast kan aan de hand van IP-adressen of netwerkreeksen tot op zekere hoogte worden vastgesteld wie of welke organisatie deze adressen gebruikt. Om deze redenen spelen IP-adressen een belangrijke rol als het gaat om informatieveiligheid. Vanwege de focus van dit onderzoek op IPv6 beperken we de analyse hier tot informatieveiligheid in relatie tot een overheidsbreed IPv6-nummerplankader. Het inrichten van een veilige ICT-omgeving vergt uiteraard ook toepassing van andere maatregelen ten behoeve van informatiebeveiliging, zoals beveiliging op applicatieniveau.

Afspraken die worden gemaakt in een overheidsbreed IPv6-nummerplankader kunnen invloed hebben op welke IPv6-adressen waar en door wie binnen de overheid worden gebruikt. De onderzoeksvraag is of er door dergelijke afspraken veiligheidsvoordelen behaald kunnen worden, of dat bepaalde afspraken juist beveiligingsrisico's met zich mee kunnen brengen. Wat betreft de mogelijke voordelen worden de volgende aspecten beschouwd:

- lagere kans op misbruik van overheids-IP-adressen op internet;
- verminderde kans op configuratiefouten;
- eenvoudiger koppelen van (vertrouwelijke) netwerken;
- monitoring ten behoeve van veiligheidsincidenten en snelle incident response tijd;

Het eerste aspect hangt samen met verschillende incidenten die zich hebben voorgedaan op internet, waarbij een land of organisatie, al dan niet bewust, bepaalde IP reeksen 'kaapt', die aan iemand anders zijn toegewezen. Een bekend voorbeeld hiervan is een incident waarbij Pakistan Telecom in 2008 korte tijd al het dataverkeer van Youtube naar zich toetrok[32]. Dit incident kon plaatsvinden, omdat

[32] YouTube Hijacking: A RIPE NCC RIS case study, https://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study

de betreffende provider onrechtmatig de IP-adressen van Youtube adverteerde, waardoor andere routers op internet het verkeer naar Pakistan Telecom stuurden in plaats van naar Youtube. Een andere mogelijkheid is dat kwaadwillenden ongebruikte IP-adressen van een organisatie inzet om bijvoorbeeld spam te versturen. Ontvangers zullen dan in eerste instantie denken dat deze spam van de betreffende organisatie komt, terwijl dit niet het geval is.

Het kapen van IP-reeksen op internet heeft geleid tot het ontwikkelen van een beveiligingsmechanisme[33], waarbij eigenaren van IP-prefixen een certificaat kunnen aanmaken waarin staat aangegeven welke netwerken deze IP-prefixen rechtmatig mogen gebruiken. Routers op internet kunnen hiermee detecteren als een IP-reeks onrechtmatig door een bepaald netwerk wordt geadverteerd. Hierop kunnen zij dan actie ondernemen, bijvoorbeeld door het verkeer daar niet heen te sturen.

De relevantie voor het nummerplankader komt naar voren als we beschouwen dat het opstellen van een dergelijk certificaat alleen gedaan kan worden door de partij die de IP-reeks toegekend heeft gekregen van RIPE NCC. In het geval dat een overheidsorganisatie gebruik maakt van IP adressen van een tussenleverancier, dan is zij ook afhankelijk van deze leverancier als het gaat om het ondertekenen van de certificaten. Indien een organisatie niet op een tussenleverancier wil of kan vertrouwen, bijvoorbeeld door verschillende belangen, dan zal de organisatie zelf de IP adressen bij RIPE NCC aan moeten vragen. Dit houdt ook in dat de uitgifte en het beheer van de certificaten door de organisatie zelf moeten worden geregeld.

Voor de Duitse federale overheid is deze directe controle een belangrijk argument om te kiezen voor een eigen overheidsbrede IPv6-adresreeks. Dit volgt uit een meer strategische keuze die zij hebben gemaakt aangaande informatiebeveiliging bij de overheid. Daarnaast geldt in Duitsland bijvoorbeeld ook de verplichting dat federale overheden en staten in Duitsland onderling altijd via een besloten overheidsnetwerk moeten communiceren. De afweging hoe zwaar dit argument van misbruik van IP-reeksen voor de Nederlandse overheid weegt, hangt af meer strategische keuzes die de overheid maakt in bredere beveiligingscontext van de overheids-ICT, aangaande wat zij wel en niet aan commerciële leveranciers wil overlaten.

> Met overheidseigenadressen kan de overheid zelf certificering van haar IP-reeksen op Internet uitvoeren in plaats van dat dit door een leverancier moet worden gedaan. Het belang dat de Nederlandse overheid hier aan hecht zal in bredere ICT-beveiligingscontext moeten worden afgewogen.

De andere genoemde aspecten hebben, wat betreft een IPv6-nummerplankader, voor een belangrijk deel te maken met het aanbrengen van structuur in de gebruikte IP-adressen binnen de overheid. Hierbij gaat het enerzijds om het aanbrengen van

[33] BGP origin validation, https://www.ripe.net/lir-services/resource-management/certification/bgp-origin-validation

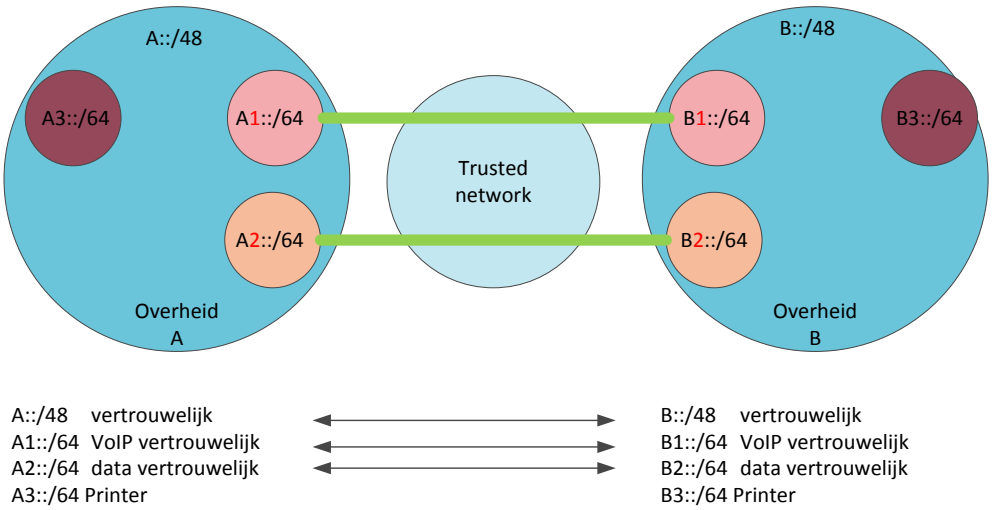
structuur in het nummerplan van een specifieke overheidsorganisatie en anderzijds om het aanbrengen van structuur in het gebruik van IPv6-adressen overheidsbreed.

Het aanbrengen van structuur in een IPv6-nummerplan kan worden gedaan door apparaten en netwerken die voor eenzelfde doel worden gebruikt en waarvoor dezelfde beveiligingseisen gelden in hetzelfde subnet te plaatsen. Zo kunnen bijvoorbeeld alle werkplekken in dezelfde adresreeks worden geplaatst of kunnen servers van een bepaalde dienst in één subnet worden geplaatst. Indien een firewallconfiguratie voor deze groep apparaten nodig is, volstaat slechts het configureren van een regel op één specifieke IP-reeks. Hiermee wordt de beveiligingsconfiguratie overzichtelijk en wordt de kans op fouten verminderd, waarmee de kans op een beveiligingsincident door misconfiguratie kleiner wordt. Bovendien kan hierdoor autorisatie tot netwerken en systemen overzichtelijker worden ingericht en eenvoudiger onderhouden worden. Het aanbrengen van een dergelijke structuur staat verder los van of dit een overheidseigen IPv6-blok is of niet.

> Structuur aanbrengen door middel van een nummerplan verkleint de kans op beveiligingsincidenten als gevolg van configuratiefouten en vereenvoudigt autorisatie. Deze structuur op organisatieniveau aanbrengen, zonder verdere afspraken tussen overheidsorganisaties, brengt op zichzelf al een voordeel met zich mee.

Het koppelen van netwerken van verschillende overheidsorganisaties vereist onder meer dat beide netwerken voldoen aan vergelijkbare beveiligingseisen die voor de betreffende toepassing van die netwerken gelden. Door bij voorbaat afspraken te maken tussen overheden over deze eisen voor netwerken die mogelijk in de toekomst worden gekoppeld, kan het koppelen van deze netwerken op het moment dat het zover is, eenvoudiger worden. Het koppelen op IP-niveau is hierbij één aspect. Door in het IPv6-nummerplan van een overheidsorganisatie adresblokken te reserveren voor beveiligde netwerken die mogelijk in de toekomst kunnen worden gekoppeld, kan het koppelen wat betreft IPv6-adressering worden vereenvoudigd. Het gaat hierbij met name om het koppelen van netwerken met een rubricering vertrouwelijk of hoger.

In Figuur 7 is het koppelen van IPv6-netwerken uitgewerkt in een voorbeeld. Stel, overheid A (links in de figuur) wil een vertrouwelijk datanetwerk koppelen aan het vertrouwelijke datanetwerk van overheid B (rechts in de figuur). Omdat beide overheden volgens dezelfde eisen een vertrouwelijk datanetwerk hebben ingericht (A1 en B1) en hiervoor een aparte netwerkprefix hebben gebruikt, kunnen zij de netwerken op IP-niveau eenvoudig koppelen. Met ‘eenvoudig’ wordt bedoeld dat de procedures om te mogen koppelen sneller kunnen worden afgehandeld en dat geen IPv6-omnummeractiviteiten noodzakelijk zijn om de koppeling technisch te realiseren.



Figuur 7: Voorbeeld van het koppelen van overheidsnetwerken met een gereserveerde prefix.

Door bepaalde IPv6-reeksen te reserveren en vergelijkbare eisen te hanteren voor netwerken met een bepaald beveiligingsniveau, wordt het koppelen van deze netwerken wat betreft IPv6-adressen in de toekomst eenvoudiger. Bijvoorbeeld kan hiervoor een standaardprefix worden afgesproken.

Wat betreft het gebruik van één overheidsadresreeks is het de vraag of het monitoren van overheidsnetwerken eenvoudiger wordt. Hierbij is het cruciale punt of het hanteren van overheids-IPv6-adressen het voor beveiligingsinstanties binnen de overheid eenvoudiger maakt om te bepalen van welk systeem bij welke overheid bepaald verkeer vandaan komt, of meer in het algemeen te kunnen constateren dat het adressen betreft die in gebruik zijn voor een overheidsnetwerk of -dienst. Hierbij is de registratie van de IP-adressen die bij de overheid in gebruik zijn een cruciaal element. De geïnterviewde partijen zijn het erover eens dat inzicht hierin bijdraagt aan betere monitoring van incidenten (bijvoorbeeld het identificeren van gehackte systemen binnen de overheid), en het reageren hierop (bijvoorbeeld het in quarantaine plaatsen van een bepaald netwerk bij een bepaalde overheidsorganisatie). Op zich maakt het hiervoor niet veel uit wat voor IP-adressen overheden gebruiken en of deze al dan niet uit één blok komen.

Echter, het hebben van een overheidsreeks maakt meteen inzichtelijk dat het om overheidsadressen gaat, terwijl het gebruik van allerlei verschillende reeksen van verschillende LIR's bij allerhande overheden en leveranciers het maken van een compleet en up-to-date overzicht bewerkelijker maakt. Indien het overzicht niet compleet is, betekent dit dat op het moment dat een incident plaatsvindt veel meer tijd moet worden besteed om de juiste beheerder van het juiste netwerk te vinden. Het NCSC heeft in een interview aangegeven dat dit slechts een klein voordeel met zich meebrengt, omdat IP-adresreeksen ook bekend zijn voor incident response

doeleinden als zij niet uit één blok komen. In het interview met het ministerie van Binnenlandse Zaken van Duitsland en tijdens de 2e workshop met de begeleidingscommissie werd aangegeven dat het beperken van het aantal overheidsblokken wel degelijk grote voordelen heeft, omdat het creëren van een betrouwbaar overzicht van welke IP-adressen in gebruik zijn bij welke overheid een grote uitdaging is als er totaal geen sprake is van coördinatie van IP-adressen. Het gaat hierbij om het inzichtelijk maken van 1) dat het overheidsadressen zijn en 2) wie de verantwoordelijke beheerder is van de adressen.

Naast het voordeel van inzichtelijkheid voor incident response maakt het gebruik van een overheidsreeks het voor beheerders makkelijker om te identificeren wanneer er 'verkeerd' (lees: niet overheids-) verkeer op bepaalde verbindingen loopt. Als alleen verkeer vanuit de overheidsprefix is toegestaan dan is eenvoudig te monitoren wanneer er zich verkeer van anderen op het netwerk bevindt en volstaat een beveiligingsregel op die ene overheidsprefix.

> Het hanteren van één overheidsprefix maakt de IP-adressen van de overheid herkenbaarder, waardoor sneller kan worden geconstateerd dat er overheids-IP-adressen worden misbruikt. Daarnaast helpt helpt bij het detecteren van (kwaadwillend) niet-overheidsverkeer binnen in overheidsnetwerken.

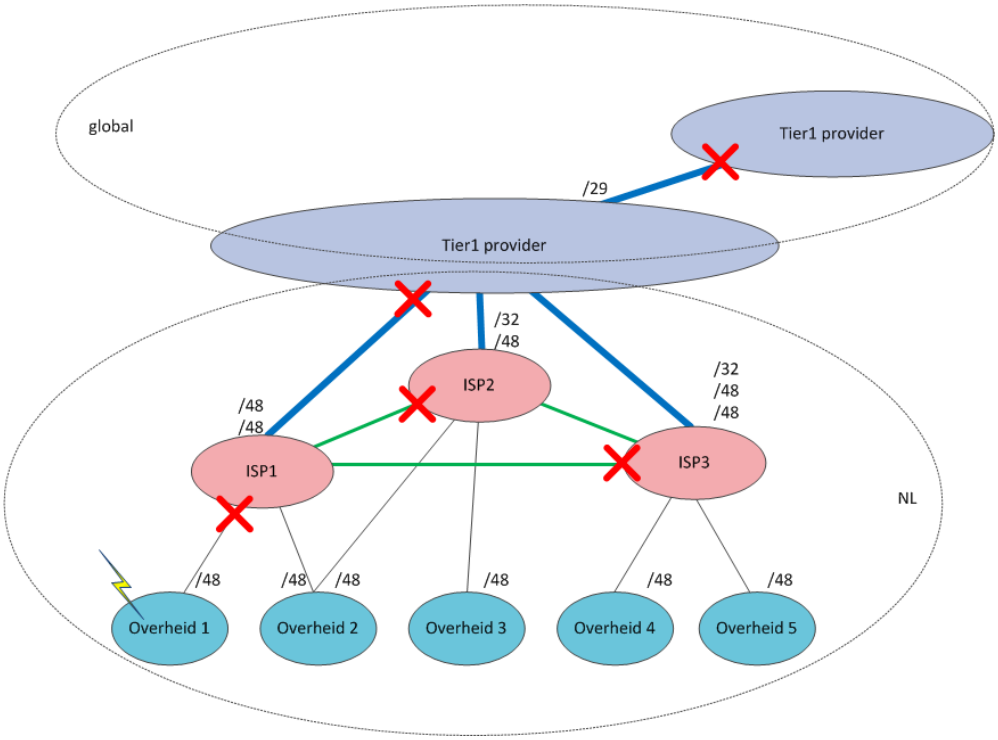
Het gebruik van een overheidsadresreeks roept ook de vraag op of dit mogelijk ook nadelen heeft voor de informatieveiligheid van de overheid. Hierbij zijn de volgende aspecten van belang:

- Het gebruik van overheids-IP-adressen maakt het voor kwaadwillenden direct inzichtelijk dat het om systemen van de overheid gaat.
- Als alle overheidsadressen door één LIR worden aangevraagd worden, in hoeverre hebben andere overheidsorganisaties er last van als deze LIR zijn taken niet naar behoren uitvoert.
- Door één prefix te gebruiken kan een fout van één overheidsorganisatie leiden tot connectiviteitsproblemen van de gehele overheid.

Bij deze aspecten is het van belang op te merken dat de overheids-IPv6-adresreeks in kleine, niet-aaneengesloten delen door verschillende ISP's op Internet bereikbaar zal worden gemaakt. Stel dat bijvoorbeeld één prefix kwaadwillend verkeer genereert, dan is in de eerste plaats de lokale ISP die de betreffende prefix routeert er voor verantwoordelijk dit probleem op te lossen, danwel de betreffende prefix af te sluiten. Mocht de ISP dit niet afdoende doen, dan zullen upstream ISP's dit doen, waarbij de impact, afhankelijk van de onderlinge peeringrelaties, tot een deel van de overheden beperkt wordt.

Dit is weergegeven in een voorbeeld in Figuur 8. Stel, vanuit overheidsorganisatie 1 neemt een gecompromitteerd systeem deel aan een cyberaanval. Normaal gesproken wordt dit door upstream providers gedetecteerd en onderneemt ISP1 maatregelen, desnoods door het afsluiten (of: *blacklisten*) van overheidsorganisatie 1 (in de figuur aangegeven met een X). Op die manier heeft geen enkele andere overheidsorganisatie hier last van. Alleen in het geval dat ISP1 dit onvoldoende

doet zullen ISP2, ISP3 en de Tier-1 provider actie ondernemen en verkeer vanaf de overheidsprefix vanuit ISP1 blokkeren. Indien ISP1 alle overheidsprefixen als één blok adverteert worden meer overheden die via ISP1 zijn aangesloten op Internet geblokkeerd. De kans dat deze blokken aaneengesloten zijn is echter klein, omdat alle overheidsorganisaties zelf hun ISP selecteren. De overheden die zijn aangesloten via andere ISP's dan ISP1 zullen hier in geen enkel geval last van ondervinden.



Figuur 8: De kans op blacklisting van de gehele overheidsprefix indien één deel-prefix problemen veroorzaakt is minimaal.

Wat betreft het argument dat het voor kwaadwillenden inzichtelijk is welke IP-adressen in gebruik zijn bij de overheid stelt het Nationaal Bureau voor Verbindingsbeveiliging (NBV) in een onderzoek, dat zij hebben uitgevoerd in het kader van het IPv6-nummerplan voor de Rijksoverheid[34], dat "er echter ook andere kernmerken zijn waaruit en methodes waarmee een aanvaller kan concluderen dat het mogelijk gerubriceerde informatie betreft".

Doordat de overheidsprefix in stukken via verschillende ISP's op internet bereikbaar wordt gemaakt, is de afhankelijkheid tussen overheden via de overheidsprefix wat betreft routering op Internet zeer beperkt. Daarnaast introduceert het zichtbaar maken van een overheidsprefix op Internet slechts een beperkt risico.

[34] "IPv6-nummerplan – Security overwegingen geharmoniseerd IPv6-nummerplan Rijk", NBV, juli 2014

Indien er een overheids-LIR is en deze LIR houdt zich niet aan de regels die RIPE NCC stelt aan het lidmaatschap, dan ontstaat er mogelijk een risico voor de overheidsorganisaties die een deel van de adresreeks van deze LIR gebruiken. In zulke gevallen kan RIPE NCC in theorie de toegekende adressen van de LIR terugnemen. In de praktijk kan dit door borging binnen de overheid eenvoudig worden voorkomen. Uit de raadpleging bij SURFnet blijkt dat zij geen geval kennen waarbij dit zich heeft voorgedaan. Bovendien heeft LIR-schap ook voordelen, in de zin dat iedere LIR bij RIPE inspraak heeft en voorstellen kan doen aangaande het IP-uitgiftebeleid dat RIPE NCC uitvoert. In geval van een centrale LIR kan het overheidsbelang via één partij worden behartigd (naast eventuele andere individuele LIR's die dit recht ook behouden).

Het bewaken van de continuïteit van een eventuele overheids-LIR moet door de overheid worden geborgd. Daarnaast kan een centrale LIR de belangen van de overheid als geheel behartigen bij het opstellen van RIPE beleid aangaande de uitgifte van IP-adressen.

4.2.2 Conclusie

Het hebben van een overheidsbreed IPv6-nummerplankader kan leiden tot betere informatieveiligheid:

- door het certificeren van IP-reeksen op internet zelf in de hand te hebben, in plaats van dit in de handen van leveranciers te leggen;
- indien gebruik gemaakt wordt van één of een beperkt aantal overheidsprefixes dan kunnen beheerders en systemen binnen de gehele overheid sneller detecteren of verkeer al dan niet bij de overheid vandaan komt.
- indien structuur wordt aangebracht in IPv6-nummerplannen op organisatieniveau. Dit vermindert de kans op beveiligingsincidenten ten gevolge van configuratiefouten en vereenvoudigt autorisatie tot netwerken en systemen.
- gezamenlijke afspraken binnen het IPv6-nummerplankader over de beveiligingsniveaus van specifieke adresreeksen kunnen bijdragen aan het eenvoudiger koppelen van overheidsnetwerken.

Los van de discussie over nummerplannen is een veilige introductie van IPv6 op zichzelf van groot belang. Verschillende best-practices[35] zijn beschikbaar om dit te realiseren.

4.3 Financieel voordeel

4.3.1 Analyse

Uit de voorgaande discussies rond het IPv6 Rijksnummerplan en de interviews, die tijdens dit onderzoek zijn uitgevoerd, komen uiteenlopende financiële aspecten naar voren. Tijdens de tweede projectworkshop met de begeleidingscommissie zijn

[35] SURFnet-rapport "IPv6 Beveiliging", 11 maart 2014, I. van Beijnum, https://www.surf.nl/kennis-en-innovatie/kennisbank/2014/rapport-ipv6-beveiliging.html

een aantal hypothesen over financieel voordeel besproken. Uit deze discussie volgt dat de analyse van financieel voordeel door het toepassen van een overheidsbreed IPv6-nummerplankader zich in ieder geval zou moeten richten op drie aspecten:

- het aantal LIR-lidmaatschappen binnen de overheid wordt beperkt;
- het centraal uitvoeren van bepaalde taken ontlast decentrale overheden;
- niet of minder hoeven omnummeren voorkomt of bespaart kosten voor omnummeractiviteiten.

Uit de gehouden interviews blijkt dat financieel voordeel in relatie tot het voorkomen van omnummeren door het gebruik van eigen IPv6-adressen lastig te kwantificeren is. In deze analyse zal in de eerste plaats een kwalitatieve duiding gegeven worden van financieel voordeel en een model worden opgenomen in de bijlage waarmee een voorbeeldberekening kan worden uitgevoerd. Deze voorbeeldberekening is beperkt in scope en gebaseerd op een aantal aannames die een ruime onzekerheidsmarge met zich meebrengen. In deze context moeten deze inschattingen gezien worden als indicatie.

LIR-lidmaatschapskosten

Wat betreft het aspect van LIR-lidmaatschappen onderscheiden we drie situaties:

1. De huidige situatie van Nederlandse overheidsorganisaties die LIR zijn;
2. Het geval waarin gemigreerd wordt naar één overheids-LIR;
3. Het geval waarin bijna iedere overheidsorganisatie LIR zou worden.

In de huidige situatie zijn er volgens de publieke lijst van LIR's die is gepubliceerd door RIPE NCC zo'n 18 Nederlandse overheidsorganisaties LIR[36]. Een aantal daarvan leveren als LIR ook diensten aan andere overheidsorganisaties.

In het Rijks IPv6-nummerplan is er sprake van één LIR (met uitzondering van het ministerie van Defensie). In het geval dat deze LIR, ook de LIR wordt voor de gehele Nederlandse overheid, dan treedt situatie 2 op. In dit geval zullen decentrale overheidsorganisaties hun IPv6-adressen aanvragen bij de overheids-LIR in plaats van dat zij dit bij een andere LIR, bijvoorbeeld een leverancier, doen. In principe verandert er weinig in de activiteiten die een overheidsorganisatie moet uitvoeren, behalve dat ze naar een ander 'loket' moet.

De LIR lidmaatschapskosten aan RIPE NCC, ter waarde van €1.700 per jaar, hoeven in het geval van één centrale LIR slechts door deze ene partij betaald te worden. Ook de (her)training van personeel en de interactie met RIPE NCC hoeft maar vanuit één organisatie gedaan te worden. De mensinzet die hiermee gepaard gaat wordt ingeschat op een paar dagen per jaar, per persoon. Hier staat tegenover dat er ook interactie nodig zal zijn tussen de centrale LIR en de decentrale overheidsorganisaties. Al met al schatten we in dat het beperken van het aantal LIR-schappen tot één centrale LIR onder de huidige omstandigheden een beperkte besparing op kan leveren van enkele tienduizenden euro's per jaar.

Een andere toekomstige situatie die zou kunnen ontstaan is dat er een sterke toename komt van het aantal overheidsorganisaties dat LIR wordt. Bijvoorbeeld, indien het gebruik van overheidseigen adressen sterk wordt aangemoedigd, zonder

[36] www.ripe.net/membership/indices/NL.html

dat het afnemen van IPv6-adressen van één centrale LIR wordt gestimuleerd. In theorie zou dat kunnen leiden tot een situatie van honderden overheden die (al dan niet op beperkte schaal gezamenlijk) LIR worden. In dat geval komen de activiteiten behorende bij LIR-schap bij de betreffende overheidsorganisatie te liggen en stijgen de LIR-kosten fors, in de orde van honderdduizenden euro's per jaar. Voor sommige gemeenten, of shared service centra past het zijn van LIR bij hun manier van werken, maar voor veel decentrale overheden zal dit niet de voorkeur hebben. Kortom, mits de werkwijze van individuele overheidsorganisaties door een centrale LIR niet verder wordt ingeperkt dan de algemene voorschriften die RIPE NCC aan haar LIR's stelt[37] (behoud van autonomie), lijkt voor individuele overheden die nog geen LIR zijn de stap klein om gebruik te gaan maken van één centrale overheid-LIR. Met degenen die al wel LIR zijn zal moeten worden afgestemd hoe zij op een zo kosteneffectief mogelijke manier deel uit kunnen maken van het overheidsbrede IPv6-nummerplankader.

Het introduceren van één overheids-LIR zal de jaarlijkse lidmaatschapskosten voor de overheid als geheel reduceren, zonder dat dit voor (de meeste) overheidsorganisaties invloed zal hebben op hun werkwijze. Ten opzichte van de huidige situatie is een geringe, jaarlijkse kostenreductie mogelijk. Een toekomstige situatie waarin honderden individuele overheden LIR worden, is onwenselijk vanuit het oogpunt van significant hogere LIR-kosten ten opzichte van de huidige situatie.

Centraal uitvoeren van taken ontlast decentrale overheden

Zoals hierboven is aangegeven zullen bij een centraal LIR-schap bijbehorende taken van decentrale LIR's overgeheveld worden naar de centrale LIR. In principe biedt een overheidsbreed nummerplankader de mogelijkheid om meer IPv6-adres beheertaken te centraliseren en daarmee decentrale overheden te ontlasten. Hoewel dit in principe mogelijk is, zien we hierbij een aantal belemmeringen. Ten eerste, constateren we dat er altijd IPv6 (en IPv4) configuratie en registratie taken decentraal uitgevoerd moeten worden. Bijvoorbeeld, voor het uitvoeren van eventuele IP adres configuratie (herstel)werkzaamheden op fysieke apparaten blijft het decentraal uitvoeren ervan veel efficiënter. In de praktijk zal het centraliseren van LIR-schap tot weinig wijzingen leiden in de kosten voor het uitvoeren van taken bij decentrale overheden.

[37] RIPE NCC stelt een aantal (policy) regels aan haar leden (LIRs) m.b.t. IP adres toekenning en m.b.t. compleetheid en correctheid van IP adres registratie. Deze regels zijn door de leden opgesteld. Zie de "RIPE NCC LIR Training Course van oktober 2014".

De verwachting is dat het ontlasten van decentrale overheden door het centraliseren van IPv6 LIR-schap beperkt zal zijn en tot weinig significante kostenbesparingen zal leiden. Ook het centraliseren van andere taken op het gebied van IPv6 adresbeheer ligt niet voor de hand.

Kosten voor omnummeren

Kosten voor omnummeren zijn eerder beschreven in Paragraaf 4.1, waarbij de mogelijke omnummeractiviteiten zijn beschreven in Tabel 3. Door een rekenvoorbeeld te geven van het aantal omnummeractiviteiten dat op jaarbasis nodig is kan een indicatie gegeven worden voor de omnummerkosten die de Nederlandse overheid (of leveranciers van overheidsdiensten) jaarlijks als geheel maakt ten gevolge van een wissel van connectiviteitleverancier. Dit rekenvoorbeeld is terug te vinden in de bijlage A. De omnummerkostenraming komt daarin op ongeveer twee miljoen euro per jaar, voor de overheid als geheel. Ten opzichte van de totale IP-beheerlast van alle overheden bij elkaar is dit een beperkt bedrag. Het wordt door sommige partijen echter wel als belemmerend ervaren.

In sommige gevallen zullen de omnummerkosten direct zichtbaar zijn op een projectbegroting, in andere gevallen kan een gereduceerde omnummerinspanning leiden tot een toegenomen productie-efficiëntie, omdat het de werkdruk van netwerkbeheerders kan verminderen[38] zodat zij meer tijd aan andere zaken kunnen besteden.

Wat uit deze voorbeeldberekening direct volgt is dat de kostenvoordelen groter worden naarmate meer overheden gebruik maken van overheid-eigen IPv6-adressen en vooral naarmate er meer koppelingen tussen overheden bestaan waarop met IP adresreeksen wordt gewerkt voor bijvoorbeeld filtering of routering.

Het zal, gezien de levenscyclus van ICT systemen wellicht 5 tot 10 jaar kunnen duren voordat een overheidsbreed IPv6-nummerplankader breed door overheidsorganisaties wordt opgevolgd. Om die reden zullen de hiergenoemde kostenvoordelen pas op langere termijn gerealiseerd worden.

Nogmaals merken we op dat bovenstaande aannamen reeds aangeven dat deze berekening een flinke onnauwkeurigheidsmarge heeft. Het verdient dan ook de aanbeveling om de aannamen achter deze berekening verder te laten toetsen en aan te scherpen. Desalniettemin illustreert deze kosteninschatting dat “omnummeren van diensten en netwerken waarvoor door andere overheden/diensten filter-regels of verwijzingen naar IP-adressen zijn opgenomen, grote omnummer-impact introduceren”.

[38] Een geïnterviewde leverancier gaf aan dat omnummeractiviteiten vaak in het weekend plaatsvinden, omdat het zo min mogelijk verstoringen voor de bedrijfsvoering moet opleveren. Dit betekent dat beheerders dit soort werkzaamheden buiten reguliere werktijden moeten uitvoeren.

Van de genoemde potentiële financiële voordelen lijkt de reductie van omnummerinspanning bij een leverancierwissel door het gebruik van overheid-eigen IPv6 adressen het omvangrijkst. Echter, “of”, “voor wie”, “wanneer” en “in welke vorm” deze baten worden behaald hangt sterk af van de specifieke situatie.

Overige financiële aspecten

Het voeren van een overheidsbreed IPv6-nummerplankader introduceert extra kosten voor communicatie over en afstemming van de afspraken in het kader. Dit zijn jaarlijks terugkerende kosten. In Duitsland heeft de overheids-LIR een bredere taak om te adviseren bij de uitrol van IPv6 bij overheidsorganisaties en ook internationaal, bijvoorbeeld op het niveau van de Europese Commissie, dragen zij actief hun plannen uit. Om dit te kunnen realiseren hebben zij twee personen aangenomen, één meer beleidsmatig persoon en één technisch adviseur.

Daarnaast hebben sommige overheidsorganisaties al een IPv6-nummerplan opgesteld en ingezet. Voor deze partijen vereist omnummeren naar overheidsadressen een bepaalde additionele inspanning. Voor partijen die IPv6 nog moeten gaan invoeren wordt het een regulier onderdeel van de inrichting van IPv6, die ze sowieso hadden moeten uitvoeren.

Het verdient hierom de voorkeur om de eventuele overgang naar een overheidsbreed IPv6-nummerplankader op logische momenten voor individuele overheidsorganisaties te doen, bijvoorbeeld op momenten waarop herconfiguratie van de ICT-omgeving om andere reden toch al aan de orde is, bijvoorbeeld bij een aanbestedingstraject en leverancierswissel.

4.3.2 Conclusie

Het gebruik van eigen overheidsadressen, ongeacht wie ze aanvraagt, kan kostenvoordelen met zich meebrengen als daardoor een significant aantal omnummeractiviteiten kan worden voorkomen. Het aantal omnummeractiviteiten dat wordt voorkomen hangt af van het aantal IP-specifieke configuraties die moeten worden aangepast op andere plekken binnen de overheid en overheidsdiensten als gevolg van een leverancierswissel van één netwerk of dienst. Omnummeren zal voor een centrale overheidsdienst in de regel een veel grotere impact hebben, dan voor een lokale dienst. De omnummerkosten zijn niet altijd direct zichtbaar voor de overheid. Soms leidt minder omnummeren alleen tot een lagere werkdruk van de beheerder, of tot minder werk bij een leverancier die de omnummering normaal gesproken zou hebben uitgevoerd.

De kosten en verantwoordelijkheden die komen kijken bij een LIR-schap zijn voor veel overheidsorganisaties niet aantrekkelijk. Om die reden is het verstandig het aantal LIR’s binnen de overheid te beperken.

De kostenvoordelen nemen toe naarmate meer partijen gebruik maken van overheidsnummers. Ze nemen daarmee vooral op lange termijn toe (5-10 jaar), zijn verdeeld over een groot aantal partijen en daardoor per partij beperkt.

Daartegenover staat dat de invoering van een overheids-IPv6-nummerplankader naar verwachting ook geen dermate hoge kosten met zich meebrengt, dat deze een reden zijn om een dergelijk kader niet in te voeren. Deze kosten relateren aan het uitvoeren van activiteiten met betrekking tot communicatie en het uitdragen van het kader.

4.4 Overige baten en randvoorwaarden

4.4.1 Toekomstvastheid

Indien een IPv6-nummerplankader voor de overheid wordt opgesteld is het belangrijk om ervoor te zorgen dat de uitgedeelde IPv6-reeksen en -indelingen liefst niet meer veranderen. Dit betekent enerzijds dat ruimte moet worden overgehouden om nieuwe adresreeksen te kunnen inzetten voor nieuwe toepassingen in de toekomst. Wat betreft het aansluiten van vele apparaten en sensoren binnen een subnet (voor zogeheten Internet of Things-toepassingen) geldt dat een IPv6 subnet altijd een prefix van 64 bits en een zeer grote omvang kent om apparaten/sensoren aan te sluiten. Bovendien is het bij IPv6 niet nodig om IPv6-adressen dubbel in gebruik te hebben op andere plekken binnen de overheid, zoals met IPv4 wel gebeurt met private adressen[39].

> De vaste en omvangrijke IPv6 subnetomvang (/64) en de grote IPv6-adresruimte zijn uitermate geschikt om vele apparaten binnen een subnet aan te sluiten, en nieuwe subnetten te definiëren wanneer nodig.

In geval van organisatorische veranderingen op bijvoorbeeld departementaal niveau of gemeentelijke herindelingen dan geldt dat:

- in geval van het samenvoegen van twee overheidsorganisaties dit niet leidt tot een verandering in de uitgedeelde prefixen aan deze organisaties. Wel kan er binnen de organisaties sprake zijn van benodigde omnummer-acties of blijven beide nummerreeksen in gebruik. Dit levert niet meer werk op ten gevolge van een organisatorische verandering, dan als er geen overheidsbreed nummerplankader zou zijn.
- in geval van het splitsen een overheidsorganisatie er kan worden gekozen om een nieuw nummerblok te introduceren voor één van de nieuw ontstane organisaties. Uitgedeelde adresblokken blijven ongewijzigd. Omnummeractiviteiten binnen de organisaties zijn mogelijk noodzakelijk, niet anders dan als er geen overheidsbreed nummerplankader zou zijn.

[39] RFC1918

Een goed nummerplankader houdt ruimte over voor nieuwe overheidsorganisaties die ontstaan en een goed nummerplan houdt ruimte over voor nieuwe netwerken en diensten die in de toekomst mogelijk worden uitgerold.

4.4.2 Bestuurlijke autonomie

Een kader zal zich moeten beperken tot de strikt noodzakelijke afspraken tenzij er zwaarwegende overwegingen zijn voor verdergaande afspraken. Nederlandse overheden kennen een grote autonomie in de keuzes die zij maken ten aanzien van de inrichting van hun ICT. Overheden moeten zo weinig mogelijk door het kader beperkt worden in het maken van keuzes ten aanzien van hun eigen bedrijfsvoering. Het zelf aansturen van aanbestedingstrajecten, contractmanagement, aansturingen van technische netwerkinrichting en beheer, het uitrollen van nieuwe diensten, het aansturen van inzet van mensen en middelen op het gebied van ICT blijft de verantwoordelijkheid van de afzonderlijke organisaties. Dat geldt ook voor de invulling van het nummerplan van de individuele organisatie.

Daarnaast liggen de huidige keuzes vaak vast in contracten en systemen en zijn ze lokaal bepaald. De voordelen van bepaalde gezamenlijke afspraken zullen daar zeer afhankelijk van zijn.

Tot slot brengt een uitgebreid en stringent kader grote inspanningen met zich mee ten aanzien van handhaving. Bijvoorbeeld, strikte handhaving uitvoeren op de mogelijke aanbeveling “iedere organisatie moet een actueel IPv6-nummerplan hebben” zou kunnen betekenen dat er een instantie moet zijn die periodiek nummerplannen opvraagt bij organisaties en in de eigenlijke infrastructuur controleert of het nummerplan correct wordt toegepast. Hier wordt verder op ingegaan in Paragraaf 5.6 aangaande de governance van het nummerplankader.

4.4.3 Overige technische aandachtspunten van het gebruik van een overheidsprefix

Overwegingen van het gebruik van een overheidsprefix voor routering
Het gebruik van een eigen prefix heeft implicaties op het gebied van routering. Hier spelen twee verschillende aspecten een rol:

1. Iedere (de)centrale overheid moet zijn eigen adresblok door een externe internetprovider op Internet bereikbaar laten maken.
2. Er moet een keuze worden gemaakt of er één of meerdere prefixen op het netwerk van een overheidsorganisatie worden gebruikt.

Wat betreft het eerste aspect moeten er afspraken worden gemaakt met een internetprovider die het blok naar internet routeert. Hierbij gelden de volgende aandachtspunten:

- Een geïnterviewde internetprovider gaf aan bereid te zijn om overheidsadressen op deze manier bereikbaar te maken op internet. In het geval dat deze adressen onderdeel zijn van een centraal overheidsnummerblok wil deze leverancier een contractuele afspraak maken met zowel de overheids-

LIR als de betreffende decentrale overheid over de verantwoordelijkheden. Voor een andere leverancier is dit 'business as usual' en zij voorziet geen enkel probleem of noodzaak tot verdergaande afspraken. Dit punt kan meegenomen worden in de reguliere contractbesprekingen met leveranciers van de overheid.

- Indien blokken die kleiner zijn dan een /32 moeten worden gerouteerd door leveranciers dan zou er mogelijk een probleem kunnen ontstaan met de routeerbaarheid van deze adresreeksen op internet. In gesprekken met BT en KPN Lokale Overheid werd aangegeven dat het routeren van leveranciersonafhankelijke /48 prefixen van individuele organisaties geen probleem met zich meebrengt. In het interview met Duitsland werd aangegeven, dat je hier als overheid niet in alle gevallen op kunt rekenen. Het kan immers zo zijn dat een upstream provider van de overheids-ISP, andere routingregels toepast waardoor de /48 niet wordt gerouteerd. Om deze reden is in Duitsland het voorstel gedaan om afspraken te maken tussen alle leveranciers van de overheid om de overheidsprefixen die eenieder adverteert correct te routeren. Daarnaast overwegen zij om ook zelf de volledige overheidsprefix te adverteren op Internet, zodat dit als backup-mechanisme kan worden gebruikt indien meer-specifieke reeksen onbereikbaar zijn. Een alternatief hiervoor is erop te vertrouwen, of in contracten op te nemen, dat ISP's van overheidsorganisaties er zorg voor dragen dat zij dit met hun upstream en peering-partners correct regelen. Omdat ook in Duitsland nog geen definitief uitsluitsel bestaat over de (on)mogelijkheden van een dergelijke oplossing verdient het de aanbeveling om dit soort overwegingen mee te nemen bij de daadwerkelijke invoering van een overheidsbreed IPv6-nummerplankader.
- In interviews (onder meer door KING/IBD[40] en de Gemeente Alkmaar) werd aangegeven dat een ISP-abonnement van een gemeente mogelijk duurder wordt. Hier konden, ook door leveranciers, echter geen specifiek bedragen voor genoemd worden. Een mogelijk voorbeeld dat hierbij werd gegeven is dat van een partij die een MKB-internetabonnement gebruikt en vanwege het gebruik van een overheidsprefix een iets duurder zakelijk abonnement moet afnemen.

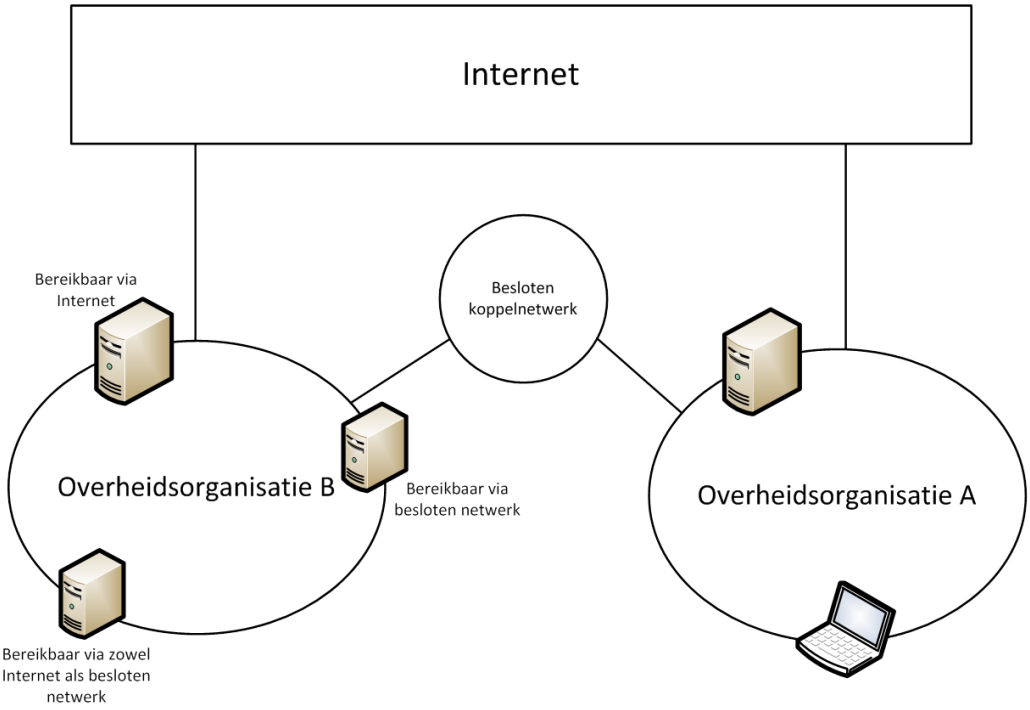
> Bij gebruik van een overheidsbreed IPv6 adresblok, zal iedere decentrale overheidsorganisatie afspraken moeten maken met haar ISP én mogelijk ook de overheids-LIR, om de aan haar toegewezen reeks via Internet bereikbaar te maken. Deze reeks mag niet kleiner zijn dan /48.
>
> Er bestaat een kans dat niet iedere internetrouter alle /48s op een goede manier routeert. Op dit moment wordt er gewerkt aan mogelijke oplossingen hiervoor (met name Duitsland). Bij definitieve vaststelling van een overheidsbreedkader zullen de ontwikkelingen hieromtrent gevolgd en meegenomen moeten worden.

Figuur 9 geeft de situatie weer waarbij een overheid gekoppeld is aan meerdere netwerken: een besloten netwerk en Internet. Het verdient de aanbeveling om op het interne netwerk maar één globale IPv6-reeks te gebruiken en ervoor te kiezen

[40] Informatie Beveiligings Dienst (IBD), http://www.ibdgemeenten.nl

hier de overheidsreeks voor te gebruiken. Hierbij spelen de volgende aspecten een rol:

- Uit tests (onder meer door Fraunhofer Duitsland) blijkt dat je niet kunt vertrouwen op besturingssystemen van client devices om een keuze te maken in het bron-IP-adres dat wordt gebruikt. Een verkeerde keuze van bronadres kan mogelijk leiden tot asymmetrisch routeren[41].
- Door dit toe te passen kan worden gerealiseerd dat verkeer tussen overheden altijd verloopt over besloten netwerken.
- Vanuit beheer- en beveiligingsoogpunt is het handig om op het interne netwerk met één IP-reeks te werken, omdat anders voor elke reeks alle configuraties moeten worden ingesteld.
- Voor servers is het eventueel wel mogelijk deze ofwel op internet ofwel op het besloten netwerk of op beiden bereikbaar te maken, door gebruik te maken van IP-adressen uit verschillende reeksen. Het is hierbij verstandig andere interfaces te gebruiken, zodat hierop ook andere routing policies kunnen worden toegepast.



Figuur 9: Overheidsorganisatie A heeft een koppeling naar Internet en een besloten koppelnetwerk (bijvoorbeeld Diginetwerk). Overheidsdiensten kunnen door A worden benaderd via Internet of het besloten netwerk, afhankelijk van de betreffende dienst, die hier staan weergegeven in Overheidsorganisatie B.

[41] Met asymmetrisch routeren wordt bedoeld dat het antwoord van bijvoorbeeld een server onbedoeld via een andere route (bijvoorbeeld over internet) wordt teruggestuurd,dan het oorspronkelijke verzoek naar de server toe heeft afgelegd (bijvoorbeeld over een besloten netwerk).

Het verdient de aanbeveling om op het interne netwerk één globale IPv6-reeks te gebruiken en ervoor te kiezen hier de overheidsreeks voor te gebruiken.

Andere mogelijkheden om omnummeren te vereenvoudigen
Indien de omnummeren niet kan worden voorkomen is het zaak om de kosten van omnummeren zo laag mogelijk te houden (minimaliseer $K_{omnummeren}$). Onder meer de IETF zoekt naar manieren om het omnummeren van netwerken te vereenvoudigen. Hierbij richt zich men specifiek op het omnummeren van IPv6-netwerken. RFC6879[42] benoemt verschillende technieken die beschikbaar zijn om het omnummeren van een bedrijfsnetwerk te vereenvoudigen. Zowel tijdens de netwerkontwerpfase als tijdens de voorbereiding van het omnummerproces en het omnummerproces zelf dien hier rekening mee te worden gehouden. Het verdient de aanbeveling om dit waar mogelijk toe te passen. Ondanks dat zal dit in de praktijk niet overal gebeuren. Bovendien zijn bijvoorbeeld statische IP-adressen nog vaak in gebruik en niet alle gevallen te voorkomen[43].

Omnummerinspanning kan bij IPv6 door goede netwerkinrichting worden verminderd. Het kan in de praktijk echter nog niet overal worden voorkomen.

Network Address Translation (NAT)
In IPv4 wordt Network Address Translation (NAT) in de eerste plaats toegepast om meerdere apparaten te kunnen aansluiten achter één bepaald publiek IP-adres, omdat het aantal publieke IPv4-adressen te klein werd om alle apparaten van een uniek adres te voorzien. Echter, NAT kan ook worden ingezet om het omnummeren van alle apparaten op een IP-netwerk te voorkomen. In plaats van het omnummeren van het interne netwerk en de systemen daarop, volstaat het aanpassen van de vertaalregels in de NAT-tabel op de rand van het netwerk.

Bij IPv6 is NAT niet meer nodig, omdat er voldoende adressen zijn om ieder apparaat met een uniek IPv6-adres te kunnen aansluiten op Internet. De afwezigheid van NAT vereenvoudigt bovendien end-to-end communicatie, end-to-end security en netwerkmonitoring tot op het individuele apparaat, hetgeen detectie van verkeer dat niet betrouwbaar is vereenvoudigt. Door de afwezigheid van NAT is het door de overkoepelende organisatie snel aan te wijzen vanuit welke subafdeling van een bepaalde overheid het ongewenste verkeer komt.

In de gehouden interviews werd NAT in IPv6 zowel genoemd als ongewenste technologie als een oplossing voor individuele overheidsorganisaties om interne netwerken niet meer te hoeven omnummeren.

[42] “RFC6879 - IPv6 Enterprise Network Renumbering Scenarios, Considerations, and Methods”, S. Jiang et al., februari 2013, IETF, https://tools.ietf.org/html/rfc6879
[43] “RFC6866 - Problem Statement for Renumbering IPv6 Hosts with Static Addresses in Enterprise Networks”, B. Carpenter et al., februari 2013, IETF, https://tools.ietf.org/html/rfc6866

Het gebruik van NAT in IPv6 wordt afgeraden. Hoewel het een voordeel lijkt te geven om niet te hoeven om te nummeren, wegen deze niet op tegen de nadelen die het geeft. Belangrijke nadelen zijn bijvoorbeeld:

- Problemen met bepaalde applicaties niet alle applicaties kunnen goed met NAT omgaan bv VPN, FTP en/ of applicaties die gebruik maken van peer-to-peer protocollen.
- Security, er is geen zicht op end point achter NAT, het is het NAT vertaler die de end point bepaalt. Doordat de oorspronkelijke header wordt vertaald kan een protocol als IPsec hierop problemen geven.
- Extra activiteit in het netwerk, het vertalen van de adressen geeft extra werk en dus toename in de performance overhead van het netwerk. Zeker bij toepassing op grote schaal en bij veel verkeer kan dit tot een performance probleem leiden of tot noodzakelijke investeringen in “krachtige” apparatuur om de vertaling te kunnen maken.
- En misschien wel de belangrijkste: er is op dit moment geen standaard aanwezig voor IPv6 NAT.

Er is wel een experimentele RFC beschikbaar voor IPv6 Network Prefix Translation. waarbij alleen de netwerkprefix wordt vertaald[44]. Deze technologie geeft minder problemen met applicaties omdat de end-to-end communicatie vastligt. Echter de problemen met IPsec en de extra performance overhead vanwege de vertalingen blijven bestaan.

4.5 Conclusie

Leveranciersafhankelijk kan worden vergroot door eigen overheidsadressen te gebruiken omdat:

- omnummeren bij een leverancierswissel kan worden voorkomen;
- het overheden de gelegenheid geeft om via meerdere leveranciers verbonden te zijn met internet, zodat hun beschikbaarheid toeneemt;

Informatieveiligheid kan met name worden vergroot door eigen overheidsadressen omdat:

- de overheid zelf de controle krijgt over het certificeren van overheids-IP-reeksen op internet.
- door het gebruiken van één overheidsblok, vanwege herkenbaarheid, makkelijker wordt om overheidsverkeer te onderscheiden van niet-overheidsverkeer waardoor misbruik eenvoudiger is te constateren en het zetten van beveiligingsregels op niet-overheidsverkeer eenvoudiger wordt.

Een nummerplankader kan slechts in beperkte mate bijdragen aan kostenvoordelen:

- het voorkomen van omnummeren spaart kosten uit en vergroot de productie-effectiviteit van beheerders omdat zij hun energie aan andere zaken kunnen besteden;
- indien je kiest voor het gebruik van overheidsadressen dan is het de verwachting dat veel overheidspartijen niet op de kosten en taken van LIR-schap zitten te wachten. In zo’n geval is het voordeliger dit centraal in te richten;

[44] “RFC6296 – IPv6-to-IPv6 Network Prefix Translation”, M. Wasserman & F. Baker, juni 2011, IETF, https://tools.ietf.org/html/rfc6296

- Een centraal nummerplankader vraagt om centraal onderhoud en afstemming. Echter, overheidsorganisaties behouden hun taken aangaande inrichting en beheer. Voor hen verandert slechts het ‘loket’.

Een belangrijk technisch aandachtspunt is verder de aanbeveling om client-apparaten maar van één globaal uniek IPv6-adres, uit één IPv6-reeks, te voorzien, ook indien dit apparaat gekoppeld is aan zowel internet als aan een besloten netwerk.

De mate waarin deze argumenten al dan niet zwaar wegen voor de overheid hangt mede af hoe de Nederlandse overheid in bredere context aankijkt tegen informatieveiligheid en de rol van leveranciers hierin. Bijvoorbeeld in Duitsland streeft men naar een zo groot mogelijke onafhankelijkheid van leveranciers aangaande connectiviteit vanwege informatiebeveiliging. Daarnaast zijn federale overheden en staten daar verplicht om met elkaar te communiceren via een besloten netwerk hetgeen een sterke drijfveer is voor het hanteren van één overheids-IPv6-adresblok, omdat hiermee de routering op dit besloten netwerk kan worden vereenvoudigd.

Het verdient verder de aanbeveling om bij de definitieve vaststelling van het kader de ontwikkelingen en ervaringen op dit gebied in Duitsland de komende periode te volgen. Ook daar zijn nog niet alle vraagstukken aangaande het praktisch implementeren van het nationale IPv6-nummerplan opgelost.

5 Elementen IPv6-nummerplankader NL overheden

Dit hoofdstuk beschrijft de afspraken die gezamenlijk kunnen worden gemaakt als onderdeel van een overheidsbreed IPv6-nummerplankader. Hierbij wordt per zogenaamd *element* beschreven welke mogelijkheden tot het maken van afspraken er zijn, en welke mogelijkheid de voorkeur heeft. Deze voorkeur is gebaseerd op de analyse van de potentiële voordelen van en randvoorwaarden voor een overheidsbreed IPv6-nummerplankader, zoals is uitgevoerd in Hoofdstuk 4. In dit hoofdstuk worden de elementen, de mogelijke keuzes en de voorkeursinrichting met de argumentatie daarbij genoemd. Voor ieder element wordt dit beschreven in een eigen paragraaf.

Dit kader dient te worden gelezen als startpunt voor een definitief kader. De ervaringen met het Nederlandse Rijks IPv6-nummerplan en de ervaringen in Duitsland en Spanje laten zien dat het cruciaal is om het definitieve IPv6-nummerplankader gezamenlijk met de relevante stakeholders op te stellen. In het geval van een overheidsbreed kader gaat het dan om het betrekken van technische stakeholders van decentrale overheden om de uiteindelijke kaders mee af te stemmen.

Om de elementen van het IPv6-nummerplankader te definiëren is tevens gekeken naar verschillende bronnen[45] waarin IPv6-nummerplannen, bijbehorend beleid of handleidingen daarvoor worden beschreven. De in dit onderzoek vastgestelde elementen zijn getoetst en akkoord bevonden tijdens de tweede workshop[46] met de begeleidingscommissie.

Het overheidsbreed IPv6-nummerplankader bestaat uit de volgende elementen:

- Element 1: Eigendom van door de overheid gebruikte IPv6-adressen
- Element 2: Herkomst van gebruikte IPv6-adressen (LIR-schap)
- Element 3: IPv6 uitgiftebeleid binnen de overheid
- Element 4: Zonering binnen overheidsorganisaties
- Element 5: Overige afspraken over IPv6-nummerplannen

Uit interviews en analyse blijkt dat het de moeite waard is naar overzichtelijkheid in ICT en een bepaalde mate van coördinatie te streven. Gelet op het belang van de autonomie van overheden, ten aanzien van de inrichting van hun ICT beperken we het kader tot een set afspraken die er vooral op gericht zijn overheden te faciliteren bij het gebruik van IPv6-adressen. De voorkeursinrichting dient met dit in het achterhoofd te worden gelezen. Daarnaast moet worden opgemerkt dat de voordelen van een overheidsbreed IPv6-nummerplankader groter worden, naarmate vanuit informatiebeveiligingsoogpunt meer belang wordt gehecht aan het hebben van directere controle over IP-reeksen en overheidscommunicatie over besloten netwerken.

[45] Onder andere is gekeken naar: SURFnet Handleiding IPv6-nummerplan, GEN6 Booklet Government IPv6 Addressing (http: //www.gen6-project.eu), IPv6-nummerplannen van SSC Zwolle en de gemeente Den Haag, IPv6 reference guide Duitsland

[46] Projectworkshop 2 met de begeleidingscommissie vond plaats op maandag 9 februari 2015

5.1 Element 1: Eigendom van door de overheid gebruikte IPv6-adressen

5.1.1 Toelichting element 1

Zoals in Paragraaf 2.5 is toegelicht verloopt de mondiale allocatie van IPv6-adresblokken via IANA en RIPE NCC naar de LIR's en richting de organisaties die uiteindelijk de IPv6-adressen op apparaten configureren. Het eerste element van het IPv6-nummerplankader heeft betrekking op het eigendom[47] van de IPv6-adressen die door een overheidsorganisatie worden gebruikt. Met *eigendom* wordt hier bedoeld dat het uiteindelijke gebruiksrecht van de betreffende IPv6-adressen bij de overheid ligt of bij de particuliere leverancier waarvan een overheidsorganisatie haar internetverbinding afneemt.

5.1.2 Voorkeursinrichting element 1

> Streef ernaar dat overheidsorganisaties gebruik maken van IPv6-adressen die eigendom zijn van de overheid.

De belangrijkste argumenten uit de analyse hiervoor zijn:

- Door eigen overheidsadressen te hebben, kan de overheid deze IP-reeksen zelf certificeren op internet.
- Door eigen overheidsadressen te gebruiken komt omnummeren als gevolg van een leveranciersoverstap minder vaak voor, hetgeen kostenvoordelen met zich meebrengt. In bepaalde gevallen kan hierdoor een leveranciersoverstap technisch eenvoudiger worden uitgevoerd.
- Het aansluiten van een overheidsorganisatie op internet via twee internetproviders vereist dat de overheidsorganisatie beschikt over eigen IP-adressen;

In verschillende interviews die zijn gehouden wordt uitgesproken dat het gebruik van overheidsadressen voordelen heeft voor de overheid (en soms ook voor de leverancier) en er worden weinig tot geen redenen gezien om dit niet te doen. De beveiligingsrisico's en extra kosten die het met zich meebrengt worden minimaal ingeschat. Vanuit Duitsland worden nog wel enkele aandachtspunten genoemd aangaande het verkrijgen van maximale zekerheid over het bereikbaar houden van deze overheidsadressen op internet. Bij definitieve vaststelling van het kader dienen deze aandachtspunten meegenomen te worden.

Daarnaast zijn er nog een aantal punten genoemd in de interviews, waarvan de impact bij het definitief vaststellen van het kader nader moet worden ingeschat:

- Eventuele impact op de kosten van een internetabonnement voor kleine overheden met een standaard MKB-internetaansluiting;

[47] IP adresblokken worden door RIPE NCC toegewezen aan organisaties, die de adressen mogen gebruiken, maar niet officieel in eigendom hebben. RIPE NCC behoudt zich het recht voor om, in bepaalde gevallen, de toegewezen adresruimte terug te vorderen.

- Een leverancier heeft in een interview aangegeven dat het gebruik van overheidsadressen mogelijk een aantal wijzigingen in de standaardcontracten vereist. De impact daarvan is niet op voorhand in te schatten, maar de verwachting is niet dat dit een drempel opwerpt voor het gebruik van eigen IPv6-adressen.
- Voor het gebruik van het koppelnetwerk GEMNET op Diginetwerk is in een interview aangegeven dat het gebruik van overheidsadressen daar niet zomaar mogelijk is.
- Het bepalen van eventuele uitzonderingssituaties.
- In principe zijn cloudservices ook gewoon diensten waar het zelfde voor geldt als voor andere diensten. Echter, in dit onderzoek is niet onderzocht hoe bijvoorbeeld SaaS[48] providers tegenover het gebruik van overheidseigen IPv6-adressen staan. Een alternatief is om bepaalde overheidsclouddiensten zelf te gaan organiseren in bijvoorbeeld een overheidscloud.

5.2 Element 2: Herkomst van gebruikte IPv6-adressen (LIR-schap)

5.2.1 Toelichting element 2

Een overheidsorganisatie kan op verschillende manieren aan haar IPv6-adressen komen, namelijk door zelf LIR te worden bij RIPE NCC of ze af te nemen bij een andere LIR. Deze LIR kan een bedrijf zijn, vaak een ISP, of een andere overheidsorganisatie. De centrale vraag hierbij is of je als overheid streeft naar één groot overheidseigen IPv6-adresblok, of dat dit niet uit maakt.

5.2.2 Voorkeursinrichting element 2

In element 1 staat beschreven dat het de voorkeur heeft om met overheidseigen IPv6-adressen te werken. Daarmee wordt de voorkeursinrichting voor element 2:

> Beperk het aantal overheidseigen IPv6-adresblokken en maak Logius de centrale LIR, waarbij decentrale overheden terechtkunnen.

De argumenten om te kiezen voor één overheidsbreed adresblok (bij een overheids-LIR), ten opzichte van vele overheidsadresblokken (bijvoorbeeld van diverse decentrale overheids-LIR's) zijn:

- Het hanteren van één overheidsprefix maakt de IPv6-adressen van de overheid herkenbaarder wat het onderscheiden van overheidsverkeer van niet-overheidsverkeer eenvoudiger maakt voor detectiesystemen en beheerders. Ook het registreren van overheidsadressen ten bate van het detecteren van misbruik op internet wordt eenvoudiger.
- Voor veel overheidsorganisaties zal het onwenselijk zijn om LIR te worden vanwege de kosten en verantwoordelijkheid die dit met zich meebrengt. Door een centrale LIR in te richten kunnen zij toch gebruik maken van overheidsadressen. Deze keuze is er dan ook vooral op gericht om overheden te faciliteren en te ondersteunen bij het aanvragen van IPv6-adressen.

[48] Software as a Service (Saas), http://nl.wikipedia.org/wiki/Software_as_a_Service

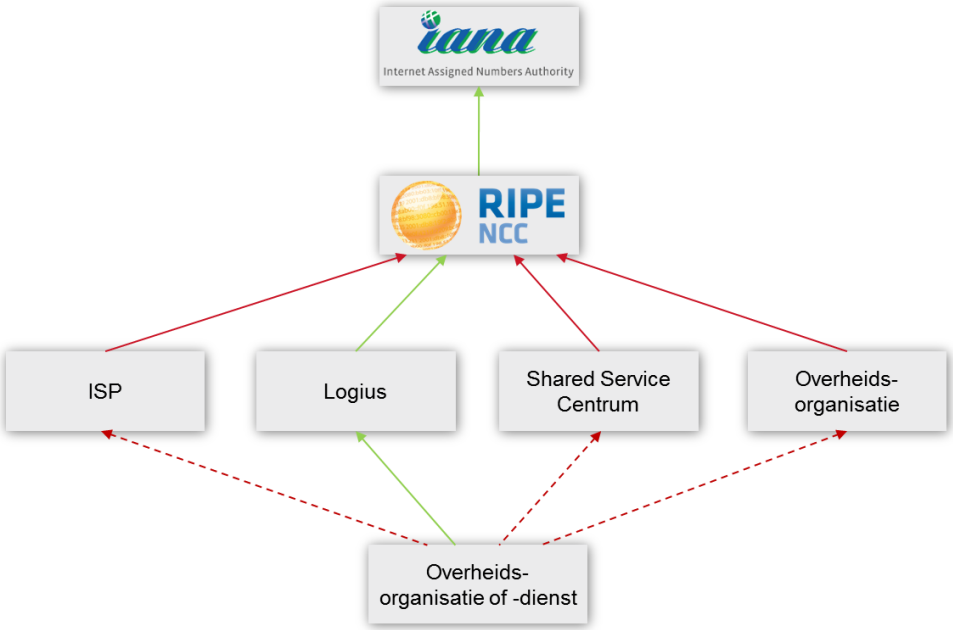
- Het gebruik van één overheidsadresblok ten opzichte van vele overheidsadresblokken kan leiden tot een afname van het aantal regels in routers en firewalls op verbindingen tussen overheden.

De nadelen van het hanteren van één overheidsprefix zijn technisch gezien beperkt, vooral omdat in de praktijk de overheidsreeks in kleine stukken via verschillende internetproviders naar Internet zal worden gerouteerd. Wel zijn er enkele aandachtspunten aangaande centraal LIR-schap:

- Het bewaken van de continuïteit van een overheids-LIR en het zich houden aan de regels van RIPE NCC is cruciaal om de overheidsadressen nu en in de toekomst voor alle overheden bruikbaar te houden.
- Enkele overheidsorganisaties beschikken al over eigen IPv6-adressen die zij als LIR hebben aangevraagd. Deze partijen moeten overwegen of en zo ja, wanneer het voor hen voordelig is om over te stappen naar de centrale overheidsadresreeks.

Indien een centrale LIR wordt gekozen ligt het voor de hand om deze rol te beleggen bij Logius. Logius is momenteel beheerder van het Rijks IPv6-nummerplan en heeft onder meer daardoor de benodigde kennis in huis voor het beheer en de uitvoering van het kader. Daarnaast is Logius de beheerder van meerdere overheidsvoorzieningen en is daardoor in staat de samenhang tussen het plan en de voorzieningen te bewaken.

In Figuur 10 wordt weergegeven hoe het IPv6 aanvraagproces er momenteel uitziet. De groene lijn geeft aan welke uitgifterelatie blijft bestaan indien er één overheids-LIR zou komen en dit Logius zou zijn. De rode relaties vervallen.



Figuur 10: Visualisatie van het element LIR-schap: bij welke LIR vraagt een overheidsorganisatie haar IPv6-adressen aan. De pijlen geven de aanvraagrichting aan.

5.3 Element 3: IPv6 uitgiftebeleid binnen de overheid

5.3.1 Toelichting element 3

Indien de overheid beschikt over een eigen IPv6-adresblok dat door andere overheidsorganisaties kan worden gebruikt, dan moet er structuur worden aangebracht in dit adresblok. Dit gebeurt door middel van het IPv6-uitgiftebeleid.

De omvang van het IPv6-adresblok dat een overheidsorganisatie krijgt toegewezen hangt af van het aantal systemen en netwerken dat moet worden voorzien van IPv6-adressen. Een LIR kan bij RIPE NCC zonder verdere rechtvaardiging een /29 gealloceerd krijgen. Dat was in het verleden een kleiner blok, namelijk een /32. Voor standaardbedrijfsomgevingen wordt standaard met /48 gerekend, tenzij kan worden aangetoond dat meer ruimte nodig is.

5.3.2 Voorkeursinrichting element 3

> Gebruik bij het overheids-IPv6-uitgiftebeleid de conventies van RIPE-beleid. Werk met standaard /32 of /48 per organisatie, tenzij meer nodig is. Routeer nooit kleiner dan /48 naar internet.

De geïnterviewde leveranciers verwachten hiervoor geen probleem. In het interview met Duitsland kwam naar voren dat zij alle risico's willen uitsluiten en overwegen om verdere maatregelen te nemen om /48 te allen tijde routeerbaar te houden, ook als bepaalde upstream providers op Internet dit niet doen. De aanbeveling is om deze ontwikkeling bij vaststelling van het nummerplankader in de gaten te houden.

> Houd ruimte over bij het uitdelen van IPv6-adresblokken aan overheidsorganisaties, zodat bij uitbreiding in de toekomst het adresblok kan worden vergroot.

Een LIR moet bepaalde activiteiten uitvoeren richting de organisaties die IP adressen toegewezen krijgen. Zo moeten de adressen worden goedgekeurd door en worden geregistreerd bij RIPE NCC. De LIR Logius zal als onderdeel van het uitgiftebeleid de adresaanvragen van overheidsorganisaties goed moeten keuren.

5.4 Element 4: Zonering binnen overheidsorganisaties

5.4.1 Toelichting element 4

Organisaties die gebruik maken van IPv6-adresreeksen uit het overheidseigen IPv6-adresblok kunnen nog aanvullende afspraken maken over het gebruik van de adressen. Zo kunnen afspraken gemaakt worden over:

- De verdeling van de nummers over deelorganisaties, netwerken en systemen,

- Het reserveren van een blok voor bepaalde doeleinden, bijvoorbeeld voor vertrouwelijke netwerken,
- Het vastleggen van deze afspraken, bijvoorbeeld in een nummerplan.

5.4.2 Voorkeursinrichting element 4

> Adviseer organisaties om structuur aan te brengen in hun IPv6-nummerplan.

Overheidsorganisaties brengen zelf structuur aan in hun nummerplan, zoals verder staat beschreven in element 5. Op het moment dat wordt voorzien dat overheidsorganisaties in de toekomst vertrouwelijke netwerken willen koppelen, dan kunnen organisaties hier zelf in het opstellen van het IPv6-nummerplan rekening mee te houden. Het reserveren van een aparte prefix voor diensten in vertrouwelijke netwerken kan hierbij helpen.

Het is aan te raden om clients maar van één IP-adres te voorzien dat gebruikt wordt voor alle communicatie. Indien een client zowel gekoppeld is via internet als een besloten netwerk dan zal het daarvoor hetzelfde adres uit de overheidsreeks gebruiken.

Deze afspraken moeten vastgelegd worden in de IPv6-nummerplannen van de betreffende organisaties. Een dergelijk plan per organisatie brengt structuur aan en houdt het beheer behapbaar.

5.5 Element 5: Overige afspraken over IPv6-nummerplannen

5.5.1 Toelichting element 5

Er zijn verschillende keuzes die organisaties kunnen maken aangaande het opstellen van hun eigen IPv6-nummerplan. Hier zouden in een overheidsbreed IPv6-nummerplankader richtlijnen voor opgenomen kunnen worden. Het kan dan gaan over het gebruik van bepaalde typen IPv6-adressen en subnetverdelingen.

5.5.2 Voorkeursinrichting element 5

> Iedere overheidsorganisatie dient te beschikken over een goed leesbaar IPv6-nummerplan, waarbij best practices (zoals weergegeven in bijvoorbeeld dit rapport en in het Rijksnummerplan) in beschouwing zijn genomen.

Bij het inrichten van een nummerplan moeten organisaties ervoor zorgen dat zij hun subnetindeling zo onafhankelijk mogelijk van organisatorische veranderingen maken waardoor het aantal wijzigingen in het nummerplan in de toekomst beperkt

kan blijven. Ook het hanteren van ruimte in het plan waar mogelijk draagt hier aan bij. Daarnaast verkleint het hebben van een gestructureerd overzichtelijk IPv6-nummerplan de kans op configuratiefouten in IPv6-netwerken en –diensten.

Het gebruik van IPv6-adressen uit een overheidsadresblok neemt niet alle aanleidingen voor omnummeren weg. Door configuraties zoveel mogelijk IPv6-adres onafhankelijk te maken (door bijvoorbeeld geen hardgecodeerde IP-adressen in applicaties te gebruiken) en te werken met dynamische configuratie technieken kan de omnummerlast worden beperkt.

5.6 Besturing, uitvoering en financiering van het IPv6-nummerplankader

In de voorgaande paragraaf is een voorstel voor een centraal landelijk IPv6-nummerplankader beschreven, met daarin een beperkte set afspraken en een aantal adviezen. In deze paragraaf beschrijven we op welke wijze de governance van het IPv6-nummerplankader geregeld kan worden, hoe het beheer en de uitvoering van het nummerplankader georganiseerd kan worden en tenslotte gaan we in op de financieringsmogelijkheden. Besluitvorming over besturing van het nummerplankader is nadrukkelijk gescheiden van de uitvoering van de afspraken in het kader.

5.6.1 Governance van het IPv6-nummerplankader

Indien wordt gekozen om het nummerplankader op centraal niveau op te stellen dan is het advies om de besturing van de besluitvorming over de wenselijkheid en de inhoud van het kader onderdeel te maken van de Generieke Digitale Infrastructuur (GDI) en daarmee ook onderhavig te maken aan de governancestructuur van de GDI.

Deze structuur kent naast de Ministeriële Commissie Digitale Overheid (MCDO) op het politieke niveau en het Nationaal Beraad op bestuurlijk niveau, ook een aantal regieraden op strategisch niveau. Gelet op de huidige indeling van de GDI lijkt het cluster Interconnectiviteit (en daarmee de Regieraad Interconnectiviteit) de aangewezen plaats voor het onderbrengen van een nummerplankader.

In de Regieraad zijn verschillende vertegenwoordigers van afnemers, beheerders, leveranciers, opdrachtgevers en beleidsverantwoordelijken opgenomen. Besluitvorming met betrekking tot het overheidsbrede IPv6-nummerplankader kan centraal via de Regieraad Interconnectiviteit georganiseerd worden. Voor technisch-inhoudelijke discussies over het nummerplankader kan een centrale IPv6-werkgroep in het leven worden geroepen. Via deze centrale IPv6-werkgroep kunnen dan ook de stakeholders betrokken worden die relevant zijn voor de technisch-inhoudelijke afspraken.

Maak het kader onderdeel van de GDI en daarmee de besluitvorming over de wenselijkheid en inhoud van het kader onderhavig aan de daarvoor geldende governancestructuur.

Naast het beleggen van de besluitvorming bij dit orgaan kunnen verschillende partijen zelfstandig beslissen om sectoraal of regionaal verdere invulling te geven aan het kader. Het voorgestelde kader biedt namelijk ruimte voor het maken van verdere afspraken binnen sectoren. Een voorbeeld hiervan zijn eventuele afspraken tussen decentrale overheden onderling over het gebruik van specifieke adresblokken voor onderlinge samenwerking. In de centrale IPv6-werkgroep worden dan de hoofdafspraken gemaakt die leidend zijn voor de afspraken die op sectoraal of regionaal niveau gemaakt worden.

Voor het afstemmen van deze afspraken kunnen aparte IPv6-werkgroepen bij de sectorale koepelorganisaties of regionale samenwerkingsverbanden worden opgezet of dit kan plaatsvinden in bestaande technische-inhoudelijke werkgroepen. De werkgroepen bereiden de afspraken voor en deze worden binnen de koepelorganisaties of samenwerkingsverbanden vastgesteld. Indien er een centrale LIR komt kan deze informatie daar samenkomen en kan vanuit de centrale LIR gerapporteerd worden aan het centrale besturingsorgaan, zoals de Regieraad Interconnectiviteit van de MCDO.

Geef sectoren en regionale samenwerkingsverbanden de vrijheid om onderling verdergaande afspraken te maken ter verdere invulling van het overheidsbrede kader. Zorg er via de centrale LIR voor dat deze afspraken binnen het overheidsbrede kader passen.

Om de voordelen van het voorgestelde nummerplankader te behalen is het van belang dat overheidsorganisaties er aan mee doen. De vraag is op welke manier individuele partijen gestimuleerd kunnen worden om het nummerplankader te adopteren. Indien het nummerplankader dwingend wordt opgelegd, dan vraagt dit ook om toezicht en handhaving. Toezicht en handhaving brengen grote kosten met zich mee. Of deze kosten in verhouding staan tot de beoogde voordelen van het kader hangt mede af van bepaalde strategische keuzes die de Nederlandse overheid maakt, bijvoorbeeld met betrekking tot leveranciersonafhankelijkheid, informatiebeveiliging en het gebruik van besloten netwerken voor communicatie tussen overheden.

Los van het dwingend opleggen van de afspraken uit het nummerplankader, is een aantal maatregelen denkbaar die het gebruik van het nummerplankader wel verder kunnen stimuleren:

- Het maken van afspraken met generieke e-overheidsvoorzieningen over het gebruik van het kader. Via deze voorzieningen kan het gebruik bij overige partijen worden gestimuleerd.
- Het opnemen van het kader in de bestaande referentiearchitecturen, zoals NORA[49], GEMMA[50] etc.
- Het opnemen van het kader in de pas-toe-of-leg-uit-lijst van het College Standaardisatie (dat binnenkort op zal gaan in het Nationaal Beraad[51]) als

[49] Nederlandse Overheid Referentie Architectuur (NORA), http://www.e-overheid.nl/onderwerpen/over-de-e-overheid/architectuur/nora-familie/nora
[50] GEMeentelijke Model Architectuur (GEMMA), https://www.kinggemeenten.nl/secties/gemma/gemma

extra aanbeveling bij het gebruik van de IPv6-standaard die momenteel al op de lijst staat.

De meer strategische overwegingen, dan wel het maken van het afspraken hierover, horen ook thuis in de governancestructuur van de GDI.

Zorg ervoor dat het nummerplankader wordt gebruikt door de bestaande voorzieningen, referentiearchitecturen en als aanbeveling op de pas-toe-of-leg-uit lijst. Laat het waar mogelijk aansluiten bij andere discussies aangaande overheidscommunicatie, bijvoorbeeld over besloten netwerken en overheidscloud-initiatieven. Dit hoort thuis in de governancestructuur van de GDI.

5.6.2 Uitvoering van het IPv6-nummerplankader

In deze paragraaf beschrijven we de taken die belegd worden bij de centrale partij die het nummerplankader uitvoert en onderhoudt.

Onder de uitvoering van het nummerplankader vallen in ieder geval de volgende taken:

- Aanvragen, registreren, indelen en toewijzen van adresblokken.
- Helpdesk voor gebruikers van adresblokken met bijvoorbeeld aanvraagondersteuning.
- Evalueren en controleren van IPv6-nummerplannen van gebruikers.
- Afstemming met overige belanghebbenden bij de registratie van de nummers, bijvoorbeeld met het Nationaal Respons Netwerk in het kader van cybersecurity-incidentbeheer.

Onder het onderhoud van het kader verstaan we in dit geval minimaal de volgende aspecten:

- Doorvoeren van wijzigingen in het kader volgens een wijzigingsprotocol
- Publicatie, disseminatie en communicatie van het nummerplankader
- Afstemming met eventuele collega beheerorganisaties

In theorie kunnen deze taken bij verschillende partijen belegd worden. In de praktijk is het handig deze kennis te bundelen bij één partij. Daarnaast is het goed denkbaar dat voor een aantal taken afspraken gemaakt worden met overige partijen. Zo kan de centrale beheerder van het kader afspraken maken met bijvoorbeeld sectorale koepels over de communicatie over het gebruik van het kader.

[51] https://www.forumstandaardisatie.nl/actueel/item/titel/college-standaardisatie-draagt-taken-over-aan-nationaal-beraad-digitale-overheid/

Beleg de uitvoering en het onderhoud van het nummerplankader bij één landelijk centrale partij. Laat deze partij afspraken maken met overige partijen over de disseminatie van het nummerplan.

Daarnaast kan overwogen worden nog een aantal extra taken bij de centrale beheerder van het kader te beleggen. Zo kan gedacht worden aan:

- Inrichting van een kennisbank voor gebruikers.
- Ondersteuning bij het opstellen van nummerplannen door overheden.
- Duidelijk zichtbaar maken en actief uitdragen van meerwaarde van gezamenlijke aanpak voor individuele overheidsorganisaties.

Overweeg of het wenselijk is om ook overige taken ter ondersteuning van overheden bij de invoering van IPv6 bij de centrale beheerder te beleggen.

5.6.3 Financiering van het IPv6-nummerplankader

De financiering van het nummerplankader en het bijbehorende beheer is sterk afhankelijk van het niveau waarop de besluitvorming over nummerplankader en het beheer worden georganiseerd. Voor de financiering bestaan op hoofdlijnen twee opties:

- Centrale financiering, waarbinnen nog de vraag moet worden gesteld op welke wijze deze centrale “pot” wordt gevuld.
- Versleuteling van de kosten over de deelnemende organisaties. Het gaat dan om een toepassing van het profijtbeginsel.

Gelet op het advies om dit kader onderdeel te maken van de Generieke Digitale Infrastructuur ligt het voor de hand de financiering van het kader mee te nemen in de financiering van de GDI. De afspraken hieromtrent worden ten tijde van het schrijven van dit rapport nog nader uitgewerkt door de Digicommissaris.

Aanvullende afspraken, bijvoorbeeld op sectoraal niveau zullen ook vragen om aanvullende afspraken over de financiering van het beheer van die afspraken. Daarbij is het aan te bevelen te kiezen voor een systeem van centrale financiering. De hoofdoverweging hierbij zijn de relatief beperkte kosten per deelnemende partij en de relatief grote administratieve lasten die versleuteling van de kosten over de partijen met zich mee brengt.

Regel de financiering van het beheer van het nummerplankader structureel door deze mee te nemen in de financiering van de GDI.

6 Conclusies en aanbevelingen

Dit hoofdstuk beschrijft de conclusies en aanbevelingen van het onderzoek. De antwoorden op de onderzoeksvragen en de gepresenteerde conclusies hebben betrekking op IPv6-netwerken en -diensten en niet op IPv4-netwerken en -diensten.

1. In hoeverre en onder welke voorwaarden kan IPv6-nummerplanbeleid voor de Nederlandse Overheid tot kansen voor leveranciersonafhankelijkheid, informatieveiligheid, financieel voordeel en eventuele overige baten leiden, rekening houden met het organisatorische en bestuurlijke landschap?

Leidt het tot grotere leveranciersonafhankelijkheid?
Een IPv6-nummerplankader kan bijdragen aan het vergroten van leveranciersonafhankelijkheid. Daarvoor is vooral het in eigen beheer hebben van IPv6-adressen door overheden van belang. Bij overheden die de nummers niet in eigen beheer hebben kunnen de kosten voor omnummeren een leverancierswissel tegenhouden. Naast de kosten voor omnummeren spelen ook andere zaken dan deze kosten een rol. Daarnaast geven eigen overheidsnummers de mogelijkheid om netwerken en diensten via verschillende leveranciers op internet aan te sluiten.

Leidt het tot betere informatieveiligheid?
Het in eigen beheer hebben IPv6-adressen biedt overheden de mogelijkheid hun adressen op internet te certificeren en op die manier misbruik moeilijker te maken, in plaats van dat leveranciers dit voor de overheid doen. Daarnaast kan het hebben van een overheidsbreed IPv6-nummerplankader door het realiseren van structuur en herkenbaarheid bijdragen aan het onderscheiden van overheidsverkeer van niet-overheidsverkeer, om bijvoorbeeld misbruik te kunnen signaleren en beveiligingsregels eenvoudiger te kunnen configureren. Het gaat hier met name om het eenvoudiger maken van het administreren welke adressen door overheden in gebruik zijn.

Leidt het tot financieel voordeel?
Het gebruik van eigen overheidsadressen kan kostenvoordelen met zich meebrengen als daardoor een significant aantal omnummeractiviteiten kan worden voorkomen. Het aantal omnummeractiviteiten dat wordt voorkomen hangt af van het aantal IP-specifieke configuraties die moeten worden aangepast op andere plekken binnen de overheid en overheidsdiensten als gevolg van een leverancierswissel van één netwerk of dienst.

Leidt het tot overige baten?
Structuur aanbrengen in IPv6-nummerplannen in het algemeen is een goed idee, om een goed beheersbare IPv6 infrastructuur te realiseren bij overheidsorganisaties en deze toekomstvast in te richten. Daarnaast kan met overheidsadressen uit één overheidsadresreeks het beheer van koppelingen en routes tussen overheden eenvoudiger worden gemaakt.

2. Op welke wijze kan een overheidsbreed IPv6-nummerplan bestuurlijk ingericht worden, mede in relatie tot de Generieke Digitale Infrastructuur?
Het verdient de aanbeveling een overheidsbreed IPv6-nummerplankader onderdeel te laten zijn van de Generieke Digitale Infrastructuur (GDI), meer specifiek het

onderdeel Interconnectiviteit. Daartoe kan een verzoek ingebracht worden bij de Digicommissaris. De bestuurlijke verantwoordelijkheid voor het kader komt dan te liggen bij het Nationaal Beraad en de Ministeriële Commissie Digitale Overheid (MCDO). De invoering van een overheidsbreed IPv6-nummerplan relateert aan strategisch vraagstukken bij de overheden aangaande leveranciersonafhankelijkheid en informatiebeveiliging. Het verdient de aanbeveling bij discussies hieromtrent aan te sluiten, bijvoorbeeld de discussie aangaande besloten overheidsnetwerken.

3. Op welke wijze kan een overheidsbreed IPv6-nummerplankader het beste ingericht worden?
In de kern behelst het nummerplankader het gebruik van overheidseigen IPv6-adresblokken. Dit wordt gefaciliteerd door centraal één overheids-IPv6-blok aan te vragen door een centrale overheids-Local Internet Registry (LIR). Deze LIR wijst adresblokken toe aan overheidsorganisaties volgens de internationale standaardvoorschriften. Verder worden afspraken gemaakt aangaande het gebruik van adresblokken voor overheidskoppelingen en moet iedere overheidsorganisatie over IPv6-nummerplan beschikken. Clients in overheidsnetwerken gebruiken hierbij één globaal uniek IPv6-adres uit de overheidsreeks.

4. Op welke wijze kan het registratieproces en administratieve inrichting gezien de autonomie van de overheden en hun decentrale karakter het beste georganiseerd worden?
Een centrale overheids-LIR voert de taken uit die een reguliere LIR ook uit zou voeren, namelijk de verplichte taken richting RIPE NCC en het afhandelen van IPv6 aanvragen vanuit overheidsorganisaties. Voor individuele overheidsorganisaties verandert er weinig. Waar ze voorheen nummers kregen van RIPE NCC of via hun leverancier kunnen ze die in de toekomst aanvragen bij een centrale overheids-LIR.

5. Op welke wijze kan het nummerplankader het beste op strategisch, tactisch en operationeel niveau onderhouden worden?
De (strategische) besluitvorming over de wenselijkheid en inhoud van het nummerplankader hoort thuis in de governancestructuur van de GDI, als onderdeel van de MCDO. Hierdoor ontstaat oplijning met de overige onderdelen van de GDI waar dat nodig is. Besluitvorming over eventuele wijzigingen in het kader (tactische besluitvorming) dient ook ondergebracht te worden in de governancestructuur van de GDI. De uitvoering en het onderhoud van het kader (operationeel beheer) dient belegd te worden bij een centrale beheerder, de centrale LIR. In het voorgestelde IPv6 nummerplankader is deze rol bij Logius belegd.

6. Op welke wijze kan de inbedding en implementatie bij alle relevante organisaties georganiseerd worden?
Op basis van dit onderzoek is deelname van overheden aan het kader niet verplicht, maar wel een streven. Om dit streven na te jagen is het van belang ervoor te zorgen dat het kader wordt gebruikt door de bestaande voorzieningen, referentiearchitecturen en als aanbeveling op de pas-toe-of-leg-uit lijst. Daarnaast kan de centrale LIR afspraken maken met sectorale koepelorganisaties om disseminatie van het kader te bevorderen.

7. Welke wijze van financiering is gezien de voorgaande vragen het meest geëigend?

Gelet op het advies om de governance van het kader bij de MCDO onder te brengen is het logisch om ook de financiering van het kader structureel te regelen door deze mee te nemen in de financiering van de GDI.

Nederlandse overheden introduceren de komende jaren IPv6 in hun ICT-omgeving. Daarmee ontstaat een kans om vooraf gezamenlijk een aantal afspraken te maken over het gebruik van die adressen. Op basis van dit onderzoek blijkt dat een beperkte set afspraken een bijdrage levert aan leveranciersonafhankelijkheid, informatieveiligheid en efficiënt beheer van de ICT infrastructuur. Het in dit rapport voorgestelde IPv6-nummerplankader dient als startpunt voor een overheidsbreed IPv6-nummerplankader, dat nog definitief vastgesteld zal moeten worden. Bij het opstellen van het definitieve IPv6 nummerplankader is het van belang om dit gezamenlijk met (technische) stakeholders van decentrale overheden te doen. We bevelen aan om discussies aangaande de technische implementatie van een overheidsbreed IPv6-nummerplan die spelen in onder meer Duitsland en Spanje te volgen, omdat ook daar nog niet alles is uitgekristalliseerd, en om aansluiting te zoeken bij meer strategische discussies binnen de Nederlandse overheid over het gebruik van besloten netwerken en leveranciersonafhankelijkheid in het kader van informatiebeveiliging. De toegevoegde waarde van een IPv6-nummerplankader neemt sterk toe wanneer het ingezet wordt in combinatie met overige maatregelen gericht op het realiseren van dergelijke strategische doelen.

Het verdient de aanbeveling om de invoering van het IPv6-nummerplankader gelijk te laten lopen met momenten waarop overheidsorganisaties IPv6 introduceren in bepaalde netwerken of diensten, bijvoorbeeld bij aanbestedingen op het gebied van ICT. Deze invoering is van belang, omdat dan zal blijken of overheidsorganisaties daadwerkelijk het kader opvolgen en eventuele nieuwe aandachtspunten aan het licht komen.

Tot slot helpt de invoering van dit IPv6-nummerplankader overheden om na te denken over de tijdige invoering van IPv6 en de wijze waarop ze dit doen door aandacht te vestigen op het onderwerp. Bij sommige overheden zal kennis over de invoering van IPv6 in huis aanwezig zijn, maar voor andere overheden kan de invoering een uitdaging vormen. Overweeg daarom of het wenselijk is om ook andere taken ter ondersteuning van overheden bij de invoering van IPv6 bij de centrale beheerder te beleggen.

7 Ondertekening

Den Haag, 3 april 2015

Dhr. ir. F.H. Klok
Afdelingshoofd

Dhr. ir. A.C.G. Holtzer
Auteur

A Rekenvoorbeeld omnummerimpact Nederlandse overheid

In Hoofdstuk 4.1 wordt gesproken voor de kosten voor omnummeren. Tijdens dit onderzoek zijn de relevante gegevens om een kosteninschatting vanuit de overheid niet beschikbaar voor het onderzoeksteam. Echter, op basis van het in kaart brengen van de relevante factoren en enkele aannames, wordt in deze bijlage een voorbeeldberekening gegeven.

Deze voorbeeldberekening geeft een inschatting van het aantal omnummeractiviteiten dat op jaarbasis nodig is en kan een indicatie geven voor de omnummerkosten die de Nederlandse overheid, direct of via leveranciers die deze activiteiten voor de overheid uitvoeren, jaarlijks als geheel maakt ten gevolge van een wissel van connectiviteitleverancier.

De berekening berekent de kosten voor omnummeren op basis van:
- het aantal omnummeractiviteiten dat moeten worden uitgevoerd als gevolg van een leverancierswissel ergens bij de overheid;
- het aantal leverancierswissel dat op jaarbasis bij overheidsorganisaties gezamenlijk plaatsvindt.

De omnummeractiviteiten staan beschreven in Tabel 3. Hierbij is het van belang de volgende parameters in te schatten:
- Het aantal overheidsorganisaties dat overheidsdiensten raadpleegt (500);
- Het aantal overheidsdiensten dat wordt geraadpleegd;
- Het gemiddeld aantal koppelingen dat een overheidsorganisatie heeft naar overheidsdiensten, via internet en via een besloten netwerk;
- Het gemiddeld aantal koppelingen dat een overheidsdienst gemiddeld heeft naar overheidsorganisaties (via internet en via een besloten netwerk);
- Het percentage van deze koppelingen dat te maken heeft met IP-specifieke configuratie in netwerken of diensten;
- Het percentage overheden en diensten dat IP-adressen van de leverancier gebruikt;
- Het aantal aanbestedingen per jaar waar in potentie een leverancierswissel zou kunnen plaatsvinden;
- Het percentage aanbestedingen per jaar waar ook daadwerkelijk een leverancierswissel plaatsvindt;
- De gemiddelde kosten voor het omnummeren van een koppeling (netwerk, firewall en applicatieconfiguraties).

De kosten kunnen worden berekend voor elk van de vier kwadranten in Tabel 3:
- Omnummerkosten ten gevolge van een prefixwijziging in een clientorganisatie op koppelingen die via Internet lopen;
- Omnummerkosten ten gevolge van een prefixwijziging in een clientorganisatie op koppelingen die via een besloten netwerk lopen;
- Omnummerkosten ten gevolge van een prefixwijziging in een overheidsdienst op koppelingen die via Internet lopen;

- Omnummerkosten ten gevolge van een prefixwijziging in een overheidsdienst op koppelingen die via een besloten netwerk lopen.

Als rekenvoorbeeld voor de inschatting van het aantal relevante leverancierswisselingen per jaar maken we de volgende aannames[52]:

- Er zijn rond de 500 overheidsorganisaties die IPv6-nummerblokken toegekend hebben gekregen.
- We schatten in voor koppelingen naar internet organisaties onderling samenwerken (bijvoorbeeld via shared service centers), waardoor het totaal aantal internetkoppelingen dat door Nederlandse overheden gebruikt wordt ongeveer de helft is van die 500, dus zo'n 250 internetkoppelingen.
- We gaan er vooralsnog vanuit dat een zeer hoog percentage hiervan, zeg 90%, op dit moment niet over eigen IPv6-adressen beschikt en, indien zij IPv6 gebruiken in hun netwerk of diensten, hiervoor gebruik maakt van IPv6-adressen van de leverancier. Verreweg de meeste overheidsorganisaties zijn namelijk geen LIR (in maart 2014 waren er 18 overheids-LIR's[53]) en zijn niet aangesloten bij een shared service center dat LIR is.
- De overheidsorganisaties zijn een combinatie van grotere en kleinere afnemers van overheid connectiviteitdiensten; we veronderstellen dat ze via het besloten netwerk gemiddeld gebruik maken van zo'n 10 overheidsdiensten (connecties naar 10 server clusters).
- Ook voor het gemiddelde aantal overheid connectiviteitdiensten waarmee een organisatie verbonden is via internet nemen we aan dat dit ongeveer 10 betreft.
- Voor het aantal keer per jaar dat een overheidsorganisatie overweegt om van leverancier te wisselen nemen we als basis een gangbare contractduur voor connectiviteitdiensten van vier jaar. Dit komt dus neer op een heroverweging van de leverancier van een kwart, per connectiviteitdienst per jaar.
- Verder nemen we op basis van een beperkt aantal recente aanbestedingen van connectiviteitdiensten aan dat in minder dan de helft van de gevallen, zeg 35%, bij een nieuwe aanbesteding ook daadwerkelijk van leverancier gewisseld wordt.

Het tweede deel van de omnummerkosteninschatting betreft de benodigde middelen en kosten voor elk van de vier typen connectiviteit. Hierbij lijkt vooral de mensinzet voor de omnummeracties een kostendriver. Voor deze inschatting gebruiken we de volgende aannamen:

- Een gangbaar bruto uurtarief over voor het uitvoeren van specialistische IPv6 herconfiguratie activiteiten uit [bron: "Coördinatiekosten inrichting IPv6-plan Overheid", Logius, 14 november 2013]: 150 euro per uur.
- Voor de benodigde, gemiddelde tijdsinschatting voor uitvoering van de activiteiten weergegeven in Tabel 3 dient opgemerkt te worden dat er bepaalde acties zijn die dominante zijn, met name: (a) client zijde netwerkprefx wijzigingen die aanpassing vergen aan de toegangsregels van al de server-zijden die de client gebruikt en (b) server zijde netwerkprefix

[52] Dit is een voorbeeldberekening. Voor een definitieve berekening dienen de aannames en hier gebruikte getallen geverifieerd te worden bij verschillende overheidsorganisaties.
[53] www.ripe.net/membership/indices/NL.html

wijzigingen waarvoor elke client die er gebruik van maakt (eventuele hardgecodeerde) IP-adressen van B in haar systemen moet wijzigen.

a. De ureninschatting per client zijde netwerkprefix wijziging is 4 uur voor toegangsregelaanpassing (mede gebaseerd op de inschattingen in[54]) voor elk van de 10 overheidsdiensten waar de client gebruik van maakt ⇔ 40 uur per clientzijde netwerkprefix wijziging.
b. Per server zijde wijziging schatten we 16 uur in voor adreswijzigingen voor elk van de 500 clients die er gebruik van maken ⇔ 8000 uur.

Deze omnummerkosteninschattingen bij elkaar leiden tot de volgende jaarlijkse omnummerkosten die *de Nederlandse overheid als geheel* maakt ten gevolge van het wisselen van connectiviteitleverancier:

	Client (A) verandert netwerkprefix	Server (B) verandert netwerkprefix
A communiceert met B via besloten overheidsnetwerk	(500*90%*1/4*40%) * (10*4*€150) ≈ **k€270**	(10*1/4*40%) * (500*16*€150) ≈ **k€1.200**
A communiceert met B via Internet	(250*1/4*40%) * (10*4*€150) ≈ **k€150**	Nader te bepalen

In totaal komt deze omnummerkostenraming t.g.v. leverancierswissel neer op ongeveer twee miljoen euro per jaar, voor de overheid als geheel.

[54] Bron: “Coördinatiekosten inrichting IPv6-plan Overheid”, Logius, 14 november 2013