dialogic
innovatie • interactie

Mogelijkheden voor identificatie op internet op basis van IP-adres

Projectnummer:
2018.115

Publicatienummer
2018.115-1907 v1.0.1

Datum:
Utrecht, 18 oktober 2019

Auteurs:
Ir. Tommy van der Vorst
Jessica Steur MSc
Ir. Nick Jelicic
Ir. Jan van Rees

De begeleidingscommissie van dit onderzoek bestond uit de volgende leden:

- Prof.dr.ir. J. (Jan) van den Berg (TU Delft; voorzitter)
- Prof. dr. N.A.N.M. (Nico) van Eijk (UvA)
- Drs. T.L. (Theo) van Mullekom (WODC; opdrachtgever)
- Mr. drs. J. (Jan) Dobbelaar (Ministerie van Justitie en Veiligheid; aanvrager)

De onderzoekers danken de leden van de begeleidingscommissie voor hun bijdragen en prettige samenwerking.

Inhoudsopgave

Begrippenlijst

464XLAT	Het IPv4-verkeer wordt aan zijde van de gebruiker vertaald naar IPv6-pakketten en aan de zijde van de ISP weer terugvertaald naar IPv4-pakketten. 464XLAT is ontworpen voor mobiele aansluitingen.
Aansluit-netwerk	Het netwerk of het deel van een netwerk dat toegang geeft tot een telecommunicatiedienst. Dit zijn de netwerken waarop consumemten en bedrijven een aansluiting kunnen krijgen.
APN	*Access Point Name*. Naam waarmee op een mobiel apparaat wordt aangegeven op welke manier (en waarmee, meestal het openbare internet) een dataverbinding wordt opgezet.
CG-NAT	*Carrier Grade NAT*. Hierbij wordt NAT (zie elders in de begrippenlijst) toegepast door de ISP. NAT kan ook op andere plaatsen (bijvoorbeeld door een eindgebruiker) worden toegepast.
CIOT	Het *Centraal Informatiepunt Onderzoek Telecommunicatie* beheert een informatiesysteem voor telefoon- en internetgegevens voor de identificatie van personen ten behoeve van de opsporing, vervolging en onderzoeken in het kader van de nationale veiligheid. Zie voor meer informatie [1].
CPE	*Customers Premises Equiment.* Apparatuur op locatie van afnemers van telecomdiensten om deze dienst te kunnen afnemen: kabelmodems, ADSL-modems, et cetera.
Cross-referencing	Het aan elkaar koppelen van meerdere informatiebronnen door kruisverbanden te leggen tussen deze bronnen.
Dataretentie	Het door private organisaties (zoals een ISP of dienstverlener) opslaan van telefonie- en internetgegevens ten behoeve van opsporing, vervolging en onderzoeken in het kader van de nationale veiligheid.
Destination port	Getal dat aangeeft welke dienst op een server (computer die een of meerdere internetdiensten aanbiedt) wordt aangesproken.
DNS	*Domain Name System,* het systeem en netwerkprotocol dat op het internet gebruikt wordt om domeinnamen (www.website.nl) naar IP-adressen te vertalen en omgekeerd. Dit is nodig omdat verbindingen uitsluitend op basis van IP-adres kunnen worden opgebouwd.
DS-Lite	Techniek waarbij IPv4-verkeer wordt verpakt in IPv6-pakketten en aan de zijde van de ISP weer terugvertaald wordt naar IPv4-pakketten. DS-Lite wordt gebruikt voor vaste verbindingen en maakt het mogelijk om de verbinding tussen klant en ISP uitsluitend op basis van IPv6 te laten verlopen.
Dual-stack	Een IPv4- en een IPv6-aansluiting worden naast elkaar aangeboden over dezelfde verbinding.
IP-blok notatie met /XX	Met de '/'-notatie wordt aangegeven hoeveel IPv4-adressen een 'blok' van IPv4-adressen bevat. Het cijfer na de '/' geeft aan hoeveel bits van het IPv4-adres gereserveerd zijn voor het 'subnet'. Hoe lager het getal na de /, des te meer IPv4 adressen er in één blok beschikbaar zijn. Het aantal IPv4 adressen kan worden bepaald door $2^{32} - 2^{\text{getal na '/'}}$. Van dit getal dienen nog enkele (om technische redenen) niet-bruikbare adressen te worden afgetrokken. Een "/24"-blok bevat bijvoorbeeld 255 adressen waarvan er 254 bruikbaar zijn.
IPv4	*Internet Protocol versie 4*, de vierde versie van het internetprotocol (maar feitelijk de eerste wijdverspreide en vandaag de dag meest gangbare versie). Het internetprotocol vormt de basis voor adressering en uitwisseling van datapakketten op het internet.
IPv6	*Internet Protocol versie 6*, opvolger van IPv4. Biedt (naast enkele andere voordelen) met name veel langere (en daardoor veel meer) adressen.

ISP	Een *internet service provider,* ofwel internetaanbieder, is een organisatie die diensten levert op of via het internet.
LTE	*Long-Term Evolution*. Standaard voor mobiele netwerken die wordt gebruikt om '4G' te bieden.
M2M	*Machine to Machine* is een algemeen label dat gebruikt wordt om iedere technologie te omschrijven die verbonden devices in staat stelt om informatie uit te wisselen en acties uit te voeren zonder de handmatige assistentie van mensen. Dit maakt het de basis van het concept dat bekend staat als het Internet of Things (IoT).
MVNO	Een *mobile virtual network operator* is een bedrijf dat niet over een eigen vergunning voor gebruik van spectrum beschikt, maar onder eigen merknaam mobiele diensten verkoopt op basis van het netwerk van een of meerdere andere mobiele aanbieders.
NAT	*Network Address Translation* is een techniek waarbij netwerkadressen worden vertaald, zodat meerdere gebruikers/apparaten/applicaties van hetzelfde adres gebruik kunnen maken.
Pool	Een pool is een verzameling van IP-adressen.
Poortnummer	Nummer waarmee meerdere gelijktijdige verbindingen tussen dezelfde twee computers kunnen worden onderscheiden.
Publiek IP-adres	Een IP-adres dat vanaf alle locaties op het internet (in principe) bereikbaar is. Dit vereist dat het IP-adres slechts door één partij wordt gebruikt. Een privaat IP-adres mag worden hergebruikt op meerdere netwerken, maar werkt derhalve alleen binnen privénetwerken.
Router	Een router is een apparaat dat twee of meer verschillende computernetwerken aan elkaar verbindt, bijvoorbeeld het internet en een bedrijfsnetwerk, en datapakketten van het ene naar het andere netwerk overbrengt.
Source port	Het poortnummer dat de computer die een verbinding opzet, gebruikt om de verbinding te kunnen onderscheiden van andere verbindingen met dezelfde bestemmingscomputer. Vaak een willekeurig gekozen nummer.
TCP-verbinding	Transmission Control Protocol, is een verbindingsgeoriënteerd protocol (afspraak over communicatiewijze) dat veel gebruikt wordt voor gegevensoverdracht over netwerkverbindingen op het internet en op computernetwerken.
Vaste netwerk	Vaste infrastructuur ten behoeve van internetcommunicatie in ons land. Denk hierbij aan glasvezelkabels, draadloze verbindingen, het kabelnetwerk ('de televisiekabel'), het kopernetwerk ('het telefonienetwerk') en zaken als mobiele opstelpunten en straatkasten.

Managementsamenvatting

Onderzoeksvraag

In het kader van de voorgenomen wetgeving omtrent de introductie van een beperkte bewaarplicht van telecommunicatiegegevens voor opsporing en vervolging is onderzocht hoe identificatie van individuele gebruikers op basis van een publiek IP-adres technisch te realiseren is. De vraagstelling van het onderzoek luidde:

> *Hoe kunnen (mobiele) internetaanbieders, tot twaalf maanden na het gebruik, een individuele gebruiker van een publiek IP-adres identificeren, ten behoeve van opsporing en vervolging, en wat zijn relevante (maatschappelijke) afwegingen daarbij?*

Wanneer het gaat om relevante maatschappelijke afwegingen onderscheiden we (1) bruikbaarheid voor opsporing en vervolging, (2) privacy van burgers, en (3) kosten voor de internetaanbieders. Voor het beantwoorden van de onderzoeksvraag zijn literatuuronderzoek en interviews (met mobiele internetaanbieders, politie, andere stakeholders/experts) ingezet. Op basis van de bevindingen zijn beleidsopties geformuleerd.

Achtergrond

Wanneer er een strafbaar feit plaatsvindt, maar dit niet op heterdaad wordt geconstateerd, moet de dader op basis van achtergelaten sporen worden gevonden, om uiteindelijk tot vervolging over te kunnen gaan. Om bijvoorbeeld de dader van een snelheidsovertreding te vinden, kunnen kentekens worden geregistreerd. Voor online criminaliteit geldt eenzelfde principe. Wanneer communicatie plaatsvindt op het internet is bij de ontvanger typisch het *IP-adres* van de afzender bekend – dit is immers nodig voor de communicatie in de tegengestelde richting. Dit IP-adres geeft daarmee een directe aanwijzing richting de aansluiting en/of het systeem vanaf waar een bepaalde strafbare handeling werd verricht. Het IP-adres wordt uitgegeven door een (mobiele) internetaanbieder. IP-adressen worden toegekend door internetaanbieders (ISP's). Opsporingsdiensten kunnen internetaanbieders verzoeken bekend te maken aan welke abonnee een bepaald IP-adres is uitgegeven.

Als gevolg van ontwikkelingen op het internet is de koppeling tussen individu en IP-adres niet meer zo evident als voorheen. Door de schaarste van IPv4-adressen (vierde versie van het internetprotocol), moeten de adressen worden gedeeld tussen abonnees. Dit kan door *dynamisch toewijzen*; abonnees delen hetzelfde IP-adres, maar nooit tegelijkertijd. Op basis van datum, tijd en publiek IP-adres is een individuele abonnee in dat geval nog steeds identificeerbaar. Deze situatie is vergelijkbaar met wanneer een bestuurder van een huurauto wordt gezocht op basis van kenteken: het kenteken behoort weliswaar tot het verhuurbedrijf, maar deze kan, op basis van de eigen administratie, de huurder achterhalen.

In situaties waarbij het aantal beschikbare IPv4-adressen *veel* kleiner is dan het aantal apparaten dat gelijktijdig online is, is het nodig IPv4-adressen *gelijktijdig* te delen tussen gebruikers. Dit is mogelijk door toepassing van *carrier grade network address translation* (CG-NAT). In de analogie met huurauto's betekent CG-NAT dat *verschillende* huurders landelijk in verschillende huurauto's rondrijden, maar allemaal met *hetzelfde* kenteken. Zodra de politie de bestuurder wil identificeren is, behalve datum en tijd, ofwel meer informatie over de auto nodig (bijvoorbeeld: de kleur en het type van de auto) ofwel over de route (wáár is de auto gesignaleerd, of wat was de bestemming?).

CG-NAT wordt op dit moment met name toegepast op mobiele netwerken. Afhankelijk van de operator wordt een publiek IP-adres gelijktijdig gedeeld met een handvol tot duizenden

andere abonnees. Aan alleen een IP-adres heeft de politie in geval van CG-NAT dan ook te weinig informatie om de voor opsporing relevante persoon te identificeren. Aanvullende informatie is derhalve nodig om deze groep personen te verkleinen.

Bevindingen

Huidige stand van zaken

De huidige stand van zaken is als volgt:

- Identificatie van abonneehouders op basis van IP-adres en datum/tijd is op Nederlandse vaste netwerken over het algemeen goed mogelijk.

- De mogelijkheden voor identificatie op basis van IP-adres verschillen sterk tussen de mobiele operators. Alleen in specifieke gevallen (afhankelijk van beschikbaarheid poortinformatie en de operator) kan tot één abonnee worden geïdentificeerd. In andere gevallen is de groepsgrootte tussen de 84 en 84.000 abonnees groot. Dit leidt tot problemen voor opsporingsinstanties.

Mogelijkheden tot verbetering

Om identificatie te verbeteren, zien we verschillende oplossingen. Deze verschillen netto nauwelijks in kosten voor de operators, maar wel sterk als het gaat om de bruikbaarheid voor opsporing en de mate van (mogelijke) privacyschending/juridische proportionaliteit van het bijhouden van informatie.

De meest voor de hand liggende oplossing om 1:1-identificatie te realiseren is uitrol van IPv6. De sector is het erover eens dat (om meer redenen dan identificatie alleen) uiteindelijk zal moeten worden gemigreerd naar IPv6. Er bestaat op dit moment echter nauwelijks een prikkel bij de Nederlandse mobiele internetproviders om dit te doen. Een enkele ISP heeft recent aangekondigd IPv6 te zullen uitrollen op haar netwerk. Mogelijk kan sterkere druk vanuit de overheid (als 'klant' van telecommunicatiediensten) een laatste zet in de juiste richting geven. Hoewel IPv6-adoptie enige tijd zal duren, en het IPv4-verkeer waarschijnlijk nooit volledig zal vervangen, leidt adoptie wel tot een lagere druk op CG-NAT, en daarmee ook tot verbeterde identificatiemogelijkheden op basis van een IPv4-adres.

Ook *zonder* IPv6 zou binnen enkele jaren identificatie tot een kleinere groepsgrootte realiseerbaar moeten zijn. We zien het toevoegen van IPv4-adressen als de meest eenvoudige oplossing. De ISP's lijken over afdoende IPv4-adressen te beschikken die zij zouden kunnen (her)inzetten op hun mobiele netwerk (naar schatting zo'n 4,2 miljoen in totaal). Wanneer voor alle abonnees CG-NAT wordt toegepast, leidt dit tot een groepsgrootte van circa vijf abonnees. Wanneer een ISP de eigen IPv4-adressen niet anders kan of wil inzetten, zou deze IPv4-adressen kunnen inkopen. Hierbij spelen (eenmalige) kosten en de vraag of deze IPv4-adressen in de gevraagde hoeveelheid beschikbaar zijn.

Een alternatieve oplossing is om de toewijzing van *source ports* aan abonnees te loggen. Hiermee is 1:1 identificatie mogelijk wanneer poortinformatie beschibkaar is bij opsporing. Dit is echter in een minderheid van de zaken het geval. Voor de overige zaken verbetert source port logging de situatie niet.

Een tweede alternatieve oplossing is om terug te keren naar een vorm van logging van verkeersgegevens, waarbij de gegevens worden gemaskeerd. Er is dan niet meer exact te achterhalen met wie een verbinding werd opgezet, maar het is wel mogelijk een (kleinere) groep abonnees te identificeren gegeven een bepaald IP-adres. Of deze oplossingsrichting voldoende verbetering biedt gegeven de te maken kosten, is echter twijfelachtig. De privacy-

inbreuk wordt (vanwege de kleinere groepsgrootte bij identificatie) enerzijds verlaagd, maar (afhankelijk van de invulling van het maskeren) verhoogd.

De volgende tabel toont een vergelijking van de verschillende mogelijkheden.

Mogelijkheid	Bruikbaarheid voor opsporing en vervolging	Hoeveelheid te bewaren persoonsgegevens	Mate van privacy-inbreuk bij opsporing (groepsgrootte)	Kosten voor de aanbieder
1. Het uitrollen en adopteren van IPv6	Hoog. Minder inspanning nodig voor identificatie. Mogelijk kunnen meer zaken worden opgepakt. Het zal echter even duren voordat ook alle diensten gebruik maken van IPv6. Tot die tijd zullen veel sporen IPv4 zijn en is er geen verbetering.	Minimaal. Informatie over (semi)statische toewijzing IPv6-adresblok aan abonnee (analoog aan IPv4 op vaste netwerken) naar datum/tijd.	Minimaal. Een IPv6-adres is altijd specifiek voor één abonnee/aansluiting. Andere abonnees kunnen direct worden uitgesloten.	Maximaal enkele miljoenen euro. Investering in IPv6 lijkt (ook om andere redenen dan opsporing) uiteindelijk onafwendbaar. Er zijn verschillen tussen operators voor wat betreft reeds gedane investeringen.
2. Vergroten van het aantal publieke IPv4-adressen	Gemiddeld tot hoog, afhankelijk van de groepsgrootte (maximaal bij 1:1-toewijzing). Een IPv4-adres leidt in de meeste gevallen direct tot identificatie. Meer sporen leiden tot identificatie en meer zaken kunnen worden opgepakt.	Beperkt. Informatie over (semi)statische toewijzing IPv4-adres aan abonnee (wordt reeds als zodanig bijgehouden op vaste netwerken)	Gemiddeld. Afhankelijk van de verhouding tussen het aantal publieke IPv4-adressen en het aantal abonnees. Wanneer er één adres per abonnee beschikbaar is, is de inbreuk minimaal. Groepsgroottes vanaf 15 zijn haalbaar.	Maximaal enkele miljoenen euro. Te besteden aan het aankopen van (schaarse) IPv4-adressen en het aanpassen van configuratie.
3. Source port logging	Beperkt, tenzij het bijhouden van informatie over bronpoorten bij dienstaanbieders toeneemt.	Beperkt. Informatie over toewijzing van publiek IPv4-adres en poortreeks aan abonnee naar datum/tijd. Aan de zijde van de dienstaanbieder moeten poortnummers worden gelogd.	Minimaal wanneer een bronpoortnummer, IP-adres, datum en tijd bekend zijn bij opsporing. In alle andere gevallen gemiddeld tot groot, afhankelijk van het aantal abonnees dat het publieke IPv4-adres deelt.	Maximaal enkele miljoenen euro. De informatie wordt nu al (kortstondig) bijgehouden om CG-NAT te laten functioneren. Investeringen zijn nodig om de data te loggen, op te slaan en toegankelijk te maken.
4. Verkeersgegevens gemaskeerd loggen	Gemiddeld tot hoog, afhankelijk van de groepsgrootte en vorm van maskering.	Hoog. Er moet per opgezette verbinding informatie worden opgeslagen. Hieruit is in beperkte mate af te leiden met wie werd gecommuniceerd.	Gemiddeld. Afhankelijk van de verhouding tussen het aantal publieke IPv4-adressen en het aantal abonnees en de wijze waarop wordt gemaskeerd.	Maximaal enkele miljoenen euro. Het betreft opslag van grote hoeveelheden data.
5. Verhogen werkhoeveelheid politie	Laag. Sommige zaken kunnen niet worden opgelost zonder identificatie via IP-adres. In andere zaken is een significante tijdsinvestering nodig om een groep terug te brengen tot één verdachte.	Minimaal. Informatie over (semi)statische toewijzing IPv4-adres aan abonnee (wordt reeds als zodanig bijgehouden op vaste netwerken). Een enkele mobiele ISP houdt daarnaast bronpoortreeksen bij.	Minimaal (bij vaste IP-adressen), gemiddeld (bij mobiele waar gebruik kan worden gemaakt van bronpoortnummers) tot hoog (wanneer geen bronpoortnummer beschikbaar is; meerderheid van de gevallen).	Geen, anders dan de huidige kosten voor het bijhouden, opslaan en beschikbaar maken van de data.

Internationale vergelijking

Uit de internationale vergelijking zijn op hoofdlijnen drie lessen te trekken voor de Nederlandse situatie:

1. Nederland heeft een relatief zeer groot aantal IPv4-adressen ten opzichte van het aantal inwoners, waardoor er een kleinere prikkel bestaat voor ISP's om IPv6 uit te rollen dan in andere landen.

2. Nationale factoren, zoals nationaal beleid, zijn bepalend(er) dan de strategie van internationale ISP-conglomeraten bij het al dan niet adopteren van IPv6 door ISP's.

3. IPv6 op mobiele netwerken is volwassen en kan door operators binnen een afzienbare termijn worden uitgerold.

Beleidsopties

We zien een aantal beleidsopties:

1. **Een functionele verplichting voor ISP's tot 1:1-identificatie**. Gezien de aantallen (groeiend aantal apparaten/abonnees versus beschikbare hoeveelheid IPv4-adressen) betekent deze oplossing in de praktijk uiteindelijk een uitrol van IPv6. Desondanks worden de internetaanbieders in staat gesteld een eigen strategie te hanteren op de kortere termijn. Door implementatie van logging of het toevoegen van IPv4-adressen kan een operator ingrijpende wijzigingen enkele jaren uitstellen en hoeft zij investeringen in CG-NAT niet af te schrijven.

2. **IPv6-uitrol door ISP's stimuleren of verplichten.** Gelet op het aantal apparaten dat in de toekomst op internet zal zijn aangesloten, is uiteindelijke uitrol en adoptie van IPv6 onafwendbaar. Hoewel een verplichting tot uitrol van IPv6 zou kunnen worden opgelegd, is dit niet in lijn met de algemene beleidsvisie dat ISP's zelf verantwoordelijk zijn voor hun technische keuzes, en sluit het andere technische oplossingsrichtingen wellicht uit.

3. **Een functionele verplichting voor ISP's tot 1:N-identifcatie**. Aangezien de internetaanbieders waarschijnlijk niet direct kunnen voldoen aan 1:1-identificatie (daar is hun techniek immers nog niet klaar voor), kan overwogen worden om de 1:1-eis pas na, of geleidelijk in, een aantal jaar in te laten gaan.

4. **Geen nieuw specifiek beleid voeren; 'nudging'.** Eventueel kunnen 'zachtere' instrumenten worden ingezet, zoals websites/online diensten aan te sporen source ports op te slaan, en kunnen internetaanbieders worden aangesproken op hun (morele) verantwoordelijkheid. Autonome uitrol van IPv6 door de ISP's is waarschijnlijk, maar zal erg langzaam plaatsvinden.

1 Inleiding

In dit hoofdstuk beschrijven we in paragraaf 1.1 de aanleiding van dit onderzoek naar de identificatie van individuele gebruikers van IP-adressen. Vervolgens worden de doelstelling en onderzoeksvragen genoemd (paragraaf 1.2) en presenteren we de onderzoeksaanpak (paragraaf 1.3). Afsluitend is er een leeswijzer voor dit rapport toegevoegd (paragraaf 1.4).

1.1 Achtergrond en aanleiding voor het onderzoek

Met de Wet bewaarplicht van telecommunicatiegegevens[1] is per 18 juli 2009 in Nederland een algemene bewaarplicht geïntroduceerd. Deze wet beoogde te garanderen dat bepaalde telecommunicatiegegevens voor een bepaalde duur beschikbaar waren voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit (dataretentie). Het ging hier om gebruikersgegevens ter identificatie van gebruikers, alsook verkeers- en locatiegegevens die aangeven wie waar, wanneer en met wie in contact is geweest.

In december 2016 heeft het Europees Hof van Justitie een arrest (het "Tele2-arrest") gewezen over het bewaren van telecommunicatiegegevens ten behoeve van opsporing en vervolging van strafbare feiten.[2] Het oordeel was dat Europese richtlijnen zich verzetten tegen een nationale regeling die, ter bestrijding van criminaliteit, voorziet in algemene en ongedifferentieerde bewaring van alle verkeersgegevens van alle gebruikers betreffende alle elektronische communicatiemiddelen.

Mede naar aanleiding van het arrest van het Europees Hof en daaropvolgende vragen uit de Tweede Kamer is in het regeerakkoord "Vertrouwen in de toekomst" van het kabinet Rutte-III afgesproken dat het wetsvoorstel *Aanpassing bewaarplicht telecommunicatiegegevens* wordt heroverwogen [2, p. 6]. In maart 2018 heeft de minister van Justitie en Veiligheid conform het regeerakkoord medegedeeld aan de Kamer een beperkte bewaarplicht te willen introduceren van telecommunicatiegegevens, namelijk alleen de gebruikersgegevens, en niet ook de verkeers- en locatiegegevens [3]. Dat betekent dat aanbieders van openbare telecommunicatiediensten worden verplicht tot het bewaren van deze gegevens.

Door telecomaanbieders werd in gesprekken (maart 2019) over de implementatie van deze voorgenomen wetgeving aangegeven dat het kunnen opleveren van een individuele gebruiker per IP-adres op een bepaald tijdstip, of een beperkt aantal gebruikers per IP-adres, vanuit technisch oogpunt ingewikkeld en in sommige gevallen onmogelijk is. In deze studie onderzoeken wij dit standpunt en leveren wij een bijdrage aan de ontwikkeling van regelgeving over dataretentie binnen de huidige Europese juridische kaders, zoals verwoord in de Kamerbrief van 26 maart 2018 [3].

---

[1] Wet bewaarplicht van telecommunicatiegegevens, jaargang 2009, nr. 333.

[2] Arrest van het Europees Hof van Justitie in de gevoegde zaken C-203/15 en C-698/15, document 62015CJ0203, 21 december 2016.

1.2 Doelstelling en onderzoeksvragen

De vraagstelling van het onderzoek luidt als volgt:

> ***Hoe kunnen (mobiele) internetaanbieders, tot twaalf maanden na het gebruik, een individuele gebruiker van een publiek IP-adres identificeren, ten behoeve van opsporing en vervolging[3], en wat zijn relevante (maatschappelijke) afwegingen daarbij?***

Wanneer het gaat om relevante maatschappelijke afwegingen onderscheiden we de volgende zaken:

1. **De bruikbaarheid voor opsporing en vervolging.** Dit hangt samen met de omvang van de groep personen die kan worden gevonden op basis van een spoor, en de hoeveelheid informatie die daarvoor nodig is.

2. **De privacy van burgers**. Deze hangt samen met de hoeveelheid informatie die moet worden opgeslagen. Daarnaast bepaalt de groepsgrootte de impact op onschuldige burgers in een opsporingsonderzoek (en daarmee juridische proportionaliteit van de inzet ervan).

3. **De kosten voor (mobiele) internetaanbieders** voor het implementeren van de identificatiemethode.

Het antwoord op deze vraag wordt geformuleerd als *beleidsopties* waarin de bovengenoemde aspecten worden afgewogen. De volgende deelvragen staan ter onderbouwing centraal in dit onderzoek:

1. Wat zijn mogelijkheden om, tot twaalf maanden na een communicatie, een individuele gebruiker of abonnee van een publiek IP-adres te kunnen identificeren, op basis van een datum- en tijdsaanduiding van de communicatie, en hoe bruikbaar zijn deze voor opsporing en vervolging?

2. Welke gegevens van een gebruiker zouden per geïdentificeerde mogelijkheid onder de voorgenomen wettelijke bewaarplicht voor telecomaanbieders moeten vallen?

3. Wat zijn de kosten om de geïdentificeerde mogelijkheden te implementeren, waarbij rekening wordt gehouden met de reguliere/geplande kosten voor afschrijving en vervanging van hardware en software door de aanbieders? In hoeverre speelt het tijdselement daarin een rol?

1.3 Aanpak van het onderzoek op hoofdlijnen

Uitgangspunt van de gekozen onderzoeksopzet is de afweging tussen precisie van identificatie, de hoeveelheid verzamelde informatie, en de hoeveelheid benodigde IP-adressen. Ieder van deze aspecten raakt een andere set stakeholders.

---

[3] In dit onderzoek kijken wij nadrukkelijk naar opsporingsdiensten (politie/OM). Mogelijk zijn de uitkomsten ook relevant voor inlichtingendiensten, maar dit valt buiten de scope van dit onderzoek. Daarnaast is nationale veiligheid niet in de vraagstelling opgenomen, maar ook dat doel wordt gediend met dit onderzoek.

Literatuurstudie

We zijn gestart met een literatuurstudie. Het doel hiervan was om een goed en zo volledig mogelijk beeld te krijgen van wat er technisch mogelijk is binnen de wet- en regelgeving op het gebied van identificatie van individuele gebruikers van IP-adressen. Via vrij zoeken en aan de hand van literatuurtips van experts zijn de belangrijkste bronnen verzameld en (in samenhang) geanalyseerd. Berekeningen op basis van de bronnen zijn weer voorgelegd aan de experts.

Internationale vergelijking

In de internationale vergelijking inventariseren we de situatie ten aanzien van identificatie op basis van IP-adressen en de gekozen oplossingen in verschillende landen, waarbij wordt gekeken naar de onderliggende drijvers en gekozen beleidsmaatregelen daarbij. De internationale vergelijking die onderdeel uitmaakt van dit onderzoek bestaat uit drie separate analyses.

In de eerste analyse kijken we naar hoe de wereldwijde schaarste aan IPv4-adressen de adoptie van IPv6 beïnvloedt. Eerst wordt per land geïnventariseerd hoeveel IPv4-adressen per hoofd van de bevolking zijn uitgegeven.[4] Vervolgens kijken we naar het internetverkeer dat per land over IPv6 verloopt om zo uitspraken te doen over de relatie tussen de twee variabelen.

In de tweede analyse inventariseren we de situatie van de ISP's die onder dezelfde moederbedrijven vallen als de Nederlandse ISP's (Deutsche Telekom, Liberty Global en Vodafone Group). De kernvraag is of er verschillen tussen concerns en/of tussen de bedrijven binnen de concerns zijn, en of deze te verklaren zijn door concernstrategie, dan wel nationale regulering.

De derde analyselijn betreft een inventarisatie van het beleid en de situatie in landen waarmee Nederland vergelijkbaar is. In de eerste fase hiervan wordt exploratief gewerkt op basis van beschikbare literatuur. Vervolgens wordt een selectie gemaakt van interessante casussen waarbij de vergelijkbaarheid met Nederland is geanalyseerd: waarin verschillen de landen en zijn deze verschillen aantoonbaar van invloed geweest op de verschillen in de uitkomst? In deze fase wordt nadrukkelijk aandacht besteed aan Zweden en België[5].

Verkennende interviewronde

Parallel aan de literatuurstudie is een verkennende interviewronde gehouden met mobiele ISP's, politie en andere stakeholders en experts. In totaal hebben we 15 personen gesproken (zie Bijlage 1).

Het doel van de interviews is om enerzijds een beeld te krijgen van wat de wensen/eisen vanuit opsporing zijn en anderzijds om de technische aspecten van de verschillende mogelijkheden in kaart te brengen. In de gesprekken met de mobiele ISP's wordt (indien van toepassing) ook de situatie op het vaste aansluitnetwerk besproken. Daarnaast is een grootzakelijke aanbieder van vaste aansluitingen benaderd om te controleren in hoeverre de situatie daar afwijkt van de situatie op de grote netwerken.

---

[4] De uitgifte wordt gedaan door regionale internetregistrars (RIR's).

[5] Zweden is met name interessant vanwege de wetgeving omtrent data retentie. België heeft het hoogste IPv6-adoptiepercentage en de Belgische aanpak wordt voorgeschreven door internationale opsporingsdiensten zoals Europol.

Validerende interviewronde

In een validerende interviewronde is nogmaals (per e-mail en telefonisch) contact gezocht met de drie grootste mobiele ISP's (KPN, T-Mobile/Tele 2 en Vodafone). De uitgewerkte oplossingsmogelijkheden inclusief het kostenplaatje werden ter validatie aan deze partijen voorgelegd, waarbij zij de volgende vragen voorgelegd kregen:

- Hoe preferabel is deze oplossingsrichting ten opzichte van de andere oplossingsrichtingen?
- Welke investeringen moet een operator doen om deze oplossingsrichting te realiseren, en hoe groot zijn deze?

Hoewel expliciet gevraagd, heeft geen van de ISP's concrete bedragen genoemd in de beantwoording. Uit de beantwoording is echter wel naar voren gekomen welke overwegingen en voorkeuren er spelen bij de verschillende oplossingsrichtingen.

1.4 Leeswijzer

In hoofdstuk 2 beschrijven we de problemen waar men in het kader van opsporing tegen aan loopt met IP-adressen en geven we een feitelijke technische beschrijving van de problematiek. In hoofdstuk 3 werken we de diverse mogelijkheden voor betere identificatie uit en in hoofdstuk 4 beschrijven we de resultaten uit de internationale vergelijking en noemen we belangrijke lessen voor Nederland. Hoofdstuk 5 bevat de conclusies van dit onderzoek, geformuleerd als antwoorden op de onderzoeksvragen en als beleidsopties.

2 Probleemanalyse

In dit hoofdstuk beschrijven we allereerst de aanleiding voor het uitvoeren van dit onderzoek: opsporing op basis van IP-adres en de maatschappelijke context daarbij. Vervolgens beschrijven we de problemen waar men in het kader van opsporing aan de hand van IP-adressen tegen aan loopt (paragraaf 2.1) en geven we een feitelijke technische beschrijving van de problematiek (paragraaf 2.2). In paragraaf 2.3 noemen we de belangrijkste maatschappelijke afwegingen en in paragraaf 2.4 behandelen we de huidige stand van zaken bij de ISP's.

2.1 Opsporing op basis van IP-adres

Wanneer er een strafbaar feit plaatsvindt, maar dit niet op heterdaad wordt geconstateerd, moet de dader op basis van achtergelaten sporen worden gevonden, om uiteindelijk tot vervolging over te kunnen gaan. Om de dader te identificeren, kunnen verschillende middelen worden gebruikt; zo kan een getuige een dader aanwijzen, kunnen bestuurders van een auto worden getraceerd op basis van een gezien kenteken, en kunnen ook houders van bankrekeningen, onroerend goed en mobiele telefoonnummers worden gevonden via respectievelijk de bank, het Kadaster en de mobiele operator.

Steeds meer strafbare feiten vinden in het digitale domein plaats; het betreft zowel traditionele vormen van criminaliteit waarbij (deels of geheel) gebruik wordt gemaakt van het internet, als nieuwe vormen van criminaliteit die zich uitsluitend in het digitale domein bevinden, zoals een Denial-of-Service-aanval op websites.[6] Ook in het digitale domein is opsporing en identificatie van daders van belang en ook in het digitale domein laten daders van strafbare feiten sporen na. Wanneer communicatie plaatsvindt op het internet is bij de ontvanger typisch het IP-adres van de afzender bekend – dit is immers nodig voor de communicatie in de tegengestelde richting. Dit IP-adres geeft daarmee een directe aanwijzing richting het systeem vanaf waar een bepaalde strafbare handeling werd verricht.

IP-adressen worden door zogenaamde Regional Internet Registries (RIR's) uitgegeven aan ISP's, die de IP-adressen in bruikleen geven aan hun klanten. Omdat van ieder IP-adres bekend is aan welke ISP deze is uitgegeven, kunnen opsporingsdiensten de ISP verzoeken bekend te maken aan welke abonnee een bepaald adres is uitgegeven.[7]

Als gevolg van ontwikkelingen op het internet is de koppeling tussen individu en IPv4-adres[8] vandaag de dag echter niet meer zo evident als deze was. Hoewel ieder aangesloten apparaat in de begindagen van het internet een eigen, vast IPv4-adres kreeg toegewezen van zijn ISP, is dat tegenwoordig vaak niet meer het geval. Het aantal IPv4-adressen is namelijk eindig (in theorie maximaal circa 4 miljard, in de praktijk lager) en inmiddels veel kleiner dan het aantal aangesloten apparaten. In de huidige situatie worden IP-adressen dus gedeeld, soms door wel 200 mensen. 200 is echter niet de bovengrens. Vyncke [4] geeft aan

[6] Dit beeld wordt bevestigd in het interview met politiemedewerkers: zie ook sectie 2.3 voor verdere overwegingen en details.

[7] Zie voor details, waaronder de voorwaarden waaronder, en wélke opsporingsdiensten informatie kunnen opvragen, het *Besluit verstrekking gegevens telecommunicatie* [wetten.overheid.nl].

[8] Internet Protocol versie 4 (IPv4) is de vierde versie van het internetprotocol. Deze versie werd voor het eerst op grote schaal gebruikt en vormt de basis voor adressering binnen het internet.

dat met apparatuur van Cisco voor mobiele netwerken een ratio van 1:30.000 haalbaar is. Er zijn ook gevallen bekend waar 1:100.000 gebruikers per IPv4-adres werd gehanteerd.

2.2 Technische achtergrond: gedeelde IP-adressen

Om het groeiend aantal apparaten aan te kunnen sluiten op internet moeten apparaten en gebruikers IP-adressen delen. Hiervoor zijn verschillende technische oplossingen beschikbaar. Een ISP kan allereerst IPv4-adressen *dynamisch toewijzen*; hierbij delen abonnees hetzelfde IP-adres, maar nooit tegelijkertijd. De ISP wijst bij het opzetten van de verbinding een willekeurig IPv4-adres toe aan een abonnee, en houdt een log bij van welk IPv4-adres aan welke abonnee was toegewezen op welk moment. Op basis van datum, tijd en publiek IP-adres is een individuele abonnee dus nog steeds identificeerbaar. Deze situatie is vergelijkbaar met wanneer een bestuurder van een huurauto wordt gezocht op basis van kenteken: het kenteken behoort weliswaar tot het verhuurbedrijf, maar deze kan, op basis van de eigen administratie de huurder achterhalen.

In situaties waarbij het aantal beschikbare IPv4-adressen veel kleiner is dan het aantal apparaten dat gelijktijdig online is, is het nodig IPv4-adressen gelijktijdig te delen tussen gebruikers. Dit is mogelijk door toepassing van *network address translation (NAT)* gateways. De NAT-functionaliteit, die vaak geïmplementeerd wordt in thuis modem/routers, netwerk routers of firewalls, kan de communicatie van meerdere apparaten bundelen op een kleiner aantal IP-adressen. Wanneer een aangesloten apparaat op het internet wil communiceren, vertaalt de gateway de netwerkpakketten zodanig dat het voor de ontvanger net lijkt alsof de gateway de afzender was. Bij binnenkomst van verkeer kan de gateway (op basis van bijvoorbeeld de bestemming) achterhalen voor welk achterliggend apparaat het verkeer bedoeld is. Hiervoor houdt de gateway een tabel bij met openstaande verbindingen.

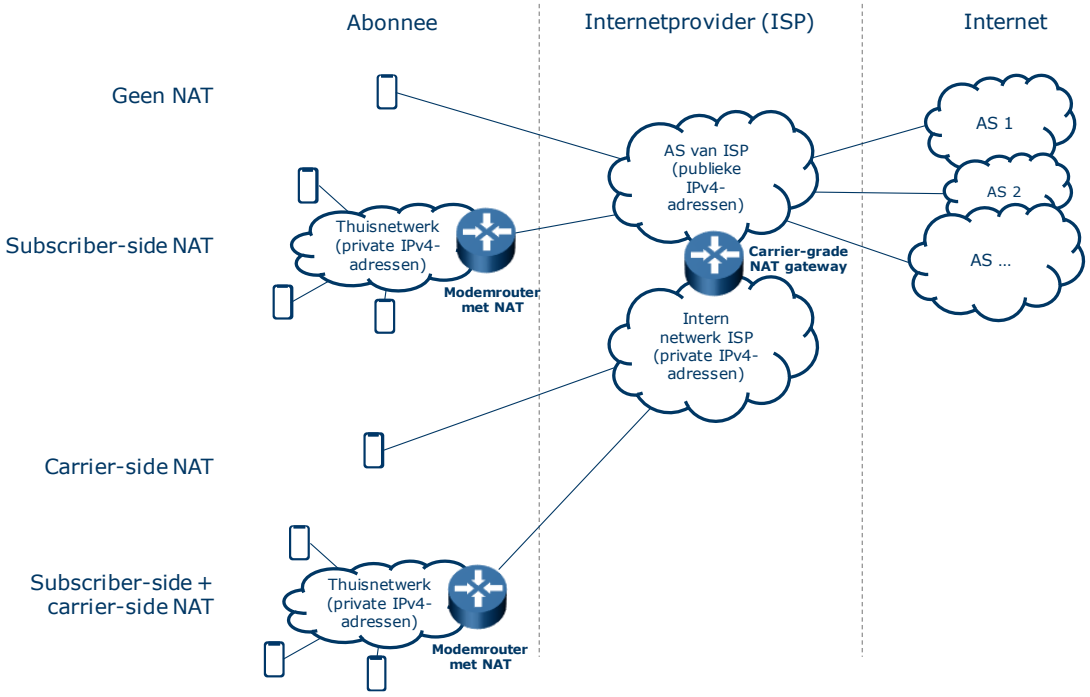
NAT wordt onder andere toegepast in thuis- en kantoornetwerken: de (modem)router van de abonnee verzorgt namens alle op het thuis- of kantoornetwerk aangesloten apparaten de communicatie op internet via één publiek IP-adres.[9] Het toepassen van NAT aan de zijde van een abonnee van een ISP is vanuit het perspectief van opsporing geen onoverkomelijk probleem: de betreffende abonnee kan worden geïdentificeerd via de ISP, en deze kan vervolgens leiden tot een mogelijke dader: het aantal gebruikers dat van een thuisaansluiting gebruik maakt, is immers niet zo groot.

Naast NAT aan de zijde van een abonnee (bijvoorbeeld ten behoeve van een thuisnetwerk) zijn andere vormen van NAT mogelijk. Figuur 1 toont de verschillende vormen van NAT die kunnen worden toegepast. Op mobiele netwerken wordt typisch[10] *carrier grade NAT* (CG-NAT, 'NAT44 carrier-side') toegepast. Hierbij bevindt de NAT-gateway zich aan de zijde van de ISP, en maken grote aantallen abonnees gebruik van een beperkte hoeveelheid publieke IP-adressen. De toewijzing van abonnees aan publieke IPv4-adressen kan zowel statisch als dynamisch worden gedaan.

---

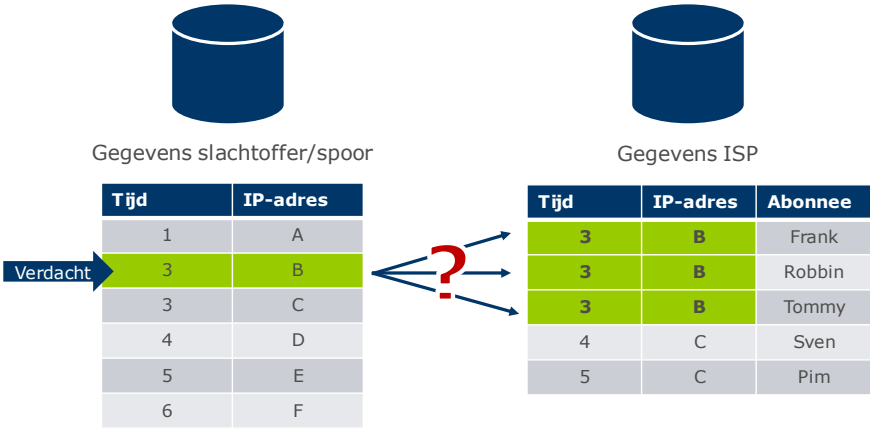
[9] De situatie voor kantoornetwerken voor midden- en kleinbedrijf is meestal vergelijkbaar met die bij consumenten. Op grotere kantoornetwerken wordt, vanwege het grotere aantal apparaten, een vorm van NAT toegepast die vergelijkbaar is met wat telecomoperators toepassen (CG-NAT), waarbij meerdere publieke IP-adressen worden ingezet. Sommige kantoornetwerken (bijvoorbeeld die van universiteiten) hebben van oudsher de beschikking over voldoende publieke IPv4-adressen, en kennen ieder apparaat een publiek IP-adres toe, waardoor geen (CG-)NAT nodig is.

[10] In 2016 werd wereldwijd op circa 50% van de mobiele netwerken CG-NAT toegepast of overwogen. [5]



Figuur 1 Schematisch overzicht van verschillende vormen van NAT [5]

De toepassing van CG-NAT levert, in tegenstelling tot NAT aan zijde van de abonnee, echter wel de nodige bezwaren op vanuit perspectief van opsporing. Een ISP houdt nu namelijk bij welke abonnee op welk moment gebruik maakte van een bepaald publiek IPv4-adres. Figuur 2 geeft dit schematisch weer: er waren drie abonnees die gebruik maakten van IP-adres "B" op tijdstip "3".



Figuur 2 Schematische weergave van het identificatieprobleem bij CG-NAT [6]

In de analogie met huurauto's betekent CG-NAT dat *verschillende* huurders landelijk in verschillende huurauto's rondrijden, maar allemaal met *hetzelfde* kenteken. Zodra de politie de bestuurder wil identificeren is, behalve datum en tijd, ofwel meer informatie over het verkeer nodig (bijvoorbeeld: de kleur en het type van de auto) ofwel over de route (wáár is de auto gesignaleerd, of wat was de bestemming?).

Zelfs wanneer een ISP bijhoudt welke abonnees op welk moment gebruik maakten van welk publiek IP-adres, kan het zijn dat het aantal abonnees zo groot is, dat meer informatie nodig

is om een preciezere selectie te kunnen maken. Eenzelfde publiek IP-adres kan immers door meerdere abonnees op dezelfde dag (of zelfs binnen een kortere tijdsperiode) worden gedeeld. Er zijn gevallen bekend met zeer grote aantallen gebruikers per IPv4 adres – Europol rapporteert dat het in specifieke casussen om 'enkele duizenden abonnees' gaat. [7]

Theoretisch gezien kan een enkel IPv4-adres (op basis van realistische aannames en een goede ervaring voor de eindgebruiker) worden gedeeld met circa 117 abonnees, wanneer de toewijzing van abonnee naar publiek IPv4-adres statisch plaatsvindt. Met *statisch* bedoelen we dat een abonnee een vaste reeks van poortnummers horend bij een vast publiek IPv4-adres krijgt toegewezen, die niet of nauwelijks wijzigt door de tijd.[11] Bij *dynamische* toewijzing wordt een publiek IPv4-adres en -poortnummer geselecteerd op het moment dat de abonnee een verbinding opzet. Omdat de poorten van inactieve abonnees niet 'gereserveerd' hoeven te blijven, kan met dynamische toewijzing efficiënter gebruik worden gemaakt van de beschikbare IPv4-adressen en -poorten: per IPv4-adres is ruimte voor circa 600 abonnees.[12] In mobiele netwerken, waar applicaties bewust maar weinig poorten tegelijkertijd gebruiken, kan dat aantal veel hoger zijn.

Door effectiever meerdere verzoeken te versturen via één TCP-verbinding[13] kan het aantal per abonnee benodigde poorten worden verlaagd. Dat leidt ertoe dat er, zeker in mobiele netweken, grotere aantallen gebruikers per IPv4-adres mogelijk worden. Meer dan 1.000 gebruikers achter één IPv4-adres is goed haalbaar in de praktijk.

Merk bij het bovenstaande op dat een operator het aantal abonnees per IPv4-adres in principe ruim zal dimensioneren, om te voorkomen dat schaarste ontstaat op piekmomenten. Mocht er op enig moment geen poort vrij zijn, dan zal een abonnee die een verbinding wil opzetten moeten wachten tot er een poort vrij is gekomen. De abonnee zal dat merken, doordat applicaties trager of helemaal niet meer werken.

Om de beperking van te weinig IP-adressen op te heffen, werd al in 1995 begonnen met het ontwikkelen van IPv6, een opvolger van het op internet gebruikte communicatieprotocol IPv4. IPv6 vergroot het aantal beschikbare IP-adressen tot (theoretisch) maximaal 2^{128} – meer dan genoeg om iedere zandkorrel op aarde van een eigen adres te voorzien. [8] Hoewel IPv6 vandaag de dag kan worden gebruikt, maakt slechts 20% tot 25% van de gebruikers wereldwijd gebruik hiervan. [9] In Nederland is IPv6 op de grootste vaste en mobiele aansluitnetwerken voor het merendeel van de abonnees niet beschikbaar, en ligt het adoptiecijfer op circa 16%. [9]

---

[11] In dit rapport hanteren we voor 'statisch' de definitie: wijzigt maximaal ééns per dag.

[12] Per IPv4-adres zijn 65.536 poortnummers beschikbaar, waarvan er 60.000 te gebruiken zijn (de poorten 0 t/m 1024 kunnen om veiligheidsredenen niet worden gebruikt voor NAT). Bij een gemiddelde van 400 poorten per gebruiker zijn (60.000 / 400 =) 150 actieve gebruikers per IPv4-adres mogelijk. Uitgaande van 25% actieve gebruikers op ieder moment kan het adres dus door (150 / 25% =) 600 abonnees worden gedeeld. Bij statische allocatie moet worden uitgegaan van een maximumaantal poorten per gebruiker (circa 512) en blijven poorten van inactieve gebruikers 'gereserveerd'; het totaal aantal abonnees per IPv4-adres komt in dat geval uit op 60.000 / 512 ≈ 117.

[13] Het Transmission Control Protocol (TCP) is een verbindingsgeoriënteerd protocol dat veel gebruikt wordt voor gegevensoverdracht over netwerkverbindingen op het internet en op computernetwerken. Op deze laag bevinden zich de poortverbindingen.

Is eenduidige identificatie op basis van IP-adres überhaupt mogelijk?

Behalve als gevolg van toepassing van NAT zijn er nog velerlei andere situaties denkbaar waarin het publieke IP-adres niet direct (meer) te herleiden is naar een individu (niet uitputtend):

- *VPN-diensten* bieden gebruikers de mogelijkheid om hun internetverkeer via een ander publiek IP-adres te laten verlopen dan zij via hun eigen ISP kunnen gebruiken. Een VPN-dienst wordt gebruikt voor extra anonimiteit of bijvoorbeeld om regioblokkades van onlinediensten (zoals Netflix en diverse games) te omzeilen.

- Via het *Tor-netwerk* kan met een hogere mate van anonimiteit internetverkeer plaatsvinden. Het verkeer wordt versleuteld en bereikt via een aantal (willekeurig geselecteerde) tussenstappen het internet. Hierdoor is het vervolgens praktisch onmogelijk om de afzender te traceren.

- Bij *spoofing* verandert een gebruiker eigenhandig zijn publieke IP-adres. In de regel is spoofing alleen mogelijk wanneer er rechtstreekse toegang is tot interconnecties tussen ISP's, of sprake is van een configuratiefout bij een ISP (waardoor een abonnee net kan doen alsof verkeer van een andere abonnee afkomstig is).

- Bij *publieke toegangslocaties tot internet*, zoals Wi-Fi-hotspots en internetcafés, wordt door de aanbieder ervan niet altijd bijgehouden welke personen gebruik maken van de dienst, waardoor communicatie niet altijd meer traceerbaar is tot een individu.

- Ook anonieme *prepaid simkaarten* leiden ertoe dat de gebruiker niet te identificeren is. Als gevolg van de recente aanslagen in Parijs, Brussel en Nice hebben enkele landen (o.a. België, Frankrijk en Duitsland) overigens een verbod op anonieme simkaarten ingevoerd. Nederland kiest hier vooralsnog niet voor. [10]

- Hoewel internetaansluitingen in de regel op naam van een persoon of organisatie worden geregistreerd, is het mogelijk dat (bijvoorbeeld) telefoons of SIM-kaarten worden doorverkocht, gestolen of geleend, waardoor een persoon kan communiceren via de aansluiting van iemand anders. Ook kan via malafide software andermans computer worden overgenomen en worden gebruikt voor het uitvoeren van strafbare activiteiten.

2.2.1 Identificeerbaarheid op vaste aansluitingen

Op vrijwel alle vaste aansluitnetwerken krijgen consumenten en kleinzakelijke gebruikers (technisch gezien) dynamisch een publiek IPv4-adres toegewezen.[14] In de praktijk is de toewijzing *statisch*: bij de meeste aansluitingen is de geldigheid van de dynamische toewijzing dertig dagen of hoger. Dat betekent dat, zolang het modem niet wordt uitgeschakeld, de

[14] Dit wil zeggen dat een apparaat dat toegang zoekt tot het internet van het netwerk een IP-adres krijgt toegewezen voor een bepaalde tijdsduur. Ook kan het adres door de gebruiker worden vrijgegeven, waarna een nieuw adres kan worden aangevraagd. In dit geval, en wanneer de tijdsduur verloopt, kan het netwerk eventueel beslissen om hetzelfde adres nog eens toe te kennen ('semi-statisch dynamisch adres').

abonnee bij inschakeling binnen deze termijn hetzelfde IPv4-adres zal ontvangen. We noemen dit in het vervolg 'semi-statisch'.

Voor deze aansluitingen is identificatie van de abonnementhouder goed en eenduidig mogelijk wanneer de ISP's bijhouden welk IPv4-adres wordt toegewezen aan een bepaald modem (en welk modem bij welke abonnementhouder hoort). De drie grote ISP's doen dit allemaal, en delen deze informatie met het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT).[15] In sommige gevallen bewaren de ISP's de gegevens nog een korte tijd (meestal dertig dagen) ten behoeve van de eigen bedrijfsvoering. In theorie is eenduidige identificatie van een abonnementhouder op basis van een publiek IPv4-adres via vaste aansluiting dus altijd mogelijk.

Van belang is wel dat goed wordt bijgehouden op welk moment een IPv4-adres van gebruiker wisselt. Typisch wordt het CIOT door een operator eens per dag voorzien van informatie over de toewijzing, maar het is mogelijk dat een IP-adres gedurende de dag van eigenaar wisselt (waarbij in sommige gevallen slechts één van beide gebruikers genoemd wordt in het informatiesysteem van het CIOT). Wanneer ISP's de IP-adressen na 'vrijgeven' niet minimaal een dag bevriezen, moet dus rekening worden gehouden met een groepsgrootte voor identificatie tot twee abonnees.

Zakelijke klanten krijgen van een ISP vaak een vast IP-adres of een reeks vaste IP-adressen. In deze gevallen is identificatie van de betreffende bedrijfsnaam eenduidig mogelijk op basis van de administratie van de ISP. Grootzakelijke klanten beschikken in sommige gevallen over een 'eigen' IP-reeks – registratie-informatie hiervoor is op te vragen bij de RIR's.

Een aantal ISP's biedt IPv6-connectiviteit aan abonnees aan. Een abonnee krijgt daarbij semi-statisch een IPv6-adres(reeks) toegewezen. Identificatie van een abonnementhouder is (mits informatie wordt bijgehouden over de toewijzing) eenduidig mogelijk op basis van een IPv6-adres.

Sommige ISP's passen de techniek 'DS-Lite' of '464XLAT' toe om klanten van IPv6-connectiviteit te voorzien (zie paragraaf 3.2.1). Hierbij wordt IPv4-verkeer verstuurd over het IPv6-kanaal, om vervolgens via een gedeeld publiek IPv4-adres vanaf de ISP het internet weer op te gaan - in feite een vorm van CG-NAT. Dit betekent dat identificatie wordt bemoeilijkt wanneer vanuit opsporing een IPv4-adres bekend is. Het betreft op dit moment een klein aantal klanten van één van de drie genoemde Nederlandse ISP's.

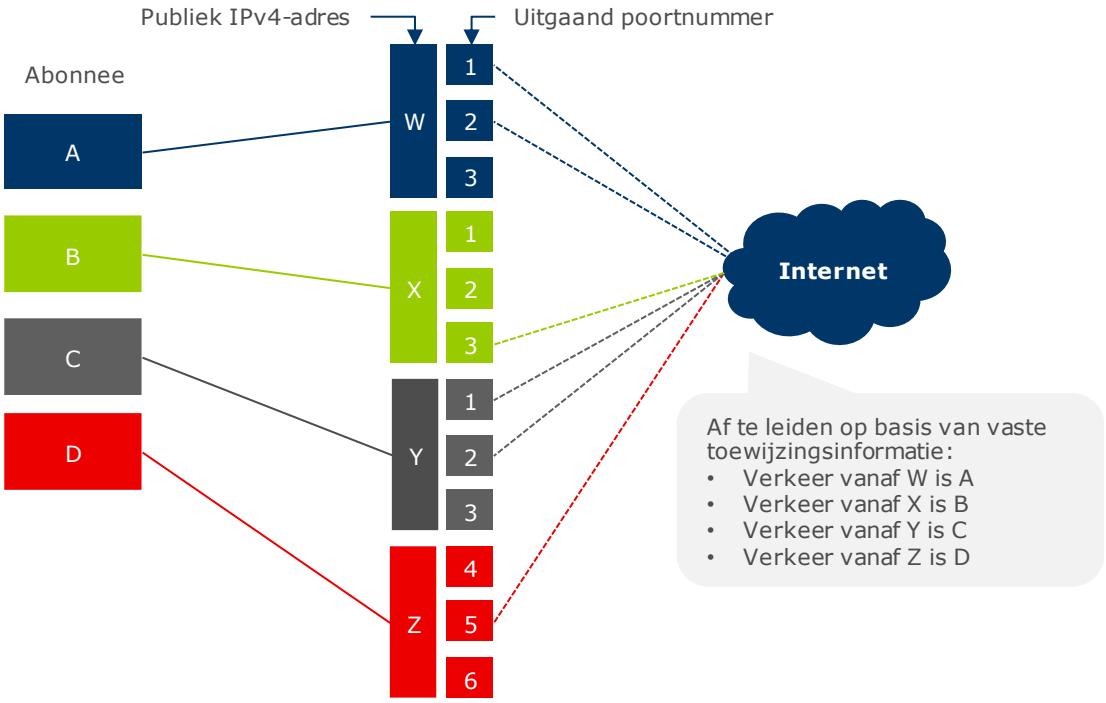
2.2.2 Identificeerbaarheid op mobiele aansluitingen

Bij vaste netwerken (huisaansluitingen en zakelijke aansluitingen) zijn er meestal weinig wisselingen in IP-adres,[16] en is de bij ISP's opvraagbare informatie specifiek genoeg voor de politie om verder onderzoek te doen. Figuur 3 toont hoe IP-adressen en poortnummers worden toegewezen aan abonnees in deze situatie. De doorgetrokken lijnen betreffen (semi)permanente toewijzingen waarover informatie wordt bijgehouden; de stippellijnen zijn

[15] Het CIOT beheert een informatiesysteem voor telefoon- en internetgegevens voor de opsporing van criminelen.

[16] Bij het 'uitdelen' van IPv4-adressen wordt meestal een geldigheid van een week tot een maand gehanteerd. Zodra die periode is verstreken kennen de meeste ISP's aan een abonnee opnieuw hetzelfde IPv4-adres toe. Wanneer er noodzaak is om de IPv4-adressen in het netwerk anders in te delen (bijvoorbeeld door scheefgroei van het aantal abonnees), of wanneer een abonnee langere tijd niet op het netwerk is aangemeld, wordt veelal een nieuw IPv4-adres worden toegekend.

dynamisch per uitgaande verbinding, waarover geen informatie wordt bijgehouden (verkeersgegevens).



Figuur 3 Statische toewijzing van publieke IPv4-adressen zonder CG-NAT

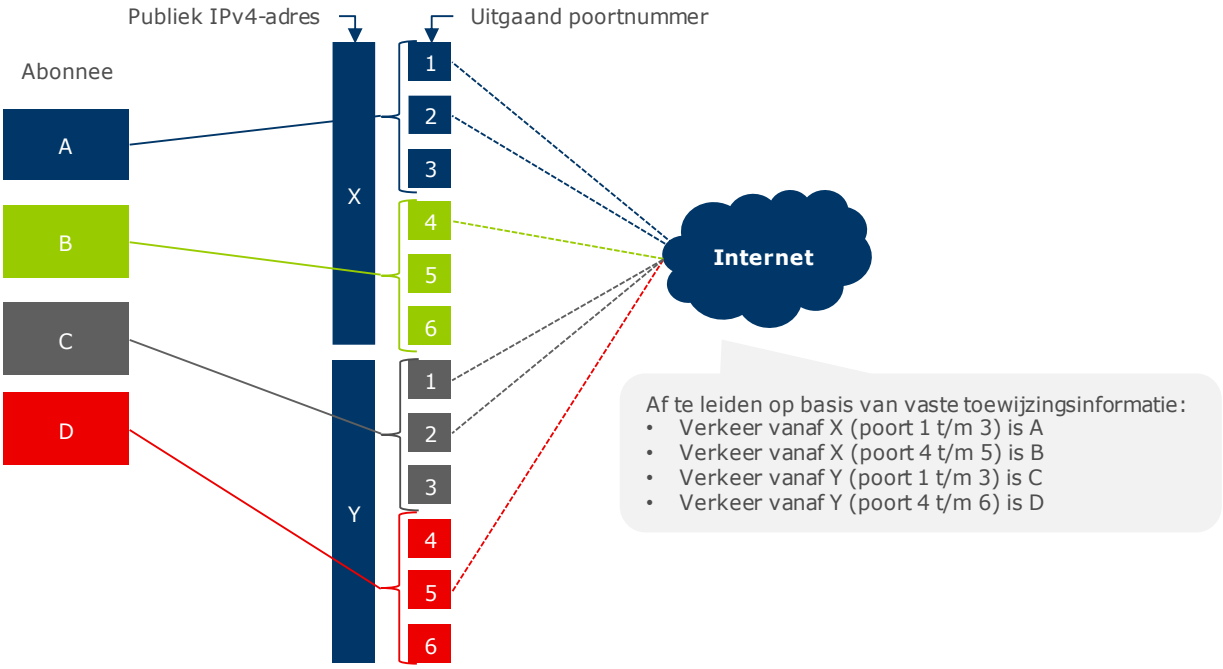
De problematiek van identificatie van personen ligt dus nadrukkelijk bij mobiele netwerken en consumentenaansluitingen. In de beginperiode van mobiele internettoegang werd wat betreft toewijzing van IPv4-adressen gewerkt op dezelfde wijze als op de vaste netwerken. Aangezien de populariteit van mobiel internet echter snel is toegenomen sinds de introductie van de smartphone, kwamen de ISP's op een gegeven moment IPv4-adressen tekort.

Er zijn grofweg twee vormen van CG-NAT in gebruik op mobiele netwerken: een vorm waarbij (semi-statisch of per mobiele datasessie[17]) een poortbereik wordt toegekend aan een abonnee, en een vorm waarbij een abonnee alleen (semi-statisch of per mobiele datasessie) wordt toegewezen aan een 'pool' van IP-adressen.

1. CG-NAT met toewijzing van abonnee aan een poortbereik

Bij deze vorm van CG-NAT wordt een abonnee toegewezen aan één publiek IPv4-adres (afkomstig uit een voorraad die specifiek is gereserveerd voor CG-NAT), en daarvan een beperkt aantal uitgaande poorten. Bij sommige ISP's blijft deze toewijzing in stand wanneer de mobiele verbinding tijdelijk wordt verbroken, bij andere vindt steeds een nieuwe toewijzing plaats. Onderstaande Figuur 4 toont op welke wijze IP-adressen en poortbereiken worden toegekend (de doorgetrokken lijnen zijn opnieuw semipermanente toewijzingen, de gestippelde lijnen zijn dynamisch per verbinding).

[17] Een sessie ontstaat wanneer een mobiel apparaat voor het eerst een dataverbinding wil opzetten en eindigt zodra het apparaat wordt uitgezet, de datasessie zelf verbreekt (bijvoorbeeld om energie te besparen), na een bepaalde tijd, of wanneer het netwerk (tijdelijk, vaak langer dan enkele minuten) buiten bereik is. Afhankelijk van de operator kan ook het verplaatsen tussen regio's leiden tot verbreken van een datasessie.



Figuur 4 (Semi)permanente toewijzing van een publiek IPv4-adres en poortbereik aan een abonnee bij CG-NAT

Als vuistregel wordt uitgegaan van 512 poorten per abonnee. Per IPv4-adres zijn minimaal circa 60.000 poorten beschikbaar voor gebruik als uitgaande poort.[18] Dat betekent dat bij statische toewijzing circa 117 klanten een IPv4-adres gelijktijdig kunnen gebruiken.

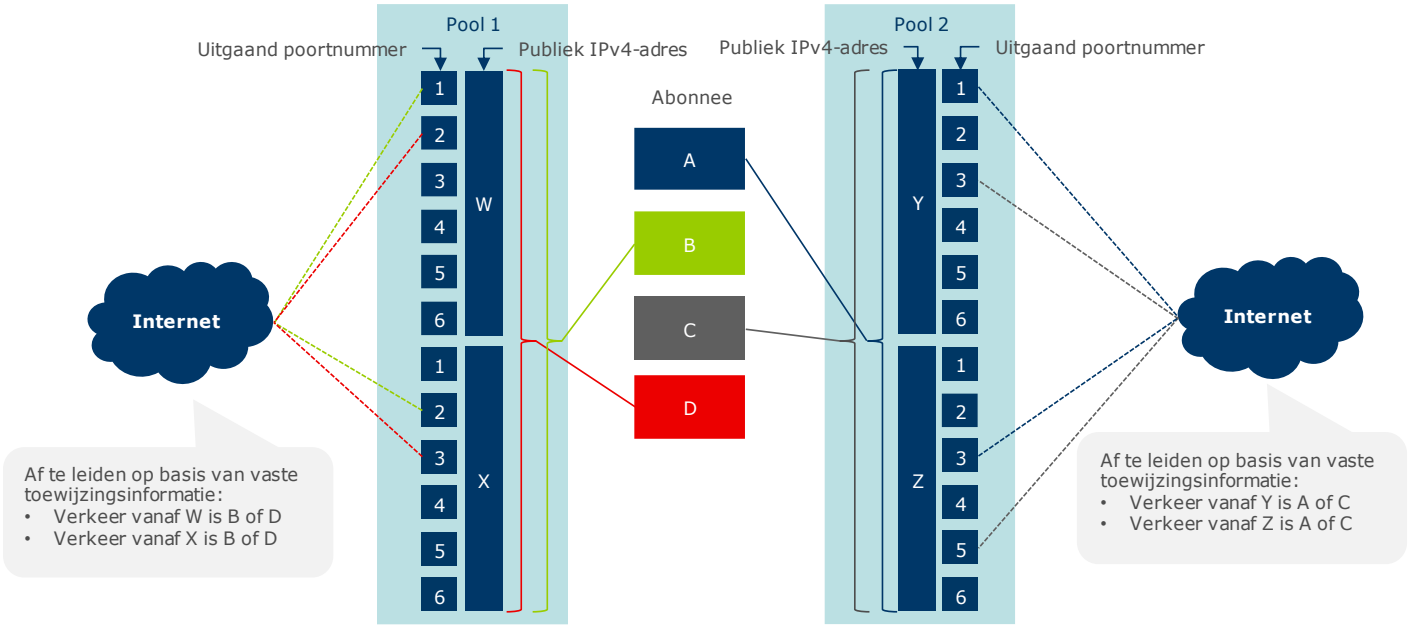
Een ISP die deze vorm van CG-NAT toepast, kan door bij te houden welke abonnee op welk moment werd toegewezen aan een bepaald IPv4-adres identificeren tot een groepsgrootte van maximaal 117 abonnees. Wanneer vanuit opsporing ook een poortnummer bekend is, zou eenduidige identificatie mogelijk zijn wanneer de ISP ook de toewijzing naar poortnummers opslaat.

Wanneer een bepaald poortbereik per dag meerdere keren wordt toegewezen, is de groep groter als vanuit opsporing geen precieze tijdsaanduiding bekend is. Wanneer het druk is op het netwerk zal hiervan mogelijk sprake zijn, afhankelijk van de grootte van de door de ISP gereserveerde voorraad publieke IPv4-adressen voor CG-NAT. De benodigde precisie van de tijdsaanduiding hangt af van deze verversingssnelheid.

[18] De poortnummers 0-1024 zijn bedoeld voor servers (inkomend verkeer). RFC7422 stelt dat alle bovengelegen poortnummers gebruikt kunnen worden voor CG-NAT. [60]

2. CG-NAT met dynamische toewijzing uit een pool

Bij deze vorm van CG-NAT wordt een klant semi-statisch of zelfs per mobiele datasessie toegewezen aan een *pool*. Een *pool* is een verzameling van publieke IPv4-adressen (typisch 255). Bij iedere verbinding die door de klant wordt opgezet wordt een beschikbaar poortnummer bij één van de IPv4-adressen uit deze set gebruikt. Figuur 5 toont schematisch hoe deze toewijzing werkt.



Figuur 5 Toewijzing van abonnees aan een 'pool' van publieke IPv4-adressen bij CG-NAt

Het voordeel van deze vorm van CG-NAT is dat deze efficiënter is dan statische toewijzing: een abonnee gebruikt immers vrijwel nooit het volledige aantal aan hem toegewezen poorten bij statische toewijzing. Het nadeel is dat identificatie wordt bemoeilijkt: bij de aanvang van een mobiele datasessie kan de ISP weliswaar opslaan aan welke *pool* een gebruiker wordt toegewezen, maar binnen diezelfde pool gebruikt de gebruiker potentieel alle beschikbare IP-adressen, en is er potentieel een groot aantal anderen klanten toegewezen aan dezelfde pool waarvoor hetzelfde geldt. Voor de ISP('s) die deze vorm van CG-NAT in Nederland toepassen, ligt de groepsgrootte bij identificatie in deze omstandigheden naar schatting op circa 60.000.

2.3 Maatschappelijke afwegingen

In het voorliggende vraagstuk staan de baten van opsporing op basis van IP-adres voor de maatschappij tegenover kosten (in brede zin) die de maatschappij daarvoor moet maken. Voor de maatschappij is het maatschappelijk wenselijk om zoveel mogelijk misdaden op te lossen. Hiervoor is eenduidige identificatie nodig. Wat betreft kosten kan gedacht worden aan de kosten voor het technisch mogelijk maken van de opsporing, maar ook aan immateriële waarden, zoals privacy en veiligheid. Hoewel het afwegen van deze maatschappelijke kosten en baten buiten de afbakening van dit onderzoek valt, is het om de verschillende beleidsopties te kunnen afwegen goed om deze elementen ter achtergrond te schetsen.

2.3.1 Maatschappelijke baten van opsporing op internet

Criminaliteit speelt zich in toenemende mate in het digitale domein af – niet alleen zijn met de opkomst van digitale diensten ook digitale vormen van criminaliteit (zoals DDoS-aanvallen, ransomware en online fraude) ontstaan, ook kennen 'traditionele' vormen van criminaliteit steeds vaker een digitale component. [11] [12] Voor opsporingsdiensten is een

IP-adres bij online criminaliteit vaak het begin van een onderzoek, en daarnaast vaak het enige beschikbare spoor.

Opsporingsdiensten[19] ondervinden op dit moment moeilijkheden bij het identificeren van personen op basis van IP-adressen, met name wanneer het gaat om IP-adressen op mobiele netwerken. Op deze netwerken worden (zo werd hierboven al toegelicht) IP-adressen gedeeld tussen een groot aantal gebruikers. Dat betekent dat de opsporingsdiensten op basis van een IP-adres slechts tot een groep gebruikers kunnen komen.

Veelal strandt een opsporingsonderzoek hier omdat het inzetten van opsporingsmiddelen jegens een grote groep (waarvan het overgrote deel niets met het onderzoek te maken heeft) disproportioneel zou zijn. De acties die de politie uitvoert om de groep personen terug te brengen tot één persoon moeten proportioneel en subsidiair zijn – als er andere, meer geschikte en/of minder invasieve methoden beschikbaar zijn, dan hebben die de voorkeur. Op dit punt speelt met name de 'last' die de andere (onschuldige) personen in de groep ondervinden van een politieonderzoek.[20] De politie legt hierover verantwoording af tegenover de officier van Justitie, die op haar beurt de bewijsvoering moet onderbouwen tegenover een rechter.

In sommige gevallen kan nog wel een nadere schifting zal moeten worden gemaakt. Opsporingsdiensten hebben hiervoor enkele middelen ter beschikking, variërend van traditionele methoden tot het 'cross-referencen' van verschillende (door de personen gebruikte) IP-adressen (indien deze beschikbaar zijn). Op dit punt speelt voor de politie een 'kosten-batenafweging'. De moeite die de politie moet doen om binnen de gevonden groep personen de juiste persoon te identificeren, moet worden afgewogen tegen de maatschappelijke baten. Bij een ernstig misdrijf zal de politie meer middelen inzetten dan bij lichtere vergrijpen. Daarnaast speelt dat verschillende eenheden van de politie verschillende handelingsmogelijkheden tot hun beschikking hebben. Zo heeft Team High Tech Crime meer mogelijkheden dan de 'reguliere' politie, maar behandelt zij tevens andere typen zaken. Verbetering van de mogelijkheden tot identificatie op basis van IP-adres maakt het de politie mogelijk om meer lichtere vergrijpen op te volgen.

Kort gezegd zou een 'online identificatieplicht', waarbij alle gebruikers op internet één-op-één te identificeren zijn, vanuit opsporingsperspectief de proportionaliteit van het inzetten van opsporingsmiddelen vergroten, omdat minder onschuldigen betrokken zijn. Gestreefd wordt naar 1:1-identificatie. Suboptimaal, maar wel een verbetering op de huidige situatie is een oplossing waarbij de groep internetgebruikers (sterk) wordt verkleind. Uit gesprekken met de politie vernemen we dat een groepsgrootte van maximaal 25 personen een werkbaar aantal is. In België wordt een grens van maximaal 16 personen aangehouden.[21]

De problematiek van opsporing via publieke IP-adressen is niet gelimiteerd tot Nederland. Uit een survey van Europol blijkt dat ruim 80% van de opsporingsdiensten in de EU problemen ondervindt bij het opsporen van individuen op basis van gedeelde IPv4-adressen. [13]

---

[19] We kijken specifiek naar de politie, maar bevindingen gelden ook voor andere opsporingsdiensten.

[20] Merk op dat het CIOT een aantal jaar geleden regelmatig onder vuur lag, omdat de database veel vaker dan redelijkerwijs verwacht mocht worden werd geraadpleegd. Zie onder andere [www.bitsoffreedom.nl].

[21] Het is niet duidelijk hoe deze grens is bepaald. Er is niet per definitie een relatie tot opsporing.

2.3.2 Maatschappelijke kosten van opsporing op internet

Voorop staat dat onopgeloste misdaad een kostenpost op zichzelf is. Het verbeteren van (de precisie van) identificatie van gebruikers op basis van IP-adres brengt echter ook maatschappelijke kosten met zich mee. Allereerst zijn er de **kosten voor (technische en operationele) implementatie** van de maatregelen die nodig zijn om identificatie te verbeteren. Deze kosten kunnen neerslaan bij overheden en ISP's (die bijvoorbeeld extra databases moeten bijhouden of speciale apparatuur moeten aanschaffen). ISP's zullen de kosten (deels) doorberekenen aan hun klanten.

Privacy

Identificatie op basis van een IP-adres kan leiden tot een inbreuk op privacy. Drie aspecten spelen een rol bij het beoordelen van de proportionaliteit:

- Hoe groot is de privacy-inbreuk bij opsporing?
- Hoeveel persoonsgegevens worden er bijgehouden ten behoeve van identificatie?
- Heeft de identificatie-oplossing andere gevolgen voor privacy?

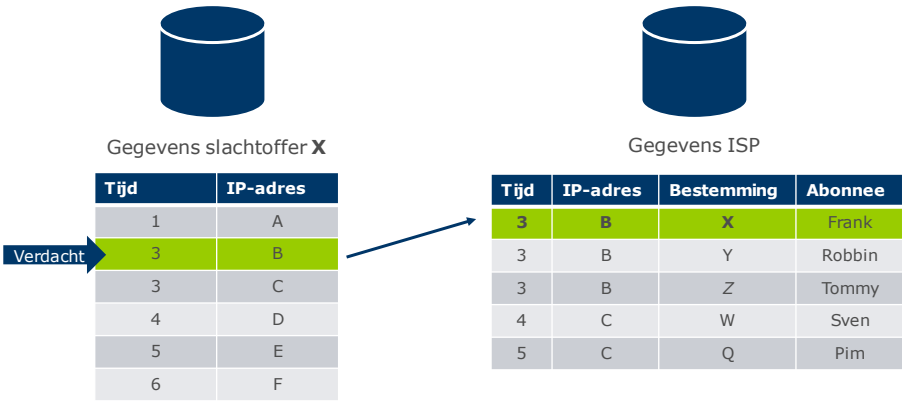
Privacy-inbreuk bij opsporing

Afhankelijk van de identificatie-oplossing leidt identificatie op basis van een IP-adres ofwel eenduidig tot een abonnee, ofwel tot een groep van mogelijk betrokken abonnees. In het eerste geval is de identificatie maximaal doeltreffend en is de privacy-inbreuk minimaal: alleen de personen die de betreffende opsporingsinstantie wenst mee te nemen in het verdere onderzoek (de abonnee en de eventuele medegebruikers van de aansluiting) worden geselecteerd.

In het tweede geval, waarin een IP-adres is gekoppeld aan een *groep* van abonnees, zal opsporing de geïdentificeerde groep abonnees moeten verkleinen om tot de juiste persoon te komen. Dit kan worden gedaan door combinatie met andere sporen (wellicht zijn er meerdere IP-adressen beschikbaar – alleen de daadwerkelijke verdachte zal in alle bijbehorende groepen voorkomen) of door nader onderzoek te doen naar de groepsleden. Met name in dit laatste geval is de privacy-inbreuk potentieel groot voor de onschuldige personen in de groep. Boven een bepaalde groepsgrootte (en afhankelijk van de zwaarte van het delict) zal een dergelijke inspanning niet meer proportioneel worden geacht te zijn, en is verdere identificatie op basis van het IP-adres niet mogelijk.

Het bijhouden van persoonsgegevens voor identificatie

Op basis van verkeersgegevens is het voor een ISP mogelijk om, bij gedeeld gebruik van een IP-adres en wanneer specifiekere informatie beschikbaar is (zoals een tijdstip of vindplaats van het IP-adres), een specifieke gebruiker te identificeren. In Nederland was dit tot voor kort de situatie: ISP's waren, ingevolge de in 2009 geïntroduceerde algemene bewaarplicht voor telecommunicatiegegevens, verplicht bij te houden welke abonnee met welke bestemming communiceerde, en op welk tijdstip. [14] Zoals Figuur 6 weergeeft, is identificatie in dat geval eenvoudig.



Figuur 6. Schematische weergave van de wijze van identificatie bij gedeelde IP-adressen op basis van verkeersgegevens

In het arrest Digital Rights Ireland (C-293/12 en C-594/12) verklaarde het Europese Hof de dataretentierichtlijn 2006/24 nietig. Naar aanleiding hiervan is de Nederlandse wetgeving rond de bewaarplicht door de rechter buiten werking gesteld in een vonnis van de voorzieningenrechter Den Haag van 11 maart 2015. [15] [16] Vervolgens is, in september 2016, het wetsvoorstel Aanpassing bewaarplicht telecommunicatiegegevens bij de Tweede Kamer ingediend. Dit wetsvoorstel voorziet in een herziening van de wettelijke regeling rond de bewaarplicht voor telecommunicatiegegevens ten behoeve van de opsporing van ernstige misdrijven.

In december 2016 heeft het Europees Hof van Justitie het 'Tele2-arrest' gewezen inzake het bewaren van telecommunicatiegegevens ten behoeve van opsporing en vervolging van strafbare feiten.[22] [17] Tele2 had aangegeven dat zij niet langer gegevens zal bewaren en de tot nu toe bewaarde gegevens zal vernietigen. Het algemeen bestuur van de nationale politie te Zweden heeft hiertegen een klacht ingediend. Tele2 deelde immers geen verkeers- en locatiegegevens meer met de politie, en volgens de politie was dit in strijd met een Zweedse regeling die het telecommunicatiediensten verplicht de abonnementsgegevens te delen met de politie indien die gegevens verband houden met een vermoeden van een strafbaar feit. Na onderzoek werd Tele2 bij nationaal besluit verplicht om gegevens te leveren. Tele2 heeft tegen dit besluit beroep en vervolgens hoger beroep ingesteld.

Uiteindelijk heeft de verwijzende rechter prejudiciële vragen aan het Hof van Justitie EU gesteld.[23] Het Hof oordeelde dat de desbetreffende bepalingen uit de e-privacyrichtlijn, tegen de achtergrond van het Handvest van de grondrechten, zich verzetten tegen een nationale regeling die, ter bestrijding van criminaliteit, voorziet in algemene en ongedifferentieerde bewaring van *alle* verkeersgegevens en locatiegegevens van *alle* abonnees en geregistreerde gebruikers betreffende *alle* elektronische communicatiemiddelen (punt 112), omdat de regeling verder gaat dan wat strikt noodzakelijk is (punt 107).

Naar aanleiding van het Tele 2-arrest is behandeling van het wetsvoorstel in de Tweede Kamer aangehouden. De minister van Justitie en Veiligheid heeft na bestudering van het arrest in maart 2018 aangekondigd dat het wetsvoorstel aanpassing behoeft, in die zin dat

[22] Het betreft de zaak van Tele2 Sverige AB tegen Post och telstryelsen (Hof van Justitie EU 21 december 2016; C-203/15) en de zaak van Secretary of State for the Home Department tegen Tom Watson, Peter Brice en Geoffrey Lewis (C-698/15).

[23] De andere zaak (C-698/15) betrof afzonderlijke beroepen van Watson, Brice en Lewis over de onverenigbaarheid van nationale wetgeving over het bewaren van communicatiegegevens met de art. 7 en 8 van het Handvest.

dit in sterk afgeslankte vorm wordt voortgezet, bestaande uit de voorziening met betrekking tot uitsluitend gebruikersgegevens. [18] Deze gegevens hebben geen betrekking op de communicatie tussen personen maar slechts op de identificatie van een gebruiker van een elektronische communicatiedienst en het gebruikte apparaat.

Daar het bijhouden van de benodigde precieze gegevens sinds het Tele2-arrest als onwenselijk wordt gezien en juridisch niet meer is toegestaan, is de vraag welke oplossingen, nu en in de nabije toekomst, mogelijk zijn om identificatie van individuen op basis van een publiek IPv4-adres mogelijk te maken. In hoofdstuk 3 behandelen we verschillende mogelijkheden, en hoofdstuk 4 de keuze daaruit in verschillende landen.

Overige negatieve gevolgen ten aanzien van privacy

Aandacht dient tot slot uit te gaan naar de mate waarin *private* partijen (denk aan advertentienetwerken) na het doorvoeren van de oplossingen ter verbetering van identificatie ook de mogelijkheid krijgen om personen op internet eenduidig te identificeren.

Wanneer iedere gebruiker een eigen IP-adres zou hebben, 'zien' aanbieders van internetdiensten dit unieke adres in plaats van het nu gebruikelijke gedeelde IP-adres. Dit is uiteraard nu al het geval op (vaste) netwerken waar geen NAT, maar (semi-statische) publieke IP-adressen worden gebruikt. Hoewel het bij toepassing van IPv6 denkbaar is dat gebruikers ook als zij wisselen tussen netwerken gevolgd kunnen worden, zijn voldoende technische mitigaties beschikbaar.[24] Daarnaast worden zogenaamde VPN-diensten steeds populairder om identificatie op basis van IP-adres door derde partijen te bemoeilijken. Om deze redenen behandelen we deze factor niet verder in het onderzoek – aangenomen wordt dat ze in generieke zin geldt en geen argument kan zijn om de ene oplossing boven de andere te verkiezen.

2.4 Huidige stand van zaken in Nederland

In Nederland zijn 1.283 organisaties bij ACM geregistreerd als "aanbieder van openbare elektronische communicatiediensten". [19] Het merendeel van de vaste en mobiele internetaansluitingen wordt echter verzorgd door een drietal partijen: KPN, T-Mobile en VodafoneZiggo.[25,26] We beschouwen identificatie op basis van IP-adres met name vanuit het perspectief van deze partijen, waarbij wordt aangenomen dat de bevindingen ook gelden

[24] Bij IPv6 wordt het eerste deel van het adres (net als bij IPv4) bepaald op basis van het netwerk. Anders dan bij IPv4 wordt het laatste deel in de regel niet 'uitgedeeld' door het netwerk (met een mechanisme als DHCP, wat overigens wel beschikbaar is voor IPv6 in de vorm van DHCPv6), maar bepaald op basis van het wereldwijd unieke hardwareadres (MAC) van de gebruiker. Wisselt een gebruiker tussen netwerken, dan blijft het achtervoegsel dus mogelijk alsnog hetzelfde. Het probleem is te ondervangen door gebruik te maken van zogenaamde *privacy extensions*. [61]

[25] De drie partijen bieden onder eigen naam internetdiensten aan. Daarnaast zijn zij onder diverse aanvullende labels in de markt (denk aan 'Hollands Nieuwe' van VodafoneZiggo, 'XS4ALL' van KPN en 'Ben' van T-Mobile).

[26] Tele2, de vier-na-grootste partij voor wat betreft marktaandeel, is inmiddels gefuseerd met T-Mobile Nederland. De netwerken zijn tot op zekere hoogte technisch gezien nog gescheiden.

voor kleinere ISP's en ISP's die capaciteit inkopen.[27] Tabel 1 geeft een overzicht van de marktaandelen en omvang van de IPv4-adresvoorraad van de grootste Nederlandse ISP's.

Tabel 1 Marktaandeel en IPv4-adresvoorraad van de grootste Nederlandse ISP's

ISP	Aantal vaste consumentenaansluitingen (mln) [28]	Aantal mobiele aansluitingen (mln) [29]	Voorraad IPv4-adressen (mln)[30]
KPN	4,1	7,6	7,1
VodafoneZiggo	3,3	4,9	5,9
T-Mobile Nederland	0,2	4,0	1,5
Tele2	0,1	1,2	1,6
Totaal	**7,7**	**17,8**	**16,0**

Merk op dat de vier grote ISP's verantwoordelijk zijn voor vrijwel alle vaste consumenten-aansluitingen in Nederland (het aantal is iets lager dan het aantal huishoudens in Nederland. [20]) en het merendeel van de mobiele aansluitingen.

De vier grote Nederlandse ISP's beschikken in totaal over zo'n 16 miljoen IPv4-adressen. De adressen worden op hoofdlijnen als volgt ingezet:[31]

1. Mobiele consumentenaansluitingen: ca. 800.000 IPv4-adressen beschikbaar. De drie operators hebben in totaal naar schatting zo'n 18 miljoen mobiele abonnees in Nederland.[32,33] Uit gesprekken met ISP's blijkt dat ongeveer 5% van de IPv4-adressen gebruikt wordt voor mobiele netwerken.
2. (Groot)zakelijke klanten, die veelal een blok IPv4-adressen toegewezen krijgen (ca. 7 miljoen IPv4-adressen).
3. Wi-Fi-hotspotdiensten, zoals Ziggo Wifispots. Abonnees van de ISP kunnen via deze hotspots gebruik maken van internettoegang via de modems van andere abonnees van dezelfde ISP.
4. Eigen infrastructuur van de internetaanbieder.

---

[27] Dit wordt 'wholesale' genoemd. Een ISP koopt hierbij toegang tot een toegangsnetwerk (bijvoorbeeld het DSL-netwerk van KPN of een FttH-netwerk) en voorziet zelf de diensten (waaronder de internetverbinding) voor de klant, vanaf een uitkoppelpunt van KPN. Op mobiele netwerken is het equivalent de *mobile virtual network operator* of MVNO.

[28] Met 'consumentenaansluitingen' worden hier ook (klein)zakelijke aansluitingen bedoeld die via hetzelfde aansluitnetwerk verlopen en/of een soortgelijke propositie betreffen. Cijfers op basis van de jaarverslagen van de ISP's.

[29] Ibid.

[30] Analyse Dialogic op basis van BGP-gegevens, in te zien via [bgp.he.net]. Meegeteld zijn IPv4-adressen die aangekondigd worden door een AS-nummer dat geregistreerd is op naam van het Nederlandse deel van de genoemde partijen ("KPN B.V.", "T-Mobile Netherlands B.V.", "Vodafone Libertel B.V." en "Tele 2 Nederland B.V.". In een aantal gevallen zijn dochterbedrijven meegenomen, zoals "KPN Internedservices B.V.'.

[31] Schatting op basis van gegevens die door de ISP's aan Dialogic zijn verstrekt, alsook BGP- en reverse DNS-gegevens.

[32] Met een abonnee wordt in deze context een lopend postpaid contract (meestal gekoppeld aan één, maar soms meerdere SIM-kaarten) of een *actieve* prepaid SIM-kaart bedoeld.

[33] Niet meegenomen in deze cijfers zijn MVNO's die zelf hun internettoegang faciliteren via een eigen APN.

Merk op dat in het gebruik van IPv4-adressen door ISP's adressen 'verloren' gaan doordat zij om technische redenen in blokken van vaste groottes worden toegekend aan een specifiek doel. Het aantal toegekende adressen kan daarbij in sommige gevallen hoger zijn dan het aantal benodigde adressen.

Vaste aansluitnetwerken

Op de Nederlandse vaste aansluitnetwerken krijgen vrijwel alle abonnees (tenminste één) publiek IPv4-adres. In de regel worden deze adressen (semi)statisch toegewezen. Op het netwerk van KPN, enkele kleinere ISP's, en op een deel van de Ziggo-aansluitingen krijgt een abonnee een IPv6-adres. Bij een deel van de Ziggo-klanten met een IPv6-aansluiting wordt een vorm van 4-naar-6 NAT toegepast voor het IPv4-verkeer. Grosso modo betekent dit dat (indien gegevens over de toewijzing worden bewaard en beschikbaar worden gesteld) eenduidige identificatie van een abonnee op vaste netwerken in de regel mogelijk is. Tabel 2 geeft een overzicht van de beschikbaarheid en implementatie van IPv4 en IPv6 op de Nederlandse vaste aansluitnetwerken.

Tabel 2 Overzicht beschikbaarheid en implementatie IPv4 en IPv6 op vaste aansluitnetwerken

ISP	IPv4 op vaste consumentenaansluitingen	IPv6 op vaste consumentenaansluitingen
KPN	Beschikbaar op alle aansluitingen, (semi)statische adrestoewijzing	Beschikbaar op alle aansluitingen op basis van dual stack met (semi)statische adrestoewijzing.
VodafoneZiggo	Beschikbaar op alle aansluitingen. Vrijwel overal (semi)statische adrestoewijzing. Voor sommige aansluitingen met IPv6 wordt DS-Lite ingezet, waarbij het IPv4-adres gedeeld wordt.	Beschikbaar op een beperkt aantal aansluitingen, als dual stack of DS-Lite, met (semi)statische adrestoewijzing.
T-Mobile Nederland	Beschikbaar op alle aansluitingen, (semi)statische adrestoewijzing	Niet beschikbaar
Tele2	Beschikbaar op alle aansluitingen, (semi)statische adrestoewijzing	Niet beschikbaar

Hoewel er op de vaste netwerken nauwelijks sprake is van een probleem ten aanzien van identificatie is het toch zinvol om te kijken naar de uitrol van IPv6 op deze netwerken. Dergelijke uitrol zou namelijk in theorie (zie paragraaf 3.3) IPv4-adressen kunnen vrijmaken voor gebruik op de mobiele netwerken. De voorgangers van Ziggo (UPC en 'former Ziggo') begonnen al in 2012 met de uitrol van IPv6, maar zetten het meerdere malen op een lager pitje. [21] [22] De laatste publieke mededeling van Ziggo rondom IPv6 stamt uit 2016, waarin het bedrijf aangeeft dat de uitrol nog enkele jaren zal gaan duren. [23] We verwachten op basis van inschattingen in de markt dat Ziggo in de komende jaren IPv6 stapsgewijs zal gaan uitrollen.

Mobiele aansluitnetwerken

Alle Nederlandse mobiele operators passen, op consumentenaansluitingen, een vorm van CG-NAT toe. Bij specifieke abonnementen (meestal bedoeld voor de zakelijke markt en machine-to-machine (M2M) toepassingen) worden vaste of dynamische publieke IPv4-adressen toegekend. Bij een enkele operator kan de klant (door instelling van de APN) kiezen voor

internettoegang via NAT of via een dynamisch publiek IPv4-adres.[34] Tabel 3 geeft een overzicht van de beschikbaarheid en implementatievorm van IPv4 en IPv6 op de Nederlands mobiele netwerken.

Tabel 3 Overzicht beschikbaarheid en implementatie IPv4 en IPv6 op Nederlandse mobiele netwerken

ISP	IPv4 op mobiele consumentenaansluitingen	IPv6 op mobiele consumentenaansluitingen
KPN	Beschikbaar, achter CG-NAT	Niet beschikbaar, uitrol vanaf 30 september 2019 aangekondigd [24]
VodafoneZiggo	Beschikbaar, achter CG-NAT	Niet beschikbaar
T-Mobile Nederland	Beschikbaar, achter CG-NAT	Niet beschikbaar
Tele2	Beschikbaar, achter CG-NAT	Niet beschikbaar

De mate waarin een abonnee kan worden geïdentificeerd (de groepsgrootte, cq. het aantal abonnees dat potentieel van hetzelfde publieke IPv4-adres gebruik maakt) is sterk afhankelijk van het aantal IPv4-adressen dat door een operator wordt gebruikt voor CG-NAT, de vorm van CG-NAT, en het aantal abonnees dat gebruik maakt van CG-NAT. Op basis van de gegevens die de drie operators verstrekten, ligt de groepsgrootte voor mobiele aansluitingen bij benadering tussen de 84 en 84.000 – het gemiddelde, gewogen naar marktaandeel, ligt naar schatting rond de 15.600.[35]

Op de mobiele netwerken van de drie Nederlandse operators wordt op dit moment geen IPv6 aangeboden op reguliere aansluitingen.[36] De plannen voor het uitrollen van IPv6 lopen sterk uiteen tussen de Nederlandse mobiele operators. Van de drie grote mobiele ISP's geeft er één in het openbaar aan bezig te zijn met IPv6-uitrol. [24] De andere operators geven aan IPv6 niet op de planning te hebben of niet te kunnen aangeven of IPv6 binnen afzienbare tijd zal worden uitgerold.

De verschillen tussen de mobiele ISP's hebben verschillende oorzaken. Uit gesprekken met de ISP's blijkt dat een van de voornaamste oorzaken hiervoor is de beperkte vraag vanuit de markt. ISP's geven aan dat het leveren van een goede dienst het voornaamste doel is van een ISP, en dat de technologische realisatie van ondergeschikt belang is. Oftewel, wanneer een ISP zijn diensten kan leveren met behulp van IPv4 en IPv6 geen duidelijk voordeel oplevert, dan wordt een overstap naar IPv6 als redundant ervaren. Wanneer de vraag vanuit de markt naar IPv6 toeneemt zal een ISP om competitief te blijven, zijn diensten ook over IPv6 moeten aanbieden. De vraag vanuit de markt naar IPv6 blijft echter achter, en ISP's voorzien geen toename in vraag in de toekomst. Daarom is IPv6 ook niet in de roadmaps van ISP's opgenomen.

De andere oorzaak is technologische (en bijbehorende organisatorische) afhankelijkheid van IPv4. Wanneer een ISP de keuze maakt om het gebrek aan IPv4-adressen op te lossen door CG-NAT in te zetten, moet een ISP verschillende investeringen doen. Enerzijds moet een ISP

[34] Dit stelt abonnees in staat gebruik te maken van toepassingen die een publiek IPv4-adres vereisen. Operators geven als voordeel van CG-NAT aan dat ongewenst verkeer dat binnenkomt vanaf het internet (denk aan portscan- en DDoS-verkeer) het toestel niet bereikt, en dan ook niet voor rekening van de klant kan komen. Eenzelfde vorm van bescherming is echter ook mogelijk bij gebruik van publieke IPv4-adressen door toepassing van een 'stateful' firewall.

[35] Op basis van gefundeerde aannames voor wat betreft Tele2.

[36] Grootzakelijke klanten kunnen, op basis van een eigen APN, dit eventueel wel doen. Het gaat in die gevallen echter niet meer om openbare internetaansluitingen.

investeren in apparatuur om CG-NAT mogelijk te maken. Anderzijds moet een ISP investeren in de organisatie rondom CG-NAT. Denk bijvoorbeeld aan billing. Er moet worden geregistreerd hoeveel gebruik van het internet door welk abonnement plaatsvindt, om later de kosten in rekening te kunnen brengen (vooral bij mobiel waar gebruik nog vaak 'gecapped' is per type abonnement). Dit resulteert in *sunk costs* voor IPv4 en investeringen in een andere standaard (met bijbehorende organisatie) zullen niet direct evidente voordelen opleveren vanuit het perspectief van de ISP.

2.5 Conclusie

Om het groeiend aantal apparaten aan te kunnen sluiten op internet moeten apparaten en gebruikers IP-adressen delen. Hiervoor zijn verschillende technische oplossingen beschikbaar. Een ISP kan IPv4-adressen dynamisch toewijzen; hierbij delen abonnees hetzelfde IP-adres, maar nooit tegelijkertijd. In situaties waarbij het aantal beschikbare IPv4-adressen *veel* kleiner is dan het aantal apparaten dat gelijktijdig online is, is het nodig IPv4-adressen *gelijktijdig* te delen tussen gebruikers. Dit is mogelijk door toepassing van *network address translation* (NAT) gateways of carrier grade NAT (CG-NAT).

Aan enkel een IP-adres hebben opsporingsdiensten te weinig informatie om een onderzoek te starten, omdat dit zonder aanvullende gegevens niet herleidbaar is naar één persoon. Het Europees Hof van Justitie heeft echter geoordeeld dat ISP's en andere (telecommunicatie)aanbieders niet verplicht mogen worden tot algemene en ongedifferentieerde bewaring van *alle* verkeersgegevens en locatiegegevens van *alle* abonnees en geregistreerde gebruikers betreffende *alle* elektronische communicatie-middelen (Tele2-arrest). Er moet dus gezocht worden naar andere oplossingen om identificatie van individuen op basis van een publiek IPv4-adres mogelijk te maken. Daarbij spelen maatschappelijke afwegingen zoals privacy en doorberekening van kosten ook een rol.

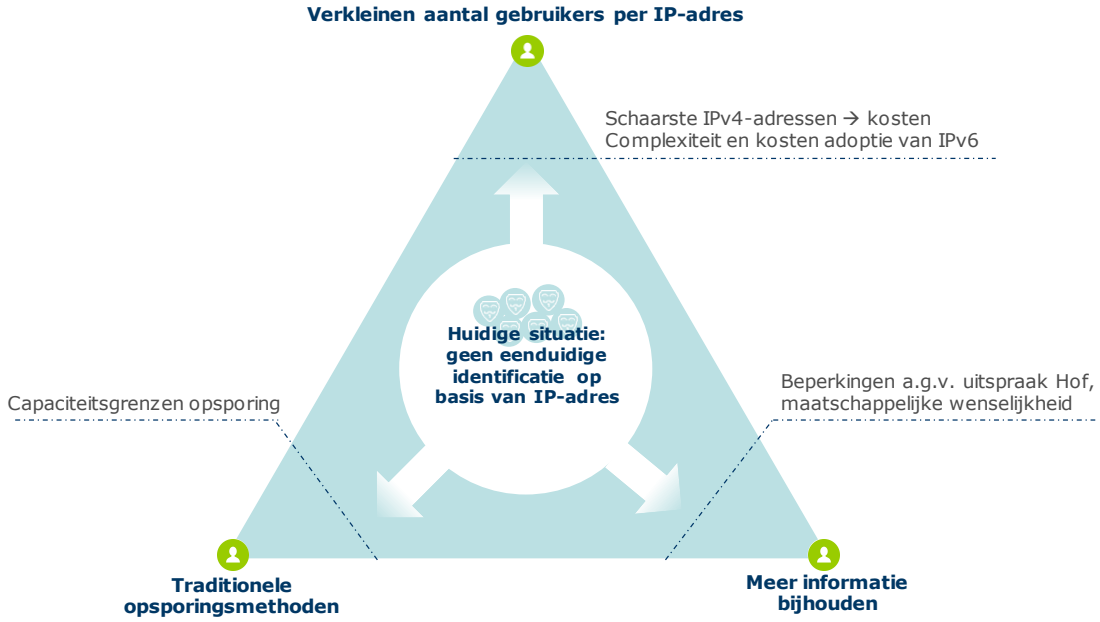
De problematiek ligt nadrukkelijk bij mobiele netwerken en consumentenaansluitingen. Bij vaste netwerken (huisaansluitingen) zijn er veel minder wisselingen in IP-adres en is de informatie specifiek genoeg om verder onderzoek te doen.

3 Mogelijkheden voor verbetering

In dit hoofdstuk bespreken we de verschillende mogelijkheden voor betere identificatie in het belang van opsporing. We starten met een overzicht van de oplossingsrichtingen waarop de mogelijkheden kunnen worden geplot (paragraaf 3.1). In de daaropvolgende paragrafen (3.2, 3.3, 3.4, 3.5 en 3.6) zullen we per mogelijkheid stilstaan bij de technische implementatie, de kosten en de overwegingen die spelen. Tot slot presenteren wij in Tabel 7 een overzicht van de mogelijkheden inclusief de voor- en nadelen.

3.1 Overzicht oplossingsrichtingen

Zoals in hoofdstuk 2 is geschetst, is de kern van het probleem dat abonnees van ISP's als gevolg van schaarste hetzelfde publieke IPv4-adres delen, waardoor zij niet meer eenduidig kunnen worden geïdentificeerd. Logischerwijs volgen uit deze probleemstelling drie oplossingsrichtingen.



Figuur 7 Schematisch overzicht mogelijkheden identificatie gebruikers

Figuur 7 toont schematisch deze drie fundamentele oplossingsrichtingen voor het vergroten van de identificatiekans:

1. **Verkleinen van het aantal gebruikers per IP-adres.** Er zouden méér publieke IP-adressen kunnen worden toegevoegd, zodat aan iedere abonnee een eigen adres kan worden toegekend. Dit maakt het toepassen van NAT overbodig en lost daarmee het persoonsidentificatieprobleem op.

2. **Meer inzet van traditionele opsporingsmethoden.** Opsporingsdiensten zouden genoegen kunnen nemen met minder eenduidige identificatie, (het aantal abonnees dat kan worden geassocieerd met één IP-adres is groter dan 1; we noemen dit verderop de 'groepsgrootte') en (op de huidige voet voortgaand) traditionele

opsporingsmethoden blijven inzetten voor nadere identificatie. Zoals eerder aangegeven heeft dit negatieve consequenties voor de mate waarin zaken worden opgepakt en opgelost.

3. **Meer informatie bijhouden.** Er kan méér informatie worden bijgehouden. Zodra immers precies bekend is welke abonnee op welk moment met welk adres een verbinding opzet, zou deze met deze informatie een abonnee kan worden geïdentificeerd.

Binnen de driehoek (cq. langs de oplossingsrichtingen) bevinden zich verschillende specifieke *mogelijkheden.* Naast het feit dat daarin de ene richting wordt afgewogen tegen de andere, kennen zij ieder een eigen kostenplaatje en overige overwegingen. Uit het onderzoek, waarbij gebruik is gemaakt van literatuurstudie en gesprekken zijn gevoerd met experts en de diverse operators, is een aantal specifieke (technische) mogelijkheden naar voren gekomen.

3.2 Mogelijkheid 1: Het uitrollen en adopteren van IPv6

IPv6 biedt, ten opzichte van voorganger IPv4, als grootste voordeel dat er substantieel meer adressen beschikbaar zijn: 2^{128} in plaats van 2^{32} – zoals eerder beargumenteerd is dat meer dan voldoende om ieder hoofd van de wereldbevolking over een zeer groot aantal (namelijk ca. 50 quadriljard per persoon[37]) adressen te laten beschikken.

De overgang van IPv4 naar IPv6 is echter complex. Dit komt omdat IPv4 en IPv6 niet compatibel met elkaar zijn: verkeer dat met IPv4 wordt verstuurd, is min of meer volledig gescheiden van IPv6-verkeer en andersom. Communicatie kan alleen op basis van IPv6 plaatsvinden als beide partijen IPv6 ondersteunen. ISP's zijn terughoudend met de adoptie van IPv6, omdat dit betekent dat moet worden geïnvesteerd in aanpassingen van CPE's (apparatuur bij consumenten thuis: kabelmodems, ADSL-modems, et cetera). Ook is het uitrollen van IPv6 een risico, daar verschillende applicaties die consumenten gebruiken in eerste instantie wellicht niet meer zullen werken (en de ISP hiervoor verantwoordelijk wordt gehouden). Daarnaast ondersteunt, naar inschatting van de mobiele ISP's, een groot deel van de (oudere) machine-to-machine apparaten mogelijk alleen IPv4. Exacte cijfers hierover zijn echter nauwelijks beschikbaar.

Uiteindelijk is een overstap op IPv6 onafwendbaar, zo blijkt uit de literatuurstudie en de interviews. De adoptie van IPv6 verloopt nog langzaam, niet in de laatste plaats omdat er voor eindgebruikers nauwelijks voordelen aan de techniek zitten en het voor ISP's een vrij fundamentele ingreep in het netwerk betreft. Vanwege de uiteindelijke noodzaak, het feit dat IPv6 op technisch vlak wel degelijk voordelen biedt (NAT is overbodig, DHCP-servers zijn overbodig, het is veiliger vanwege het IPsec-protocol, IPv6 kent een efficiëntere packetstroom en het is gebouwd op de toekomst), de sterke netwerkeffecten[38] bij adoptie, en de introductie van 5G [25], is het denkbaar dat de adoptie van IPv6 de komende jaren sterk

[37] Een quadriljard heeft 27 nullen.

[38] Hiermee wordt, in de innovatieliteratuur, bedoeld dat de waarde van een innovatie (in dit geval IPv6) stijgt naarmate een groter aantal gebruikers deze adopteert. Hoe meer gebruikers IPv6 adopteren, hoe meer gebruikers bereikbaar zijn via IPv6, en hoe hoger de waarde. In de IT-wereld is deze wetmatigheid bekend als Metcalfe's Law, die stelt dat de waarde van een netwerk kwadratisch toeneemt met het aantal aangesloten gebruikers. Mogelijk stijgt met het aantal gebruikers, en de toegenomen waarde, ook de kans dat anderen de innovatie adopteren – het *bandwagon effect* – waarmee adoptie versnelt.

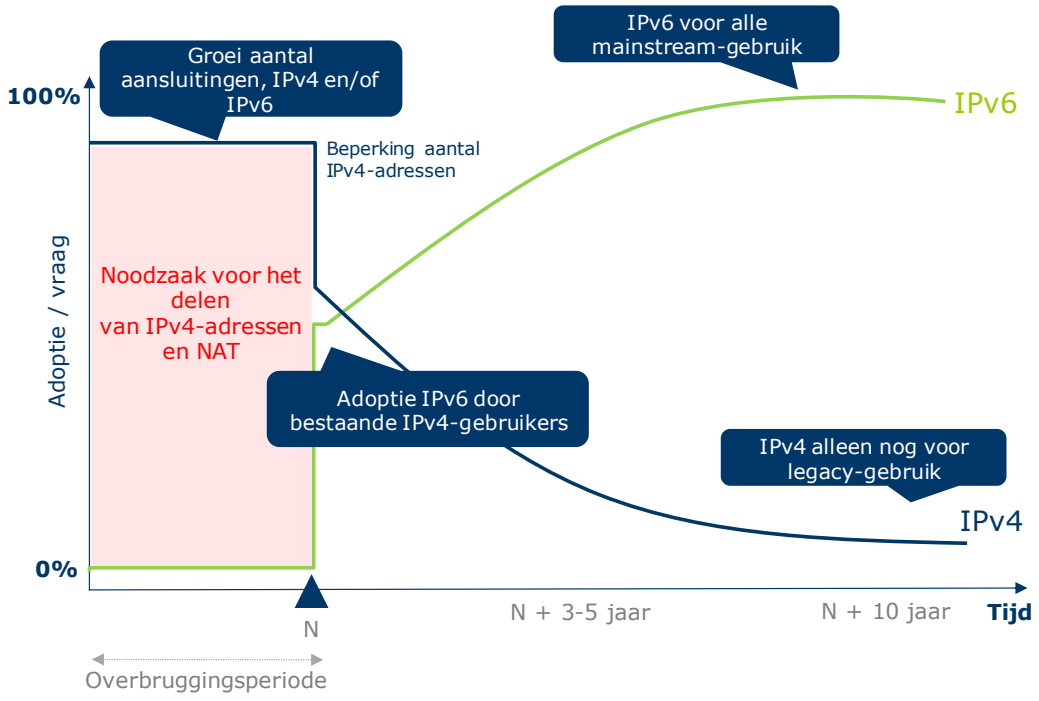
versnelt. Naarmate de adoptie van IPv6 (sterk) stijgt, zal de vraag naar IPv4-adressen naar verwachting afnemen (zie

Figuur 8). Dit betekent dat het inzetten van NAT-oplossingen steeds minder vaak nodig zal zijn. NAT-oplossingen moeten dus worden gezien als een 'overbruggingsoplossing' tussen IPv4 en IPv6.

In die zin kan er een onderscheid worden gemaakt tussen de directe en lange termijneffecten bij de overstap naar IPv6. Zodra IPv6 wordt uitgerold, zal direct een percentage van de gebruikers IPv6 gaan gebruiken, omdat de apparaten van eindgebruikers dit simpelweg al ondersteunen. Er is dus geen sprake van een geleidelijke adoptie, maar van een enorme sprong ineens, gevolgd door een 'adoptiestaartje'. Precieze percentages zijn moeilijk te bepalen, maar gedacht kan worden aan 80% direct, 90% na drie tot vijf jaar en 100% na nog eens tien jaar.[39]

Momenteel is niet alle inhoud op internet via IPv6 te bereiken. Op basis van de Cisco-data kunnen we concluderen dat in Nederland circa 64% van de inhoud via IPv6 beschikbaar is. [26] Met andere woorden, als morgen opeens alle gebruikers over IPv6 beschikken en kunnen gebruiken, dan zou 64% van het internetverkeer over IPv6 verlopen. Ook hier zal sprake zijn van een adoptiestaartje. Na tien jaar zal er nog steeds een kleine set websites en diensten overblijven die niet over IPv6 te bereiken is.

Beide effecten bepalen, vermenigvuldigd, het verloop van de hoeveelheid netto verkeer dat via IPv6 zal verlopen (in bovengenoemd voorbeeld: 64% x 80%: circa de helft van het verkeer zal vanaf inschakeling over IPv6 verlopen). De consequentie is dat direct ook minder verkeer over IPv4 zal lopen (zie onderstaande figuur).



[39] Dit betreft een schatting op basis van de APNIC-gegevens van landen die de overstap al hebben gemaakt.

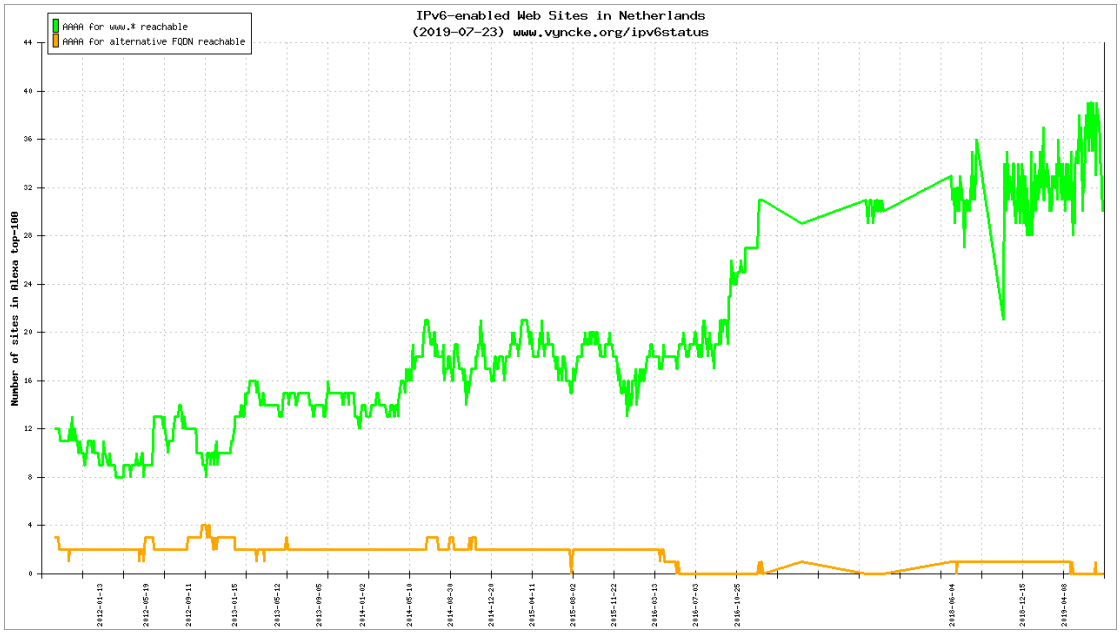
Figuur 8. De overgang van IPv4 naar IPv6 en de (tijdelijke) noodzaak voor het delen van IPv4-adressen. [27, p. 4], bewerking Dialogic.

3.2.1 Technische implementatie

Om over te kunnen schakelen op IPv6 moeten zowel de applicatie, het eindgebruikersapparaat, het netwerk, als de dienst IPv6 ondersteunen. Zodra het mobiele netwerk IPv6 ondersteunt, kan (in gevallen waar een applicatie of dienst geen IPv6 ondersteunt) een tussenoplossing wordnen geboden.

IPv6-ondersteuning door diensten

Naar schatting is circa 35% van de ".nl"-websites bereikbaar via IPv6. Circa 80% van de ".nl"-domeinen is vermeld op een DNS-server welke IPv6 ondersteunt, wat een indicatie is voor ondersteuning van IPv6 door de hoster van de website. [28] Figuur 9 toont de ontwikkeling van dit percentage over tijd voor de top 100 '.nl'-websites als bepaald voor Alexa. Merk op dat de set onderzochte websites per november 2016 is vastgezet – nieuwe (populaire) websites komen niet in deze statistieken voor. Het ".nl"-domein staat daarmee op plaats 29 wereldwijd.



Figuur 9 Aantal websites uit de Alexa top-100 voor Nederland welke bereikbaar zijn over IPv6 [28]

IPv6-ondersteuning door mobiele apparaten en apps

De meeste (moderne) mobiele apparaten (smartphones, tablets) ondersteunen IPv6. Apple verplicht ontwikkelaars van applicaties voor iOS (iPhone, iPad) die applicaties in de App Store willen publiceren om ondersteuning te bieden voor IPv6-only-netwerken. [29]

De Play Store voor Android van Google kent geen verplichting tot IPv6-ondersteuning. Sinds Android 4.3 wordt ondersteuning geboden voor 464XLAT, welke IPv4-verkeer van applicaties over een IPv6-only-verbinding kan laten verlopen. [30] Een inventarisatie uit 2012 laat zien dat 85% van de top 200 gratis apps voor de destijds courante versie van Android zonder problemen werkte op het IPv6-only-netwerk van T-Mobile US. [31]

Samen hebben iOS en Android in Nederland meer dan 99% marktaandeel als het gaat om smartphones. [32] [33] Dat wil niet zeggen dat alle mobiele apparaten die zijn aangesloten op een mobiel netwerk IPv6 ondersteunen. Naast tablets en laptops (waar de variatie in

besturingssystemen en ouderdom iets groter is) worden mobiele netwerken gebruikt door machine-to-machinetoepassingen. Dit zijn veelal zeer specifieke oplossingen die voor lange tijd worden ingezet (denk aan communicatie ten behoeve van de borden bij bushokjes, slimme meters, het volgen van voertuigen, beveiligingscamera's, et cetera). De kans dat deze apparaten geen IPv4 ondersteunen, is groot. Daarnaast wordt voor dergelijke toepassingen vaker een vast IPv4-adres gevraagd.

Technische oplossingen voor legacy IPv4

Er is een aantal oplossingen denkbaar waarin zowel IPv4- als IPv6-connectiviteit via dezelfde aansluiting kan worden geleverd. De meest voor de hand liggende en eenvoudige is een 'dual-stack'-oplossing – hierbij worden simpelweg een IPv4- en een IPv6-aansluiting naast elkaar aangeboden. Naast dual stack kan ook gelijktijdig IPv4- en IPv6-connectiviteit worden geboden op basis van technologieën waarbij het IPv4-verkeer wordt 'getunneld' over het IPv6-kanaal (DS-Lite en 464XLAT).

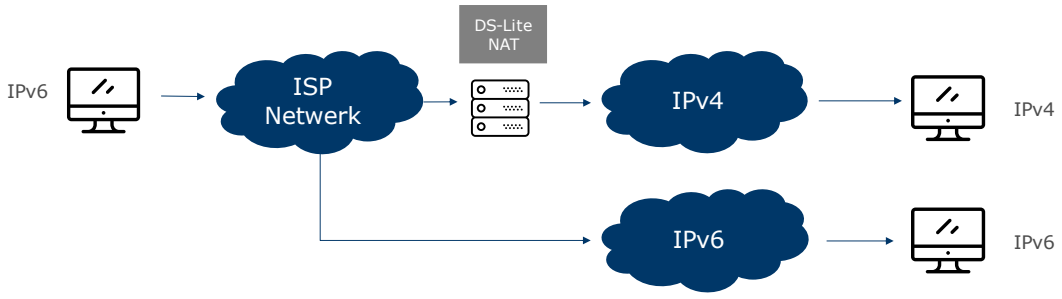
Dual stack

Bij een dual stackaansluiting krijgt de afnemer zowel een IPv4-adres (al dan niet achter NAT) als een IPv6-adres, en een onderlaag die beide protocollen kan transporteren. Een dual-stackoplossing ligt echter minder voor de hand op mobiele netwerken, omdat dit betekent dat (in het LTE-protocol) meerdere logische verbindingen moeten worden opgezet. Dat leidt tot extra belasting van de accu van smartphones en is lastig vanuit perspectief van 'provisioning' (het door het netwerk voorzien van eindapparaten met de juiste instellingen).

Voor vaste netwerken bestaat er de Dual Stack-Lite (DS-Lite) technologie; voor mobiele netwerken bestaat er 464XLAT. Beide technologieën kunnen worden gebruikt om IPv4 en IPv6 te laten communiceren.

DS-Lite

Bij DS-Lite [34] verloopt de communicatie tussen de eindgebruiker en de ISP standaard over IPv6. Eventueel IPv4-verkeer wordt aan de zijde van de abonnee (bijvoorbeeld door de modemrouter) 'omgeschreven' naar een IPv6-pakket. Aan de zijde van de ISP wordt een dergelijk pakket weer vertaald naar een IPv4-pakket, en gaat deze als zodanig het internet op. Hierbij vindt in de regel (maar niet noodzakelijkerwijs) NAT plaats met deling van publieke IPv4-adressen tussen abonnees. Doordat IPv6 beschikbaar is, loopt het merendeel van het verkeer van een eindgebruiker rechtstreeks over IPv6 – de 'truc' om IPv4-verkeer af te kunnen wikkelen, is daarmee echt een overgangsmaatregel.

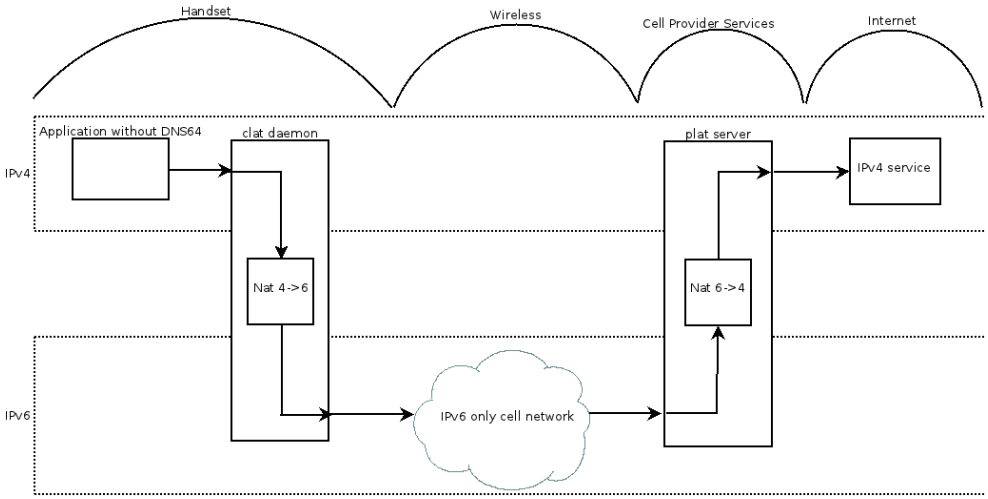


Figuur 10. Schematische weergave van de werking van DS-Lite

464XLAT

Op mobiele aansluitingen wordt om technische redenen bij voorkeur niet gewerkt met een dual-stackoplossing. In plaats daarvan wordt een IPv6-only-verbinding gebruikt; applicaties die met IPv6 overweg kunnen, maar moeten communiceren met een IPv4-dienst, gebruiken DNS64 en NAT64 (aan de providerzijde; ook bekend als 'PLAT'). Legacy-applicaties die geen

IPv6 ondersteunen, maken aanvullend gebruik van CLAT. Deze verzameling oplossingen heet 464XLAT [35].



Figuur 11 Schematische weergave van de werking van 464XLAT op Android (bron: [30])

Identificeerbaarheid voor het legacy IPv4-verkeer

Wanneer IPv4 door een ISP na uitrol van IPv6 zou worden 'uitgezet' of wanneer het IPv4-verkeer gaat verlopen via CG-NAT (zoals het geval bij DS-Lite en 464XLAT), komt IPv4-adresruimte vrij. Deze adressen kunnen deels worden herverdeeld om de druk op IPv4-adressen voor mobiel te verminderen, al moet een klein deel bewaard blijven voor het verkeer dat van IPv6 naar IPv4 moet worden getunneld door middel van NAT64. Geen van de ISP's heeft dit tot nu toe overigens gedaan, en we verwachten dat de meeste ISP's tenminste de komende vijf tot tien jaar nog IPv4 zullen ondersteunen.

Merk op dat wanneer CG-NAT wordt toegepast voor IPv4-verkeer, een van de andere in dit onderzoek benoemde oplossingsrichtingen moet worden gekozen voor dit verkeer.

3.2.2 Kosten

De kosten voor deze oplossing zijn op te delen in kosten voor de upgrade van netwerkcomponenten en organisatorische kosten. De kosten van IPv6-adressen zijn, in tegenstelling tot de kosten voor IPv4 adressen, verwaarloosbaar. Een "/36"-IPv6-blok[40] heeft in totaal $2^{128 - 36} = 2^{92}$ adressen. ARIN 'verhuurt' dergelijke "/36"-blokken voor 500 dollar per jaar. Eén IPv6-*adres* is daarmee praktisch gezien gratis.

Uit gesprekken met leveranciers van netwerkapparatuur komt naar voren dat een overstap naar IPv6 een aantal upgrades vereist. Met name:

1. DNS. Van '4 naar 4', naar '6 naar 4'
2. Router: GGSN/PGW moet IPv6 ondersteunen
3. NAT: Van '4 naar 4', naar '6 naar 4'
4. CPE: moet IPv6 ondersteunen

[40] Met de '/' notatie wordt aangegeven hoeveel IPv4-adressen een 'blok' aan IPv4 adressen bevat. Het cijfer na de '/' geeft aan hoeveel bits van het IPv4-adres gereserveerd zijn voor het 'subnet'. Hoe lager het aantal na de /, des te meer IPv4-adressen er in één blok beschikbaar zijn. Het aantal IPv4 adressen kan worden bepaald door $2^{32} - 2^{\text{getal na '/'}}$

Om 464XLAT te realiseren, is er naast de implementatie in de mobiele apparaten ook een upgrade nodig in de router (waaronder GGSN/PWG en NAT). De NAT (van IPv6 naar IPv4) kan zowel fysiek als virtueel plaatsvinden binnen de router. Voor het mobiele netwerk komt NAT (IPv4 naar IPv4) al veel voor. Als een provider van NAT44 naar NAT64 wil, betekent dit vaak geen drastische aanpassingen in het netwerk. Als NAT44 al in gebruik is (wat eerder de regel is dan uitzondering voor mobiele netwerken) dan volstaat vaak een software/firmware update om NAT44 naar NAT64 om te zetten. Daarnaast moet de DNS-server naar DNS64 worden geüpgraded. DNS is maar een beperkt onderdeel van de infrastructuur en soms volstaat een upgrade van de bestaande DNS al.

Ook voor vaste netwerken dienen onderdelen van het netwerk geüpgraded te worden bij een migratie naar IPv6. In een migratie van IPv4 naar DS-Lite betekent dit een NAT64 component dat IPv6-adressen kan vertalen naar IPv4-adressen. Afhankelijk van bestaande infrastructuur kunnen de kosten sterk oplopen. Wanneer er nog geen NAT44 component in het netwerk is opgenomen, dient compleet nieuwe apparatuur te worden aangeschaft. Daarnaast dient CPE bij de klanten ook deze technologie te ondersteunen. Modems en routers bij gebruikers dienen te worden geüpgraded wanneer deze geen DS-Lite ondersteunen. Voor vaste netwerken is het dus voor de hand liggend dat de adoptie van IPv6 minder snel verloopt dan voor mobiele netwerken (waar de CPE doorgaans IPv6 ondersteunt).

Naast technische kosten worden er bij de overstap naar IPv6 ook organisatorische kosten gemaakt. Onder de organisatorische kosten vallen het trainen van personeel en het opzetten van een parallel billing en provisioning systeem. De systemen moeten gedurende de periode waarin dual-stack wordt aangeboden naast elkaar bestaan om zo IPv4 en IPv6 klanten te bedienen. Kosten worden niet alleen gemaakt in het netwerk en technisch personeel. De organisatorische kosten vertalen zich ook naar de 'voorkant' van de organisatie. Customer service moet training krijgen om met nieuwe problematiek om te gaan die IPv6 introduceert aan de klantzijde.

Hoe snel kan een mobiele ISP IPv6 uitrollen?[41]

Implementatie van IPv6 in een mobiel netwerk wordt vaak gedaan als onderdeel van een langere termijnstrategie, waarbij de diverse netwerkelementen en de ondersteunende IT-systemen geleidelijk aan gereed gemaakt worden voor IPv6-only mobiele gebruikers. Bij iedere upgrade wordt IPv6 in de vereisten meegenomen. Er zijn echter mobiele ISP's die gekozen hebben voor een strategie waar IPv6 geen onderdeel uitmaakt van de technologische 'roadmap'. De leveranciers van mobiele netwerkapparatuur leveren al jaren apparatuur die klaar is voor IPv6; het is aan de operator of IPv6 ook daadwerkelijk geactiveerd, geconfigureerd en getest wordt. Ook het grootse deel van de mobiele randapparatuur (o.a. Android- en Apple-toestellen) zijn IPv6-ready. De termijn die een mobiele ISP nodig heeft om IPv6 te adopteren hangt daarmee vrijwel uitsluitend samen met de reeds gedane voorbereidende investeringen in IPv6.

Bij de implementatie van IPv6 is een groot aantal netwerkelementen en ondersteunende IT-systemen betrokken. De eerst stap bestaat meestal uit een inventarisatie van alle betrokken onderdelen. Te denken valt aan (ten minste):

- Elementen in het mobiele netwerk, zoals HSS (Home Subscriber System), PCRF (Policy en Charging Rules Function), MME (Mobility Management Entity), S-GW,

[41] Onderstaande is gebaseerd op internationale ervaring vanuit het onderzoeksteam, gestaafd met de indicaties van de Nederlandse ISP's.

P-GW, IMS (IP Multimedia System), OCS (Online Charging System), systemen voor legal intercept, en diverse andere componenten.
- IPv6-transit
- IPv6-transportnetwerk.
- Een combinatie van NAT64, DNS64 en 464XLAT om IPv6-only mobiele gebruikers in staat te stellen om toch IPv4-content te kunnen bereiken.
- Roaming-upgrades. Lang niet alle buitenlandse netwerken ondersteunen IPv6. Er zal moeten worden ingeregeld dat deze klanten in dat geval terugvallen naar IPv4.
- IT support systemen, billing, provisioning, fraudedetectie, et cetera moeten worden bijgewerkt om met IPv6-adressen te kunnen omgaan (denk aan het wijzigen van databases en uitwisselingsformaten/koppelingen waarin adressen voorkomen).

Een inventarisatie vraagt snel enkele maanden. Daarna wordt een migratiestrategie ontwikkeld, en worden te upgraden netwerkelementen aanbesteed. Dergelijke aanbestedingen nemen enkele maanden in beslag, alsook de daarop volgende tests en implementatie.

Vervolgens wordt in de regel uitrol gestart met een selecte groep klanten. Parallel daaraan zal de klantenservice moeten worden opgeleid om vragen die betrekking hebben op de migratie van IPv4 naar IPv6 en nieuwe issues af te handelen. Pas wanneer dit geregeld is, kan de migratie met grotere aantallen klanten plaatsvinden. Tijdens de migratie worden tot slot waarschijnlijk scenario's ontdekt (denk aan legacytoepassingen) waarvoor specifieke oplossingen moeten worden gevonden.

Uit het bovenstaande volgt dat het uitrollen van IPv6, afhankelijk van de reeds getroffen voorbereidingen, een proces van enkele maanden tot meer dan een jaar kan zijn. Hoewel de bouwstenen voor IPv6 bij de Nederlandse operators aanwezig zijn, verschillen zij sterk in de mate van voorbereiding.

3.2.3 Overwegingen

De uitrol van IPv6 is een logische volgende stap. Niet alleen vanwege de directe voordelen voor de ISP's, maar ook omdat het basis infrastructuur wordt. Het betreft dus investeringen die ISP's uiteindelijk toch gaan doen om niet achterop te raken in de markt.

Daarnaast is de identificatie van gebruikers met IPv6 zeer gemakkelijk, want gebruikers kunnen een fixed IP-adres (of een set aan) krijgen zonder dat deze gedeeld hoeft te worden met andere gebruikers. De ISP hoeft dus slechts te registreren wie welk IPv6-adres heeft ontvangen (iets wat al nodig is voor de bedrijfsvoering van een ISP). Wanneer er een strafbaar feit is gepleegd, kan aan de hand van één IPv6-adres één abonnee worden geïdentificeerd.

De uitrol van IPv6 vindt in Nederland vrijwel uitsluitend en beperkt plaats op vaste aansluitnetwerken. Wanneer alle vaste aansluitingen in Nederland IPv6 zouden ondersteunen, en alle daar gebruikte IPv4-adressen zouden vrijkomen (wat onwaarschijnlijk is gezien het feit dat ook IPv4 nog langere tijd zal worden aangeboden – zie elders) zouden er nog steeds niet genoeg IPv4-adressen zijn om alle mobiele aansluitingen te voorzien van een eigen IPv4-adres. Dit komt doordat de mobiele markt op zichzelf al groter is dan het totaalaantal IPv4-adressen dat Nederlandse ISP's in bezit hebben. Daarnaast dragen de recente ontwikkelingen op het gebied van IoT bij aan de noodzaak om toe te gaan naar IPv6.

De tussenoplossingen voor IPv6 zijn nodig om met IPv6 ook het IPv4-deel van het internet te bereiken. Er zal zolang er IPv4 wordt gebruikt verkeer naar het IPv4-deel getunneld moeten worden wil een ISP dit als dienst kunnen aanbieden. Het deel dat naar IPv4 wordt getunneld, verloopt via NAT. Al dit verkeer blijft 'ontastbaar' voor opsporingsdiensten. Daarnaast zien we ook dat klanten problemen ondervinden bij een switch naar IPv6. Technologie die in een thuisnetwerk geen IPv6 ondersteunt, kan mogelijk niet meer werken (denk aan game consoles, IP-camera's, etc.).

Door uitrol van IPv6 krijgen gebruikers die nu (achter NAT) geen eigen IP-adres hebben dat ineens wel, waardoor zij beter volgbaar kunnen worden voor derde partijen (denk aan advertentienetwerken). Hoewel er ten opzichte van deze situatie mogelijk een verslechtering van de privacy optreedt, moet daarbij worden aangetekend dat (1) de nieuwe situatie in feite gelijk wordt aan die op vaste netwerken (waar alle gebruikers nu al een semi-vast IPv4-adres krijgen) en (2) de AVG onverminderd van kracht is op eventuele dataverzameling door derden. Anderzijds neemt het toewijzen van individuele IPv6-adressen echter wel de noodzaak weg om een hele groep (onterecht) 'verdachten' door te lichten in een opsporingsonderzoek. De privacyschending (voor de groep onschuldigen) is daardoor kleiner en juridisch meer proportioneel.

3.3 Mogelijkheid 2: Vergroten van het aantal publieke IPv4-adressen

Door het aantal publieke IPv4-adressen waarover een ISP bezit te vergroten, kan deze per IP-adres een kleiner aantal abonnees toewijzen bij CG-NAT. Hierdoor wordt de groepsgrootte (aantal abonnees per publiek IPv4-adres) verkleind. In het extreme geval wordt iedere abonnee voorzien van een eigen IPv4-adres (zoals dit op de meeste vaste netwerken in Nederland voor het grootste deel van de abonnees het geval is). Wanneer iedere abonnee kan worden voorzien van zijn eigen publiek IPv4-adres, is NAT niet meer nodig en identificatie eenvoudig zolang de koppeling tussen IPv4-adres en abonnee wordt bijgehouden (en uitvraagbaar is voor opsporingsdiensten).

Zoals eerder beschreven is, ligt de moeilijkheid van deze oplossing in het feit dat IPv4-adressen op dit moment schaars zijn. In theorie zijn er 2^{32} (circa 4,2 miljard) unieke IPv4-adressen. Een groot deel van deze adressen is echter niet bruikbaar voor communicatie over het publieke internet. Het gaat dan om:

- Diverse adressen (specifiek het bereik 224.0.0.0/4[42]) zijn gereserveerd voor speciale functionaliteit, zoals *multicast*, waarmee groepen computers kunnen worden geadresseerd met een IPv4-adres. Omdat dergelijke toepassingen op diverse locaties in gebruik zijn, kunnen de adressen niet zomaar ineens worden ingezet voor reguliere communicatie: het zou een wijziging van configuratie vereisen op vrijwel alle op internet aangesloten routers. [36]

[42] Een bereik IPv4-adressen kan worden genoteerd als w.x.y.z/s (de zogenaamde CIDR-notatie). De letters worden vervangen door getallen en geven dan een *prefix* aan (het eerste deel van alle adressen in het netwerk) en de 's' de lengte van dit voorvoegsel. Zo betekent "192.168.1.0/24" dat de eerste 24 bits van "192.168.1.0" moeten worden gezien als het voorvoegsel, en de rest als identificatie van een individuele node in dat netwerk. Concreet betekent dit dat het voorvoegsel "192.168.1." is, en de adressen tussen "192.168.1.0" en "192.168.1.255" binnen dit netwerk vallen. Hierbij vallen het eerste en laatste adres per definitie weg (het eerste wordt gebruikt als 'netwerkadres' en het laatste als 'broadcastadres' om alle nodes in dat netwerk aan te spreken). Hoe lager het prefixgetal, hoe hoger het aantal adressen in het netwerk: bij benadering 2^{32-s} (geen rekening houdend met netwerk- en broadcastadressen).

- Diverse adressen zijn bedoeld voor private netwerken (o.a. 192.168.0.0/16, 10.0.0.0/8, 172.16.0.0/12), één-op-één verbindingen (169.254.0.0/16) of verbindingen die binnen een host blijven (127.0.0.0/8). [37]

- Diverse adressen (waaronder 0.0.0.0/8 en 255.255.255.255) hebben een speciale betekenis binnen het IP-protocol om zaken zoals broadcasting mogelijk te maken. [37] [38]

Samen vertegenwoordigen de bovengenoemde 'speciale adressen' circa 13% van de adresruimte. Er blijven daarmee in theorie circa 3,7 miljard IPv4-adressen over voor regulier gebruik op het publieke internet. Dat wil niet zeggen dat al deze adressen in de praktijk daadwerkelijk bruikbaar zijn. De adresruimte wordt namelijk verdeeld in een zeer groot aantal 'ranges', die kunnen worden gebruikt binnen verschillende netwerken. Deze *blokken* hebben verschillende groottes – de grootte van een blok wordt bepaald naargelang het gebruik en het aantal gebruikers. Veelal worden iets meer adressen gereserveerd dan direct noodzakelijk, bijvoorbeeld om toekomstige groei of pieken op te kunnen vangen. Hoe kleiner de blokken, hoe meer adressen er verloren zullen gaan aan dergelijke 'overprovisioning'. Een voorbeeld is dat ISP's blokken adressen moeten alloceren, bijvoorbeeld (op vaste netwerken) aan regio's of groepen abonnees. Omdat de grootte van het toegewezen blok altijd hoger is dan het aantal abonnees (om te voorkomen dat er schaarste optreedt) gaan hier dus adressen verloren.

Uiteindelijk betekent dit dat er, wereldwijd gezien, (veel) minder dan één IP-adres per hoofd van de bevolking beschikbaar is. Daarentegen is het aannemelijk dat ieder hoofd van de bevolking (uiteindelijk) ten minste één of meer IP-adressen nodig zou hebben.

3.3.1 Technische implementatie

Er zijn twee manieren om het aantal publieke IPv4-adressen bij de ISP's te vergroten. De eerste is het aankopen van 'tweedehands' IPv4-adressen die bijvoorbeeld vrijkomen na een faillissement. De tweede is het aan CG-NAT toewijzen van IPv4-adressen uit de IPv4-adresblokken waar de ISP al beschikking over heeft – dit vereist het opnieuw indelen en/of gebruiken van IPv4-adressen. Beide oplossingen kunnen uiteraard worden gecombineerd.

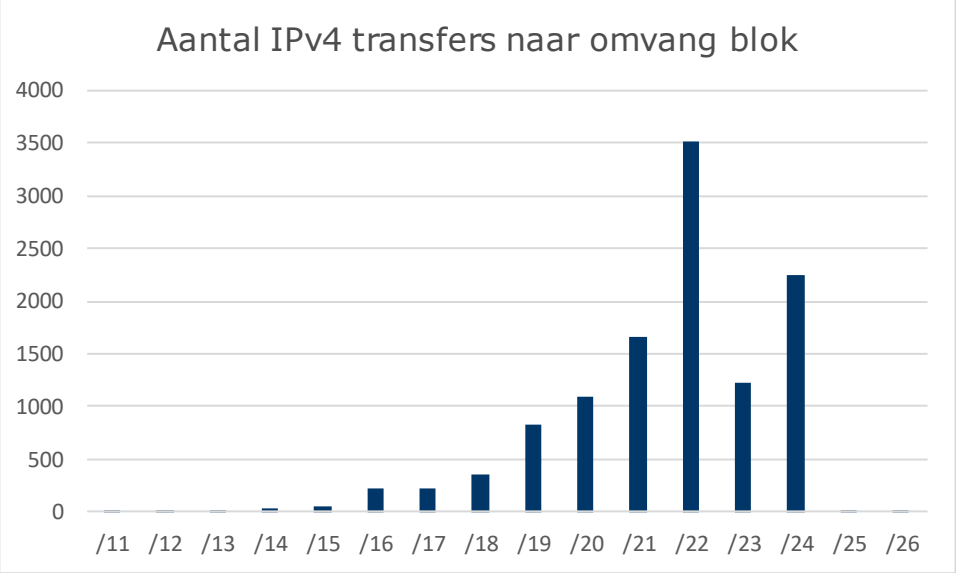
Het aanschaffen van 'tweedehands' IPv4-adressen

Ondanks het feit dat vrijwel alle IPv4-adressen door de Regional Internet Registeries (RIR's) zijn verdeeld, vindt er nog wel handel plaats in IPv4-adressen. Dit wordt een IPv4-transfer genoemd. Een sprekend voorbeeld is MIT, welke in 2017 aankondigde dat het ruim 8 miljoen IPv4-adressen ging verkopen aan Amazon [39]. Microsoft kocht reeds in 2011 IP-adressen van het failliete Nortel. [40] RIPE (de Europese RIR) geeft aan dat tussen 2012 en 2019 10.656 IP-transfers hebben plaatsgevonden in Europa en het Midden-Oosten [41]. Tussen de IPv4-transacties bevinden zich ook Nederlandse partijen. Zo heeft Telenor Neorge AS IPv4-adressen verkocht aan Canal Digital Kabel TV AS en heeft KPN na faillissement van de Brabantse ISP Edutel IPv4-adressen gekocht.

Het aanschaffen van meer IPv4 adressen is dus een reëele mogelijkheid voor een ISP mits deze beschikbaar zijn. IPv4-adressen komen doorgaans niet zomaar op de markt. IPv4-adressen komen beschikbaar wanneer ISP's failliet gaan of worden overgenomen, of (volledig) overstappen op IPv6. In Nederland bezitten niet alleen ISP's IPv4-adressen. Zo hebben (semi) overheidsorganisaties in Nederland samen meer dan 8,7 miljoen IPv4-adressen [42]. Dit is ruim 10 keer zo veel als het aantal IPv4-adressen dat ISP's beschikbaar stellen voor mobiele netwerken. In Nederland heeft SURFnet 8,468,223 IPv4-adressen in bezit. Het Ministerie van Infrastructuur en Waterstaat (229,376 IPv4-adressen) en het Ministerie van

Economische Zaken en Klimaat bezitten ook relatief veel IPv4-adressen (131,072 IPv4-adressen). In perspectief, voormalig Tele2 Nederland (nu onderdeel van T-Mobile) had slechts 171,776 IPv4-adressen in bezit.

Volgens RIPE's IPv4-transferstatistieken zijn in de periode 2015–2019 71,9 miljoen IPv4-adressen verhandeld [41]. IPv4-adressen worden sterk gefragmenteerd aangeboden. De meest verhandelde blokgrootte (een /22-blok) bevat slechts 1024 IPv4-adressen. Om aan een grotere hoeveelheid IPv4-adressen te komen, dient een ISP dan vaak verschillende blokken van verschillende organisaties over te nemen.



Figuur 12 Aantal IPv4 tranfers naar omvang blok (2015-2019) op basis van transfergegevens van RIPE, bewerkingen Dialogic [41]

Herverdeling van IPv4-adressen reeds in het bezit van de mobiele ISP

Veel ISP's zijn ontstaan als samenvoeging van een aantal kleinere ISP's. Het bekendste voorbeeld is VodafoneZiggo, ontstaan uit de samenvoeging van mobiele operator Vodafone en kabelaanbieder Ziggo. Het toenmalige Ziggo, was op haar beurt ontstaan uit een fusie van Ziggo met UPC. Ziggo en UPC zijn beide voortgekomen uit diverse fusies en overnames van kleinere, lokale en regionale kabelnetwerken. Tot op de dag van vandaag bestaan er technische verschillen tussen het voormalig Ziggo en voormalig UPC-gebied. Het is denkbaar dat in verschillende delen van het netwerk van een ISP verschillende merken en versies van apparatuur, netwerktopologieën en aanverwanten worden gebruikt, waardoor het uitwisselen of efficiënter verdelen van IPv4-adressen over deze netwerken technische uitdagingen kan opleveren.

ISP's hebben daarnaast te maken met een groot aantal legacytoepassingen[43] en klanten die in langdurige contracten eigen IP-adressen toegewezen hebben gekregen. Het wijzigen van deze IP-adressen is lastig, aangezien het hele blok leeg moet worden gemaakt om IP-adressen te kunnen herverdelen.

[43] Oudere diensten hadden vaker een vast IP-adres, terwijl nieuwere diensten vaker gebruik maken van (CG-)NAT. Het toewijzen van een vast IP-adres is een extra feature geworden met de bijbehorende kosten, maar op een oude dienst kan het nog wel inclusief zijn.

Tot slot bieden enkele ISP's aan klanten de mogelijkheid om ook op het mobiele net een publiek IPv4-adres toegewezen te krijgen. Dat kan gelden voor specifieke abonnementsvormen (bijvoorbeeld gericht op de zakelijke markt) of naar keuze zijn van de abonnementhouder (door bijvoorbeeld een ander APN te selecteren in de verbindingsinstellingen).

Ondanks de praktische bezwaren blijft herverdeling van eigen adressen een kwestie van tijd en geld. Daarnaast ondervinden de ISP's op de lange termijn waarschijnlijk ook voordelen van herverdeling in termen van beheersbaarheid van de netwerken.

Herverdeling door vaste aansluitingen achter NAT plaatsen

Een andere oplossing op basis van herverdeling zou zijn om NAT toe te gaan passen op delen van het netwerk waar nu (statisch) publieke IPv4-adressen worden uitgedeeld. De drie grote Nederlandse mobiele operators hebben alle ook een vast netwerk. Voor alle operators geldt dat (in de regel) vaste aansluitingen een (semi-vast of vast) publiek IPv4-adres krijgen toegekend, terwijl op het mobiele netwerk NAT wordt toegepast. Door ook NAT toe te passen op (een deel van) het vaste netwerk, zou het aantal publieke IPv4-adressen dat nodig is voor het vaste netwerk substantieel kunnen worden verlaagd. De overgebleven adressen kunnen worden toegevoegd aan de 'pool' met adressen voor NAT op het mobiele netwerk.

Tabel 4 geeft een rekenvoorbeeld van hoe een dergelijke herverdeling van IPv4-adressen door het toepassen van NAT op het vaste netwerk van een ISP eruit kan zien. In de tweede kolom is het aantal vaste aansluitingen per ISP gegeven (bij benadering). Merk op dat - omdat de ISP's over het algemeen (semi-)statisch IPv4-adressen uitdelen op deze netten - dit een ondergrens geeft voor het aantal IPv4-adressen dat zij (vrij) tot hun beschikking hebben.

Tabel 4 Rekenvoorbeeld inzet beschikbare IPv4-adressen van een ISP voor CG-NAT op zowel vast als mobiel (bron gehanteerde cijfers: [43])

ISP	Aantal IPv4-adressen in bezit[44]	Aantal vaste aansluitingen[45]	Aantal mobiele aansluitingen[46]	Aantal abonnees per publiek IPv4-adres[47]
VodafoneZiggo	5.862.656	3.317.200	4.966.000	1,4 – 2,5
KPN	7.071.232	4.156.000	7.586.000	1,7 – 2,8
T-Mobile	1.513.472	227.000	4.004.000	2,8 – 18,6
Totaal	**14.447.360**	**7.700.200**	**16.556.000**	**1,7 – 3,2**

Zoals in Tabel 4 is weergegeven zou de identificeerbaarheid van abonnees op mobiele netwerken kunnen worden verbeterd door ook vaste aansluitingen van diezelfde ISP achter CG-NAT te plaatsen. Het nadeel daarvan is dat de identificatie van gebruikers op vaste aansluitingen verslechtert. Bezien over alle aansluitingen gemiddels is de identificeerbaarheid

[44] Bij benadering en theoretisch; op basis van registratie-informatie van IPv4-adresblokken. Betreft de op Nederlandse netwerken inzetbare IPv4-adressen.

[45] Bij benadering, op basis van de cijfers uit de diverse jaarverslagen.

[46] Ibid.

[47] Het eerste getal geeft de meest pessimistische schatting: het aantal mobiele en vaste aansluitingen gedeeld door het aantal nu beschikbare IPv4-adressen voor vaste aansluitingen (aanname: gelijk aan het aantal vaste aansluitingen). Het tweede getal geeft de meest optimistische schatting: het aantal mobiele en vaste aansluitingen gedeeld door het theoretisch aantal beschikbare IPv4-adressen.

echter beter. In deze oplossingsrichting kan eventueel worden gekozen om niet álle vaste aansluitingen, maar slechts een deel achter CG-NAT te plaatsen (zoveel als nodig om de groepsgrootte op de mobiele netwerken onder een bepaalde werkbare grens te krijgen).

Een rigoureuze vorm van herverdeling zoals hierboven beschreven heeft belangrijke nadelen. Het meest optimistische scenario zoals geschetst in Tabel 4 gaat zeer waarschijnlijk niet op, omdat de ISP's een groot deel van hun IPv4-adresruimte (tot wel de helft) inzetten voor zakelijke klanten. Een nadeel is verder dat klanten op het vaste net niet langer een (semi-)statisch, publiek IPv4-adres krijgen, maar via NAT het internet op gaan. Dat betekent dat applicaties die een publiek IPv4-adres vereisen (zoals een internetcamera) niet meer werken. Ook wordt het onmogelijk om via een dergelijke aansluiting een server aan te bieden (zoals een VPN-server thuis) – een mogelijkheid waar naar verwachting een kleine groep consumenten gebruik van zal maken, maar die tot nu toe wel altijd is ondersteund door de ISP's (onder meer door functionaliteit voor port forwarding aan te bieden in de geleverde modemrouters). Beiden zouden kunnen worden gemitigeerd door ook IPv6 uit te rollen (IPv4-connectiviteit kan in dat geval via technieken als 464XLAT worden gerealiseerd).

Deze oplossing vereist investering in NAT-apparatuur, die een grotere capaciteit moet hebben per aansluiting (op vaste netwerken wordt typisch veel meer verkeer afgewikkeld per aansluiting dan op mobiele netwerken). Daarnaast is de migratie op zichzelf een kostbare operatie, daar het een ingrijpende wijziging in het netwerk betreft. We verwachten dat ISP's, geconfronteerd met de keuze, eerder een overstap zullen maken naar IPv6 in combinatie met CG-NAT (voor IPv4), dan te investeren in CG-NAT voor alleen IPv4. Reden is dat bij uitrol van IPv6 minder verkeer via CG-NAT hoeft te worden afgewikkeld. Daarnaast biedt dit de mogelijkheid tot het (in de toekomst) afschalen van de IPv4-dienstverlening.

We zien tot slot dat een aantal ISP's de uitrol van IPv6 op vaste netwerken (of delen van netwerken) reeds is gestart, waaronder Ziggo (delen van het netwerk) en KPN (name op het voormalige XS4ALL-netwerk). Het ligt ook gezien deze reeds gemaakte keuzes niet voor de hand om voor deze oplossing te kiezen.

3.3.2 Kosten

Het aanschaffen van IPv4-adressen

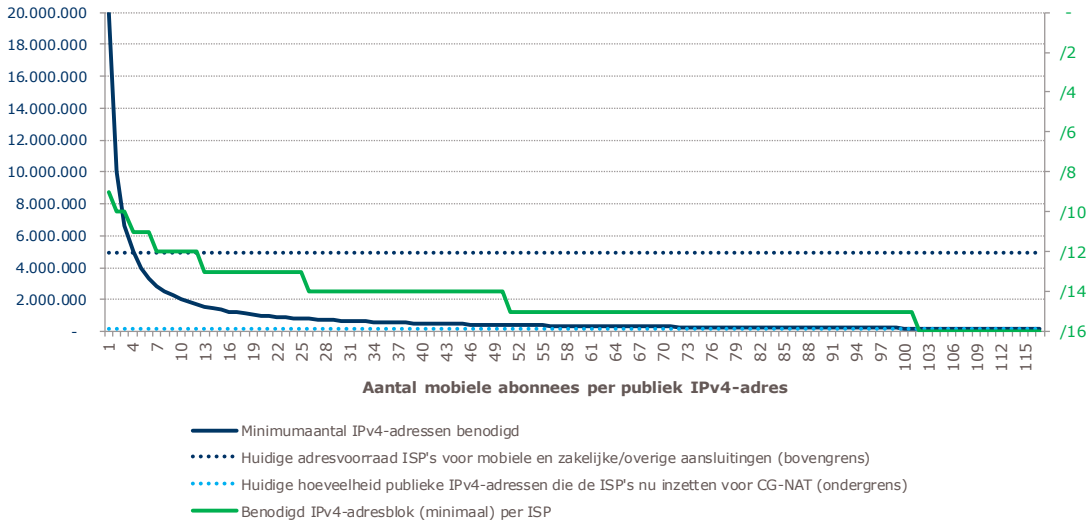
De Nederlandse mobiele markt kent ongeveer 20 miljoen aansluitingen. [43] Het totaal aantal IPv4-adressen dat KPN, T-Mobile en Vodafone opgeteld bezitten (inclusief gebruik voor hun vaste aansluitnetwerken) is, op basis van tellingen van IP-adresblokregistraties, naar schatting circa 12 miljoen. Trekken we daar de ruim 7,7 miljoen vaste aansluitingen vanaf (onder de aanname dat ieder van deze aansluiting één semipermanent IPv4-adres krijgt toegewezen), dan blijven er 4,9 miljoen IPv4-adressen over voor mobiele en overige (zakelijke) aansluitingen van deze ISP's. Wanneer alle resterende 4,9 miljoen adressen worden gedeeld over 20 miljoen aansluitingen, dan gebruiken gemiddeld ongeveer vier abonnees hetzelfde publieke IPv4-adres.

In het *beste* geval zouden de ISP's meer dan 15 miljoen IPv4-adressen moeten verkrijgen om (net als op de vaste netwerken) iedere aansluiting van één semipermanent publiek IPv4-adres te voorzien.Het verkrijgen van dergelijke aantallen IPv4-adressen lijkt, gezien de schaarste, niet realistisch (het zou gaan om een '/8'-adresblok, ofwel meer dan 1/255'ste van de volledige IPv4-adresruimte).

In combinatie met source port logging en statische toewijzing van (een reeks van) poortnummers naar abonnees zijn (uitgaande van 512 poorten per abonnee en 60.000 poorten per publiek IPv4-adres, ergo 117 abonnees per IPv4-adres) circa 170.000 IPv4-adressen

nodig. We verwachten dat de mobiele ISP's (voor zover zij niet al op deze wijze CG-NAT toepassen) deze adressen uit eigen voorraad kunnen halen.

Tussen beiden uitersten is een afweging tussen het aantal IPv4-adressen en de groepsgrootte (aantal abonnees per IPv4-adres en daarmee groepsgrootte voor identificatie) te maken. Figuur 13 geeft een indicatie van het (minimum) aantal benodigde publieke IPv4-adressen.



Figuur 13 Het benodigd aantal IPv4-adressen en -adresblokken bij verschillende groepsgroottes

Wat kost een IPv4-adres?

Formeel gezien zijn IPv4-adressen niet te koop – de registrars geven de adressen 'in bruikleen' aan leden, waarvoor zij een jaarlijkse bijdrage aan de registrar betalen.[48] De leden, vaak grotere organisaties zoals hostingpartijen en internetproviders, stellen de IP-adressen aan hun klanten ter beschikking.

Er is desondanks een klein aantal partijen die al over IP-adresreeksen beschikte *voordat* de registrars werden opgericht, waaronder Nortel en MIT. Aangezien het aantal IP-adressen dat de registrars nog ter beschikking hadden snel afnam, werd het aantrekkelijk voor deze partijen om de adresreeksen te verkopen. In 2011 kocht Microsoft dan ook 666.624 adressen van Nortel voor een bedrag van US$ 7,5 miljoen[49] en in 2017 verkocht MIT acht miljoen (van de in totaal 16 miljoen aan haar toegewezen) adressen aan Amazon voor een onbekend bedrag. Amazon en Microsoft gebruiken de adressen voor de door hen aangeboden grootschalige clouddiensten.

Ook op kleinere schaal wordt gehandeld in IPv4-adressen. De bedragen variëren tussen de 13 en 22 euro per adres, afhankelijk van de grootte van het blok en de registrar waar het blok onder valt.[50] Een aspect om rekening mee te houden bij deze vorm van aankoop

[48] Zie o.a. RIPE (2019). *Can I buy IP addresses from the RIPE NCC?* [www.ripe.net]

[49] Network World (2011). *Microsoft pays Nortel $7.5 million for IPv4 addresses* [www.networkworld.com]

[50] Zie o.a. [ipv4marketgroup.com] (US$ 18 in 2018) en [auctions.ipv4.global]. Merk op dat beide partijen handel in IP-adressen faciliteren en dus een belang zullen hebben bij de beprijzing.

is de *reputatie* van een IPv4-adres(blok): sommige adressen en adresblokken zijn inmiddels bekend als (bijvoorbeeld) afzender van spam, waardoor deze adressen minder 'waard' zijn dan adressen die lange tijd in gebruik zijn geweest door een partij met goede reputatie.

De 'openbare' handel in IPv4-adressen betreft relatief kleine blokken. Zoals hierboven al is aangegeven, hebben de Nederlandse ISP's in dit scenario grote aantallen adressen nodig. Het aankopen van grote aantallen kleine blokken is vanuit technisch en beheersmatig oogpunt onwenselijk. Daarnaast zal de marktprijs van dergelijke IPv4-adressen naar verwachting snel stijgen zodra één of meer ISP's deze in grote hoeveelheden opkoopt. Of het Nederlandse ISP's lukt om een partij te vinden die over een groot aantal IPv4-adressen beschikt én deze wil verkopen, is nog maar de vraag.

Bij alle oplossingen met een kleiner aantal IPv4-adressen dan abonnees is (ervan uitgaand dat gelijktijdig gebruik door alle abonnees wordt ondersteund) een vorm van CG-NAT nodig. Bij statische toewijzing van een poortbereik per abonnee kan worden volstaan met het bijhouden van datum, abonneenummer en toegewezen IP-adres en poortnummer. Een dergelijke tabel is maximaal enkele honderden megabytes groot. In het slechtste geval (dagelijkse hertoewijzing) dient een ISP (bij een bewaartermijn van een jaar) ongeveer 117 gigabyte continu op te slaan.[51]

Zijn er minder dan (ordegrootte) 170.000 IPv4-adressen beschikbaar voor CG-NAT, dan is dynamische toewijzing noodzakelijk. Wanneer IPv4-adressen dynamisch worden toegewezen, betekent dit dat per 1 miljoen gebruikers circa 6,4 terabyte aan logbestanden geproduceerd wordt [44]. De IoT-ontwikkelingen gaan razendsnel, maar wanneer we uitgaan van een ondergrens van 20 miljoen apparaten in Nederland waarop dynamisch toewijzing wordt toegepast (voorzichtige schatting), dan levert dit circa 130 terabyte per dag aan loggegevens op.

Als in de toekomst het aantal mobiele apparaten gelijk blijft (wat onwaarschijnlijk lijkt) en ISP's voor één jaar een IP-adres, poortnummer en timestamp moeten bewaren, dan betekent dit dat circa 47 petabyte (ofwel 47.000 terabyte) aan data worden opgeslagen. Vanuit een opsporingsperspectief is het een aantrekkelijke optie om deze logfiles te bewaren, maar opslag en verwerking van deze gegevens is niet zonder kosten.

Om een inschatting te maken van wat de kosten zijn van het opslaan van zulke grote hoeveelheden data kan worden gekeken naar de kosten die gemaakt worden voor het opslaan van data bij een aanbieder van clouddiensten. Amazon AWS biedt opslag van grote hoeveelheden data aan tussen de 0,00035 en 0,02 euro per GB per maand (afhankelijk van de frequentie waarmee de data opgehaald moeten kunnen worden). Cloudopslag van de NAT-logs kost dan tussen 168.000,- en 838.000,- euro per maand. Merk op dat de opslag van de benodigde logginggegevens bij statische toewijzing nihil zijn.

Herverdeling van IPv4-adressen reeds in het bezit van de mobiele operator

De kosten voor herverdeling van IPv4-adressen die een mobiele operator al in het bezit heeft, zijn tweeledig. Eerst moet een inventarisatie van 'ongebruikte' IP-adressen bij klanten

[51] Per abonnee dient een abonneenummer (circa 4 bytes), datum/tijdstempel (4 bytes), IPv4-adres (4 bytes) en poortbereik (2 x 2 bytes) te worden opgeslagen (16 bytes per abonnee). Uitgaande van 20 miljoen abonnees betekent dit 320 megabyte voor een 'snapshot' van de toewijzing. Zelfs wanneer abonnees dagelijks een nieuwe reeks krijgen toegewezen betreft het dus maximaal 320 x 365 ≈ 117 gigabyte per jaar.

plaatsvinden. Dit zijn IPv4-adressen die bijvoorbeeld zijn uitgegeven aan zakelijke klanten, maar die niet worden gebruikt. Deze IP-adressen kunnen relatief eenvoudig worden herverdeeld. Het wordt echter lastiger wanneer een ISP contractuele toezeggingen heeft gedaan met betrekking tot het aantal IP-adressen bij het afsluiten van een contract.

Door middel van een DNS-lookup kan een indicatie worden verkregen over de manier waarop een IP-adres wordt gebruikt.[52] Via deze methode zijn van alle IP-adressen die via BGP-gegevens behoren tot Nederlandse ISP's de domeinnamen opgehaald. Voor 13 van de 40 IP-blokken zijn geen DNS-gegevens vindbaar. Over deze blokken zijn geen uitspraken te doen; het kan dat het verzoek wordt geblokkeerd door een firewall. Van de 40 geïnspecteerde blokken worden er 9 waarschijnlijk 100% voor zakelijke doeleinden gebruikt met een gezamenlijke omvang van ongeveer 15.000 IP-adressen. In totaal zijn er ongeveer 54.000 IP-adressen gevonden die zeer waarschijnlijk voor zakelijke doeleinden worden gebruikt.[53]

Zakelijke klanten kunnen afhankelijk zijn van publieke IPv4-adressen om bepaalde diensten te leveren. Denk bijvoorbeeld aan een server of VPN-tunnel. Het publieke IPv4-adres is dan soms 'hard-coded' aan de apparatuur toegewezen. Wanneer deze adressen onder NAT worden gerouteerd, kan het zo zijn dat een groot deel van deze diensten niet meer bereikbaar is. Dit kan vergaande gevolgen hebben voor klanten. Het beter benutten van IPv4-adressen die toegekend zijn aan zakelijke klanten is dus niet in alle gevallen even eenvoudig. Er zal moeten worden geïnventariseerd welke adressen niet voor deze doeleinden worden gebruikt. Deze kunnen dan, in overleg met de klant, gebruikt worden voor mobiel NAT. Daarnaast rest er nog de vraag welk deel van de zakelijke klanten naar IPv6 overgezet kan worden.

Het blijft echter onduidelijk welk deel van de IP-adressen nu 'vrij' is, en welke kosten er gemoeid zijn om deze ongebruikte IP-adressen in gebruikt te nemen.[54] Er kan in ieder geval vanuit worden gegaan dat een ISP er rationeel gezien baat bij heeft om de pool aan IPv4-adressen zo optimaal mogelijk te gebruiken. Suboptimaal gebruik van IPv4-adressen brengt juist meer kosten met zich mee zoals investeringen in CG-NAT.

Herverdeling: vaste aansluitingen achter NAT plaatsen

Zoals hierboven aangegeven is deze mogelijkheid voor de ISP waarschijnlijk niet aantrekkelijker dan het uitrollen van IPv6 in combinatie met CG-NAT voor IPv4. De kosten voor deze mogelijkheid zijn dan ook niet nader gekwantificeerd.

---

[52] Het DNS registreert de relatie tussen een IP-adres en een domeinnaam. Normaliter wordt dit gebruikt om bij een domeinnaam (www.website.nl) het IP-adres te vinden van de server waarvandaan de website kan worden opgevraagd. Het is echter ook mogelijk om 'andersom' een naam bij een IP-adres te zoeken (een 'reverse look up'). Deze naam geeft vaak een indicatie over hoe het IP-adres wordt gebruikt, mede omdat het een goed gebruik is om deze 'reverse' namen indicatief te laten zijn voor het gebruik. Wanneer bijvoorbeeld een naam als ftth.abc.net wordt teruggegeven, dan kunnen we met redelijke zekerheid stellen dat dit IP-adres wordt gebruikt voor glasvezelverbindingen voor consumenten. Een domein webmail.abc.net zal op zijn beurt weer gebruikt worden als e-mailserver en content.abc.net zal hoogstwaarschijnlijk worden gebruikt om bepaalde informatie via het internet beschikbaar te stellen (zoals een website) et cetera.

[53] Een groot deel van de IP-adressen retourneert geen DNS-informatie, over mogelijk gebruik van deze IP-adressen zijn geen uitspraken te doen. Op basis van de DNS-lookup zijn ongeveer 2,3 miljoen IP-adressen onderzocht, maar voor slechts 827 duizend IP-adressen was DNS-informatie (publiek) beschikbaar.

[54] De geïnterviewde ISP's hebben deze vraag niet beantwoord.

3.3.3 Overwegingen

De mobiele telecommarkt heeft in de afgelopen jaren een explosieve groei meegemaakt. Tabel 2 toont het aantal mobiele aansluitingen over de afgelopen 4 jaar. Het totaal aantal mobiele aansluitingen met een datadienst is gestegen tot bijna 26 miljoen in 2018, waarvan circa 21 miljoen niet-M2M-aansluitingen. In totaal ging het in 2018 om circa 20 miljoen niet-M2M-aansluitingen met toegang tot data.[55]

Tabel 5 Ontwikkeling aantal mobiele aansluitingen (in duizendtallen). [43]

Ontwikkeling aantal mobiele aansluitingen (miljoenen)	2014-Q1	2015-Q1	2016-Q1	2017-Q1	2018-Q1
Data-only	1.017	1.120	1.112	965	570
M2M	1.315	2.259	3.036	3.382	4.477
Voice-only	9.049	7.228	6.928	2.143	1.505
Data en spraak	10.064	12.212	12.840	18.722	19.395
Totaal mobiele aansluitingen	21.445	22.819	23.916	25.212	25.947
Totaal mobiele aansluitingen met data	12.396	15.591	16.988	23.069	24.442
Totaal mobiele aansluitingen met data exclusief M2M	**11.081**	**13.332**	**13.952**	**19.687**	**19.965**

Wanneer deze trend doorzet, zal er in de toekomst voor mobiele apparaten alsmaar sterkere NAT (meer apparaten per IPv4-adres) toegepast moeten worden. De afgelopen jaren zijn veel applicaties efficiënter geworden in hun omgang met poorten, waardoor er minder poorten per gebruiker nodig zijn, en één IPv4-adres met meer gebruikers kan worden gedeeld.[56] Daarnaast speelt er de ontwikkeling van Internet of Things (IoT)-apparaten die communiceren via het internet. De vraag speelt of dit efficiëntere poortgebruik voldoende is om de sterke groei van aan het internet verbonden apparaten te faciliteren. In verschillende onderzoeken wordt verwacht dat de IoT-markt in de komende jaren aanzienlijk zal groeien. Op basis van wereldwijde voorspellingen van Analysis Mason wordt verwacht dat de Nederlandse IoT-markt in 2024 tussen 8,7 en 52,1 miljoen apparaten zal beslaan [45]. Wanneer (een deel) van deze IoT-apparaten over IPv4 communiceren, zal dit de schaarste nog verder vergroten.

3.4 Mogelijkheid 3: Source port logging

Wanneer een verbindingsverzoek plaatsvindt, 'ziet' een server op het internet niet alleen het publieke IPv4-adres van de bron, maar ook het poortnummer waarop de bron de pakketten voor die verbinding wil ontvangen. Bij toepassing van NAT is het afzenderadres een gedeeld IPv4-adres. Het poortnummer geeft echter wel extra informatie over de identiteit van een gebruiker: een poortnummer in combinatie met een tijdsperiode en een IP-adres kan naar één persoon leiden. Niet alle dienstenaanbieders houden echter poortnummers bij, waardoor deze vaak niet aanwezig zijn als 'spoor'. Daarnaast vereist deze werkwijze ook dat de ISP's de toewijzing op poortnummerniveau bijhouden en bewaren.

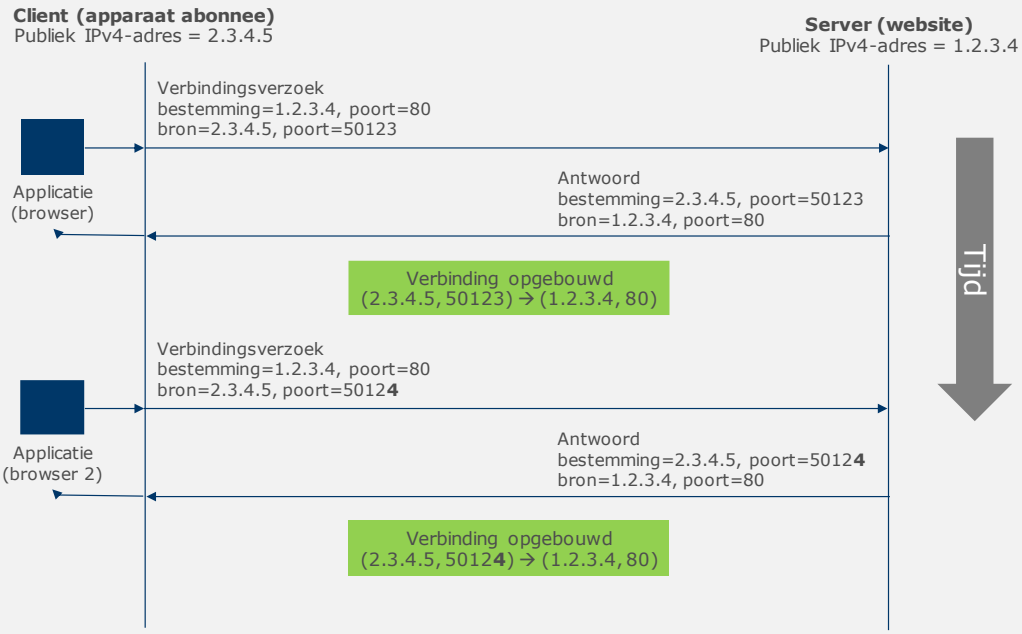
[55] We nemen M2M hier apart omdat bij M2M vaak geen publiek IPv4-adres, of juist een vast IPv4-adres, of helemaal geen IP wordt gebruikt. M2M valt daardoor typisch buiten beschouwing bij CG-NAT.

[56] Een voorbeeld is de introductie van het HTTP/2-protocol.

Hoe werken poortnummers?

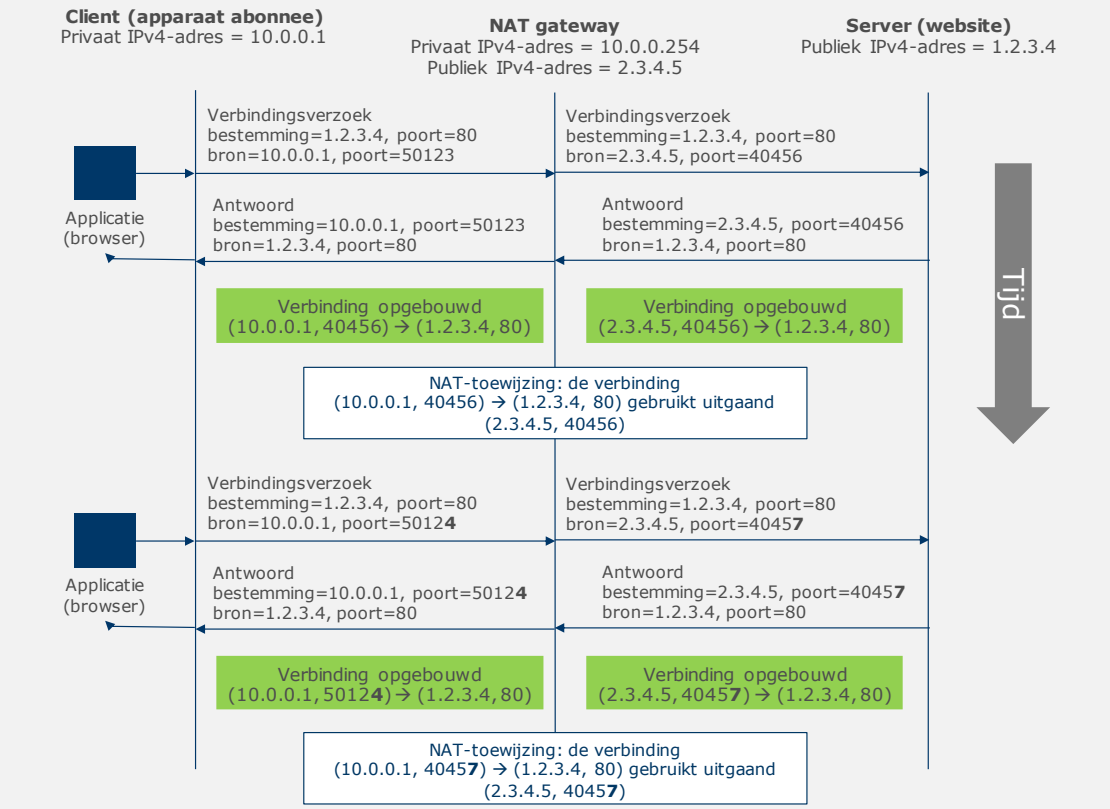
Bij het opzetten van een verbinding maakt het apparaat van de abonnee contact met een bepaald IP-adres op een bepaalde *poort*. Een poort is een getal dat aangeeft welke dienst op een computer wordt aangesproken: zo is 'poort 80' in de regel in gebruik voor HTTP-verkeer (onbeveiligde websites) en 'poort 443' in gebruik voor HTTPS (beveiligde websites). Dit heet de *destination port*. In het verbindingsverzoek is ook een poortnummer van de abonnee opgenomen (de zogenaamde *source port*): dit poortnummer stelt de abonnee in staat om antwoorden van de server te koppelen aan een specifiek verzoek (anders zou bijvoorbeeld, bij het tegelijk bezoeken van verschillende websites, de inhoud kunnen worden verwisseld). Naast het 'vertalen' van het netwerkadres wordt bij NAT typisch ook dit poortnummer vertaald.

Figuur 14 geeft schematisch aan wat er gebeurt op het moment dat een client (het apparaat van een abonnee) achtereenvolgens twee verbindingen met dezelfde server opzet (wanneer bijvoorbeeld vanuit twee browsertabs dezelfde website wordt geopend) wanneer er geen NAT wordt toegepast. Een 'verbinding' bestaat uit een unieke combinatie van *bronadres, bronpoort, bestemmingsadres* en *bestemmingspoort.* Op basis hiervan kunnen de twee verkeersstromen worden gescheiden aan beide kanten.



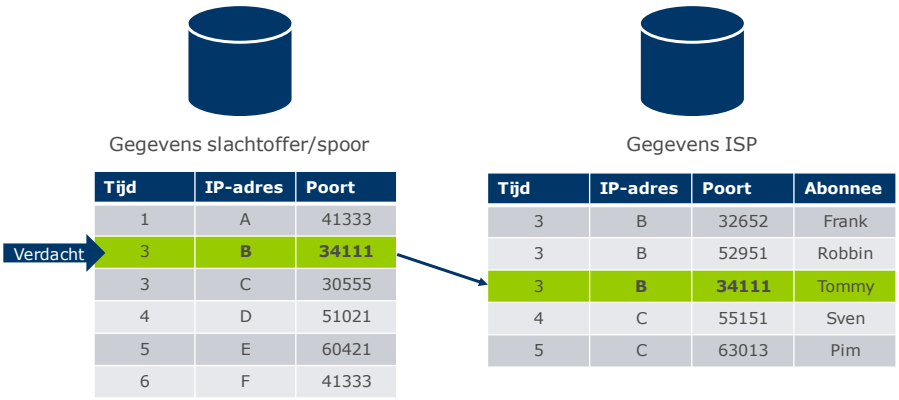
Figuur 14. Voorbeeld van verbindingsopbouw tussen een client en server op het internet (TCP/IPv4)

Bij NAT wordt het poortnummer van de bestemming niet gewijzigd, maar kan wel vertaling plaatsvinden van het poortnummer aan de zijde van de afzender. Onderstaand figuur toont schematisch hoe dit in zijn werk gaat, opnieuw in een voorbeeld waarin een client twee keer achter elkaar met dezelfde server verbindt. Zonder dat de client het doorheeft, vertaalt de NAT-gateway het pakket zodanig dat het lijkt alsof niet de *client*, maar de *gateway* de verbinding opzet naar de server. Er worden in feite twee verbindingen opgezet (één tussen de gateway en de client, en één tussen de gateway en de server), waarbij de client 'denkt' dat deze rechtstreeks met de server praat. De NAT-gateway houdt een 'mapping' bij van openstaande verbindingen en de bijbehorende in- en externe poortnummers.



Figuur 15. Voorbeeld van verbindingsopbouw tussen een client en server op het internet (TCP/IPv4) bij toepassing van NAT

Zoals in Figuur 15 is weergegeven wordt bij NAT door de NAT-gateway een koppeling gemaakt tussen een interne verbinding en een externe verbinding. Deze koppeling bestaat uit de combinatie van bronadres, bronpoort, bestemmingsadres, bestemmingspoort en het gehanteerde publieke IPv4-adres en -poort. Wanneer een abonnee steeds hetzelfde publieke IPv4-adres en een poortnummer binnen een vast bereik gebruikt (*statische allocatie*), kan de ISP op basis van het publieke adres en poortnummer de abonnee identificeren. Wanneer gebruik wordt gemaakt van *dynamische allocatie* bij NAT is dit eveneens mogelijk wanneer de ISP informatie bijhoudt over deze toewijzing (en aangezien het niet gaat om gegevens over de *bestemming* van het verkeer, maar louter het gehanteerde uitgaande poortnummer en IPv4-adres, is het aannemelijk dat dit door een rechter niet wordt gezien als een 'verkeersgegevens'). Figuur 16 geeft aan hoe het bronpoortnummer helpt bij identificatie van een abonnee.



Figuur 16 Schematisch voorbeeld van identificatie van individuen bij CG-NAT op basis van IPv4-adres en bronpoortnummer

3.4.1 Technische implementatie

Het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT) beheert een informatiesysteem (CIS) voor telefoon- en internetgegevens voor de opsporing van criminelen. Dit geautomatiseerde informatiesysteem levert persoonsgegevens die horen bij IP-adressen, telefoonnummers en e-mailadressen aan opsporingsdiensten, veiligheidsdiensten en inlichtingendiensten. Het bevat een dagelijks geactualiseerde kopie van de huidige allocatie van IPv4-adressen aan abonnees. Per IP-adres kan de houder (de naam van de ISP), een tijdstempel en een ID-nummer (door de ISP) worden herleid naar een specifieke klant. In geval van NAT kan een ISP niet naar één klant herleiden, en zal een verzoek buiten het CIOT om moeten worden gedaan. Het toevoegen van bronpoortinformatie aan het informatiesysteem zou opsporing versnellen in gevallen waar bronpoortinformatie beschikbaar is. [1]

3.4.2 Kosten

Het activeren van source port logging bij CG-NAT is voor een ISP een relatief kleine inspanning en poortnummers worden doorgaans al standaard opgenomen in de CG-NAT-logbestanden. De kosten zitten in de opslag van de gegevens (het betreft grote hoeveelheden data) en het inrichten van de organisatiestructuur en -processen om deze data te kunnen benaderen. Daarnaast moeten leveranciers van producten en diensten op internet ook bronpoortnummers opslaan, zodat ook aan die 'kant' van de verbinding bronpoortnummers beschikbaar zijn. Hoogstwaarschijnlijk zal logging van poortnummers door malafide dienstverleners daarnaast niet snel worden aangezet. Daarnaast is het onmogelijk om diensten die buiten Nederland worden gehost te verplichten source ports te loggen.

3.4.3 Overwegingen

Om source port logging zinvol te laten zijn, moet informatie over de bronpoort beschikbaar zijn. Dit laatste is problematisch, aangezien deze informatie nu nog niet standaard wordt opgeslagen. De informatie is afkomstig van diverse derde partijen. Zo zal een platform waarop misbruik heeft plaatsgevonden in veel gevallen alleen IP-adressen loggen (sommige platforms registreren het IP-adres eenmalig bij registratie, anderen houden bij vanaf welke IP-adressen een gebruiker ingelogd is geweest).

Bronpoorten worden in de regel alleen op verbindingsniveau bijgehouden, bijvoorbeeld in logbestanden van webserversoftware. In Tabel 6 wordt de beschikbaarheid van standaard source port logging van de zes meest populaire webserversoftware (naar marktaandeel) getoond. Geen enkele van de populaire webservers logt standaard de inkomende poortnummers. Desondanks wordt al sinds 2011 aangeraden bronpoorten te loggen [46], en

is het aanzetten van deze logging technisch gezien zeer eenvoudig. Vaak dient er slechts een extra regel code te worden gespecificeerd in de configuratie van de logfiles.

Tabel 6 Overzicht van de meest gebruikte webserversoftware; bij geen van alle is source port logging standaard ingeschakeld

Naam	Marktaandeel [47]	Standaard source port logging[57]
Apache	43,9%	Nee
Nginx	41,6%	Nee
Microsoft-ISS	8,4%	Nee
LiteSpeed	0,9%	Nee
Node.js	0,6%	Nee
Apache traffic server	0,5%	Nee

3.5 Mogelijkheid 4: Verkeersgegevens gemaskeerd loggen

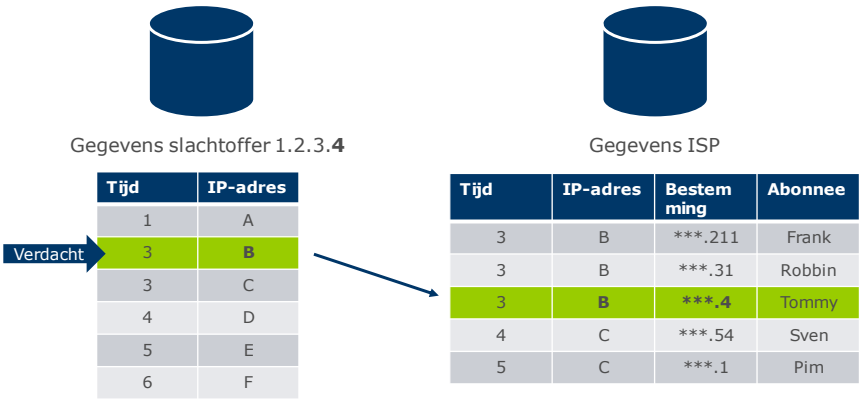
Zoals eerder beschreven kent het loggen van verkeersgegevens diverse haken en ogen vanuit juridisch perspectief en vanuit privacy-oogpunt. Logging is echter een aantrekkelijke oplossingsrichting voor ISP's die geen IPv4-adressen kunnen toevoegen aan CG-NAT en geen IPv6 willen uitrollen. Is het mogelijk om logging zo uit te voeren dat deze wél bruikbaar is voor opsporing, maar geen onnodige inbreuk maakt op de privacy van abonnees?

Mogelijk kan gebruik worden gemaakt van het feit dat vanuit opsporing de vindplaats van een IP-adresspoor in veel gevallen bekend is (bijvoorbeeld: Marktplaats bij online fraude, of de logs van een gehackte server). Deze informatie kan worden gebruikt om een groep abonnees (behorend bij het gebruikte IP-adres) verder te filteren. Dit zou uiteraard kunnen worden gedaan op basis van verkeersgegevens (welke abonnee heeft specifiek een bepaald IP-adres benaderd?). Het is echter ook mogelijk om hier een meer *statistische* benadering te kiezen: welke abonnee(s) hebben IP-adressen benaderd die eindigen in dezelfde getallenreeks als het 'spoor'-IP-adres? Een dergelijke aanpak maakt het mogelijk om minder informatie op te slaan terwijl de groepsgrootte bij identificatie effectief kan worden verkleind.

3.5.1 Technische implementatie

Een mogelijkheid zou zijn om alle door een abonnee opgezette verbindingen te loggen, maar daarbij slechts *delen* van het bestemmingsadres (bijvoorbeeld alleen de laatste byte) te bewaren. Het is dan niet te achterhalen met *wie* een abonnee communiceerde, maar het aantal 'verdachte' abonnees kan worden gereduceerd. Deze oplossing biedt zowel voordelen ten aanzien van privacy als kosten voor opslag.

[57] Op basis van de documentatie van deze software (de meest recente stabiele versie is bekeken).



Figuur 17 Schematisch voorbeeld identificatie en individuen bij CG-NAT op basis van IPv4-adres en laatste byte van bestemmingsadres

Er zijn verschillende methoden om een verkeersgegevens gemaskeerd bij te houden. Zo kunnen er verschillende keuzes worden gemaakt in welke bytes worden gemaskeerd en hoeveel bytes er worden gemaskeerd.

3.5.2 Kosten

De kosten voor het gemaskeerd bijhouden van verkeersgegevens zijn vergelijkbaar met die van de oplossingsrichting 'het aanschaffen van meer IPv4-adressen'. De kosten die een ISP moet maken om verkeersgegevens gemaskeerd bij te houden zijn onder te verdelen in kosten voor opslag en kosten voor het toegankelijk maken van de gegevens. Bij deze mogelijkheid van gemaskeerd loggen wordt echter slechts een deel van de informatie opgeslagen.

Een IPv4-adres kent 32 bytes. Vertaalde bronadressen en poortnummers nemen ongeveer 25% van een CG-NAT-log in beslag [44]. Als slechts 1/32 van het IPv4-adres wordt opgeslagen, dan kan de omvang van een logbestand met 25% worden gereduceerd. [58] Cloudopslag van de gemaskeerde NAT-logs kost voor 20 miljoen mobiele abonnees dan tussen 126.000,- en 628.000,-.euro uit per maand.[59]

3.5.3 Overwegingen

Het gemaskeerd bijhouden van verkeersgegevens heeft zowel voor- als nadelen. Hoewel het gemaskeerd bijhouden van verkeersgegevens het aantal personen reduceert, biedt het geen garanties voor een (werkbare) bovengrens. Dit is sterk afhankelijk van hoeveel gebruikers op één moment het internet op willen, en hoeveel IPv4-adressen een ISP aan zijn NAT-pool heeft gealloceerd.

Zo kan het zijn dat op sommige momenten, wanneer er weinig internetverkeer is, het gemaskeerd bijhouden een één-op-één relatie tussen gebruiker en IPv4-adres mogelijk maakt. Op momenten wanneer er veel internetverkeer is, kan het zo zijn dat het aantal gebruikers achter één IPv4-adres met dezelfde 'ongemaskeerde' byte(s) vele malen hoger is. Ook het aantal IPv4-adressen dat een ISP beschikbaar heeft gesteld voor de NAT-pool heeft invloed op de wenselijkheid van deze mogelijkheid. Voor een ISP waarbij de ratio gebruikers ten

[58] De overige elementen van de log files zijn de tijd (33%), CG-NAT hostname (8%), het transport protocol (4%), een 'add/delete' flag (4%), het onvertaalde bronadres en poortnummer (25%). De totale omvang van één record is, in tekst formaat, ongeveer 120 bytes groot.

[59] In paragraaf 3.3.2 gaan we nader in op de onderbouwing van deze kosten.

opzichte van het aantal beschikbare IPv4-adressen voor NAT hoog is, wordt weliswaar de meeste reductie gerealiseerd, maar kan het aantal mogelijke gebruikers dat één IPv4-adres deelt voor deze ISP nog steeds hoog zijn.

3.6 Mogelijkheid 5: Verhogen werkhoeveelheid politie

Van hele andere orde is het investeren in traditionele opsporingsmethoden als mogelijkheid. Dit staat los van de techniek en betreft in de eerder besproken driehoek (zie Figuur 7 en Figuur 18) de linker onderhoek. Als de politie meer onderzoekscapaciteit kan steken in zaken waarbij een IP-adres centraal staat, dan zullen ook meer zaken worden opgelost. Met andere woorden, het werk wordt niet gemakkelijker (het blijft zeer lastig tot één persoon te komen), maar door er meer tijd in te steken zal er wel vaker de juiste persoon worden gevonden.

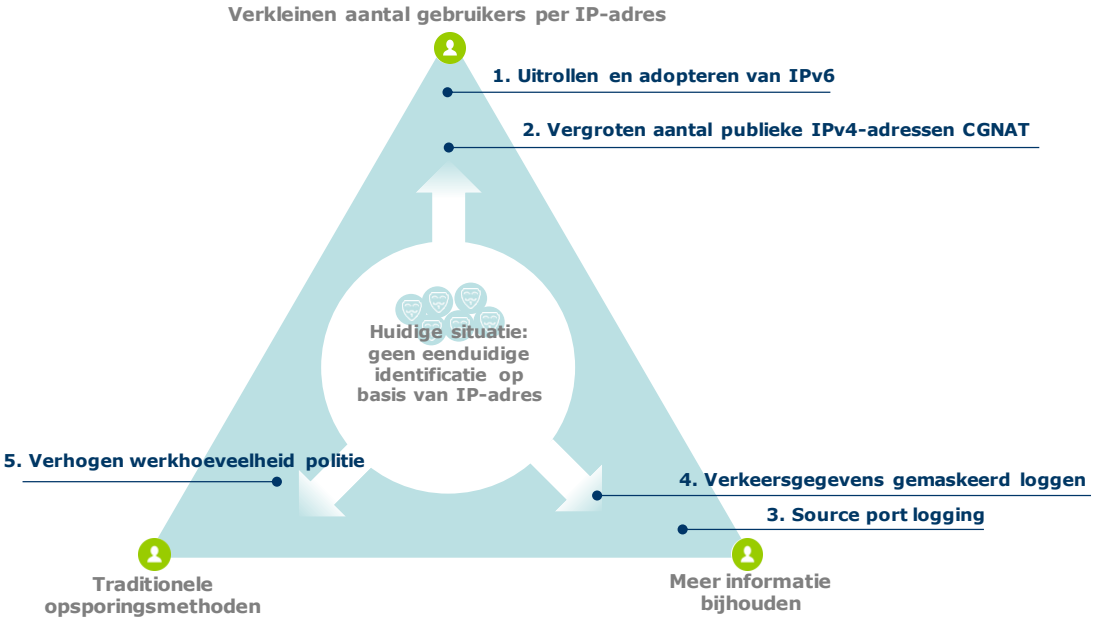
Deze mogelijkheid is waarschijnlijk onwenselijk. Het kost veel, de capaciteit, kennis en kunde is mogelijk niet in huis, en het onderliggende probleem van een moeilijk te leggen koppeling tussen individu en IP-adres wordt niet aangepakt.

3.7 Conclusie

Figuur 18 hieronder toont de besproken specifieke mogelijkheden in het eerder getoonde schema van oplossingsrichtingen. Onder de aanname dat de politie het maximale doet op basis van de methoden en instrumenten die zij nu tot haar beschikking heeft, moet een (technische) oplossing gezocht worden op de twee andere assen: ofwel het verkleinen van het aantal gebruikers per IP-adres, ofwel meer informatie bijhouden zodat een gebruiker kan worden herleid zelfs wanneer een IP-adres wordt gedeeld. In beide richtingen zien we twee mogelijkheden.

Als het gaat om het verkleinen van het aantal IP-adressen per gebruiker dan kan worden gekozen om meer IPv4-adressen aan te schaffen en toe te voegen aan de huidige 'NAT-pools', zodat effectief minder gebruikers per IPv4-adres worden toegewezen. We zien dit, in het licht van de (door het veld erkende noodzaak tot 'uiteindelijke' migratie naar IPv6) als een oplossing die kan worden gehanteerd in de periode tot de voltooide uitrol van IPv6. Uiteindelijk ligt uitrol en adoptie van IPv6 voor de hand. We zien we in de sector ook diverse bewegingen in die richting. Adoptie van IPv6 verlaagt de druk op IPv4-adressen doordat een steeds groter deel van het verkeer via IPv6 kan worden afgehandeld.

In de richting van het bijhouden van meer informatie zien we twee beperkt bruikbare oplossingen. Het bijhouden van source ports aan de zijde van de ontvanger wordt onderschreven in internetstandaarden en als 'best practice'. Het loggen, in combinatie met logging aan de zijde van de ISP (en/of het deterministisch toewijzen van poorten) maakt identificatie eenvoudig en mogelijk tot op één abonnee. Adoptie van source port logging is echter lastig te bewerkstelligen. Het gemaskeerd loggen van verkeersdata kan (al dan niet in aanvulling op source port logging), worden ingezet om de groepsgrootte te verkleinen, maar leidt hooguit tot een verkleining van de groepsgrootte, en niet tot eenduidige identificatie.



Figuur 18 Geïdentificeerde mogelijkheden voor het vergroten van de precisie van identificatie op basis van IP-adres

In onderstaande Tabel 7 presenteren we per oplossingsrichting de voor- en nadelen.

Tabel 7 Overzicht belangrijkste voor- en nadelen van mogelijkheden voor het verbeteren van identificatie op basis van IP-adres

Mogelijkheid	Bruikbaarheid voor opsporing en vervolging	Hoeveelheid te bewaren persoonsgegevens	Mate van privacy-inbreuk bij opsporing (groepsgrootte)	Kosten voor de aanbieder
1. Het uitrollen en adopteren van IPv6	Hoog. Minder inspanning nodig voor identificatie. Mogelijk kunnen meer zaken worden opgepakt. Het zal echter even duren voordat ook alle diensten gebruik maken van IPv6. Tot die tijd zullen veel sporen IPv4 zijn en is er geen verbetering.	Minimaal. Informatie over (semi)statische toewijzing IPv6-adresblok aan abonnee (analoog aan IPv4 op vaste netwerken) naar datum/tijd.	Minimaal. Een IPv6-adres is altijd specifiek voor één abonnee/aansluiting. Andere abonnees kunnen direct worden uitgesloten.	Maximaal enkele miljoenen euro. Investering in IPv6 lijkt (ook om andere redenen dan opsporing) uiteindelijk onafwendbaar. Er zijn verschillen tussen operators voor wat betreft reeds gedane investeringen.
2. Vergroten van het aantal publieke IPv4-adressen	Gemiddeld tot hoog, afhankelijk van de groepsgrootte (maximaal bij 1:1-toewijzing). Een IPv4-adres leidt in de meeste gevallen direct tot identificatie. Meer sporen leiden tot identificatie en meer zaken kunnen worden opgepakt.	Beperkt. Informatie over (semi)statische toewijzing IPv4-adres aan abonnee (wordt reeds als zodanig bijgehouden op vaste netwerken)	Gemiddeld. Afhankelijk van de verhouding tussen het aantal publieke IPv4-adressen en het aantal abonnees. Wanneer er één adres per abonnee beschikbaar is, is de inbreuk minimaal. Groepsgroottes vanaf 15 zijn haalbaar.	Maximaal enkele miljoenen euro. Te besteden aan het aankopen van (schaarse) IPv4-adressen en het aanpassen van configuratie.
3. Source port logging	Beperkt, tenzij het bijhouden van informatie over bronpoorten bij dienstaanbieders toeneemt.	Beperkt. Informatie over toewijzing van publiek IPv4-adres en poortreeks aan abonnee naar datum/tijd. Aan de zijde van de dienstaanbieder moeten poortnummers worden gelogd.	Minimaal wanneer een bronpoortnummer, IP-adres, datum en tijd bekend zijn bij opsporing. In alle andere gevallen gemiddeld tot groot, afhankelijk van het aantal abonnees dat het publieke IPv4-adres deelt.	Maximaal enkele miljoenen euro. De informatie wordt nu al (kortstondig) bijgehouden om CG-NAT te laten functioneren. Investeringen zijn nodig om de data te loggen, op te slaan en toegankelijk te maken.
4. Verkeersgegevens gemaskeerd loggen	Gemiddeld tot hoog, afhankelijk van de groepsgrootte en vorm van maskering.	Hoog. Er moet per opgezette verbinding informatie worden opgeslagen. Hieruit is in beperkte mate af te leiden met wie werd gecommuniceerd.	Gemiddeld. Afhankelijk van de verhouding tussen het aantal publieke IPv4-adressen en het aantal abonnees en de wijze waarop wordt gemaskeerd.	Maximaal enkele miljoenen euro. Het betreft opslag van grote hoeveelheden data.
5. Verhogen werkhoeveelheid politie	Laag. Sommige zaken kunnen niet worden opgelost zonder identificatie via IP-adres. In andere zaken is een significante tijdsinvestering nodig om een groep terug te brengen tot één verdachte.	Minimaal. Informatie over (semi)statische toewijzing IPv4-adres aan abonnee (wordt reeds als zodanig bijgehouden op vaste netwerken). Een enkele mobiele ISP houdt daarnaast bronpoortreeksen bij.	Minimaal (bij vaste IP-adressen), gemiddeld (bij mobiele waar gebruik kan worden gemaakt van bronpoortnummers) tot hoog (wanneer geen bronpoortnummer beschikbaar is; meerderheid van de gevallen).	Geen, anders dan de huidige kosten voor het bijhouden, opslaan en beschikbaar maken van de data.

Uiteraard zijn er meer oplossingen denkbaar, maar deze liggen (getuige de gesprekken en ons literatuuronderzoek) minder voor de hand. De volgende mogelijkheden zijn door ons beoordeeld:

- Het via *cross-referencing* (het aan elkaar koppelen van meerdere informatiebronnen) mogelijk toch verbanden ontdekken. Wanneer van een persoon bijvoorbeeld meerdere IP-adressen beschikbaar zijn als spoor, dan kunnen de 'sets' met personen die van deze IP-adressen gebruik maakten over elkaar worden gelegd als een 'zeef' waarbij de daadwerkelijke 'verdachte' uiteindelijk overblijft. Deze techniek wordt al toegepast, en is in de praktijk lastiger dan ze lijkt. Zo spelen er tijdsverschillen tussen servers en kost het de politie veel moeite om de juiste data te verzamelen en te analyseren.

- Het *regionaal uitdelen van IP-adressen* is een mogelijkheid om opsporingsonderzoek verder toe te spitsen. Bij belangrijke zaken kan alle informatie over een persoon waardevol zijn, juist in het bijzonder de locatie (bij benadering). Technisch is geografisch toewijzen van IP-adressen bij NAT voor mobiel echter erg lastig. De internetgebruiker gaat immers via een beperkt aantal locaties het internet op en er is (doorgaans) geen nieuwe toewijzing van een IP-adres aan een gebruiker bij verplaatsing tussen regio's.

4 Internationale vergelijking

In dit hoofdstuk kijken we naar internationale ontwikkelingen op het gebied van NAT en opsporingscapaciteiten. In paragraaf 4.1 beschrijven we het beleid ten aanzien van online identificatie in een aantal relevante referentielanden. Vervolgens concentreren we ons rond IPv6: hoe verhoudt Nederland zich tot andere landen als het gaat om adoptie van IPv6 (paragraaf 4.2) en wat kunnen we verwachten van ISP's, gezien hun internationale context? (4.3). Tot slot bespreken we de belangrijkste lessen die uit de internationale vergelijking kunnen worden getrokken ten aanzien van de Nederlandse situatie.

4.1 Beleid voor online identificatie

Howard et al. [48] concluderen op basis van een internationale vergelijking dat overheden met de ambitie om IPv6 uit te rollen dit het snelste kunnen laten verlopen door de volgende acties:

1. Gebruik IPv6 voor overheidswebsites
2. Verplicht leveranciers aan overheden om IPv6 te gebruiken
3. Communiceer met industrie vertegenwoordigers de zorgen over groeiende kosten van IPv4
4. Benadruk het effect van NAT op opsporingscapaciteiten

In een studie van Levin en Schmidt [49] worden dezelfde beleidsopties onderschreven.

Wanneer overheden eigen websites over IPv6 laten lopen geven ze zelf het goede voorbeeld. Howard et al. [48] laten zien dat de breedste IPv6-implementatie naar websites is in landen met een overheidsbeleid dat IPv6 vereist voor overheidswebsites. Om IPv6-adoptie te stimuleren, kan de overheid als *launching customer* optreden. Als stimulans lijkt dit positieve effecten te hebben gehad. Het heeft de ontwikkeling van de operationele capaciteiten en strategische planning van IPv6 door overheidscontractanten bevorderd. [48]

IPv6 heeft beduidend lagere operationele kosten dan IPv4. Investeringen uit het verleden ten aanzien van CG-NAT zorgen er echter voor dat de apparatuur niet snel vervangen zal worden. ISP's die tegen de limieten van hun CG-NAT-capaciteiten lopen, worden als eerste 'gedwongen' toch de overstap te maken. Door te communiceren over de kosten van CG-NAT kunnen ISP's mogelijk al eerder verleid worden om IPv6 als een serieuze optie te overwegen.

In België is de afspraak om het aantal klanten achter één IPv4-adres te limiteren tot maximaal 16 niet uit de lucht komen vallen. Ingenieurs van Cisco benadrukten bij de Belgische federale overheid de risico's van CG-NAT met betrekking tot opsporing. De 1:16 limiet gaf ISP's en mobiele carriers een stimulans om IPv6 in te zetten. Deze ISP's zagen de limiet op schaalbaarheid en groei in CG-NAT en konden dit vergelijken met de verwachte groei in IPv4-adressen die benodigd waren om de limiet te hanteren.

4.1.1 België

België kent (relatief) het grootste aantal IPv6-gebruikers ter wereld: het internetverkeer van ruim 58% van de gebruikers in België verloopt via IPv6. Dat België een hoog IPv6-adoptiepercentage kent, heeft verschillende oorzaken. Vanuit een beleidsperspectief zijn twee stappen genomen die hebben bijgedragen aan de sterke IPv6-adoptie.

In juni 2012 heeft de Belgische federale overheid een document verspreid onder overheidsinstanties waarin zij werden geadviseerd om IPv6 te verplichten in aanbestedingen. Deze

beleidsmaatregel is niet alleen effectief geweest in België. Uit onderzoek van Howard et al. (2014) blijkt het opnemen van IPv6 in aanbestedingen in verschillende landen positief bij te dragen aan de adoptie van IPv6.

Daarnaast heeft de Belgische overheid met een aantal Belgische ISP's de afspraak gemaakt om het aantal gebruikers over één IPv4-adres te limiteren tot 16. Door één IPv4-adres met maar maximaal 16 gebruikers te delen, wordt de druk op het aantal beschikbare IPv4-adressen verhoogd. Door de gecreëerde schaarste was er voldoende incentive voor (een aantal van) de Belgische ISP's om over te stappen op IPv6. Belgische ISP's die voldoende IPv4-adressen hadden om onder de 1:16 ratio te blijven, hadden minder incentive om over te stappen.

In 2017 houden de meeste van de Belgische ISP's zich aan de 1:16 gebruikersratio. Eén Belgische ISP heeft zelfs een lagere ratio van 1:8 gebruikers geïmplementeerd. Vanuit een opsporingsperspectief is het Belgische beleid succesvol: het gemiddelde aantal gebruikers dat nu achter een mobiel IP-adres zit in het geval van een misdrijf is slechts 4.

4.1.2 Zweden

Zweden kent een turbulente geschiedenis met betrekking tot dataretentiewetgeving. Begin 2003 heeft de Zweedse overheid wetgeving geïntroduceerd dat de ISP's in Zweden verplicht om metadata van gebruikers voor zes maanden te bewaren.

Met het arrest van Digital Rights (Ierland) heeft het Europese Hof (2014) de Europese dataretentierichtlijn onverbindend verklaard. Het Europese Hof heeft bepaald dat generiek en ongedifferentieerd bewaren van communicatiedata niet is toegestaan. In 2014 is Tele2 dan ook gestopt met dataretentie van klanten. Dit werd door de PTS (de Zweedse ACM) niet geaccepteerd en leidde tot een rechtszaak. De Zweedse rechter heeft hier bepaald dat de Zweedse regelgeving niet in strijd was met Zweedse, Europese of andere internationale wet- en regelgeving.

In hoger beroep heeft de Zweedse rechter bepaald dat zij niet voldoende juridische informatie bezat om over deze zaak een oordeel te kunnen vellen. Dit heeft ervoor gezorgd dat de zaak Tele2 vs. PTS naar het Europese Hof is gegaan. Het Europese hof heeft uiteindelijk bepaald dat de Zweedse wetgeving in strijd was met de Europese wetgeving (het Tele2 - arrest).De belangrijkste reden was dat de Zweedse wetgeving voorschrijft dat alle informatie moet worden bewaard, ongeacht het soort informatie, het gebruikte communicatiemiddel of de betrokken persoon. Deze verplichting om algemene en ongedifferentieerde elektronische communicatiegegevens te bewaren, werd niet evenredig gezien bij het maken van een algemene beoordeling van het rechtshandhavingsdoel van de bewaring.

Desondanks heeft de Zweedse regering nu een nieuwe wet omtrent dataretentie geformuleerd (die op 1 oktober 2019 in werking zal treden). De Zweedse overheid stelt dat bij onderzoeken naar internetgerelateerde criminaliteit informatie over wie een bepaald IP-adres heeft, van essentieel belang is om overtreders te kunnen opsporen en identificeren. De wet schrijft voor dat telecommunicatie-exploitanten informatie over elektronische communicatie (waaronder IP-adressen) voor een half jaar opslaan. In Zweden lijkt de problematiek rond CG-NAT en IPv4-adressen te worden geaddresseerd met meer dataretentie. De Zweedse casus geeft aan dat verschillende landen een andere aanpak hebben, en dat de mogelijkheden voor dataretentie nog niet uitgeput zijn.

4.1.3 Europol

De problematiek omtrent de opsporing van personen achter CG-NAT worden ook op Europees niveau onderschreven. [50] [51] In de Internet Organised Crime Threat Assessment (IOCTA)

van 2014 en 2016 wordt CG-NAT als hinderlijk bestempeld in de opsporing van online criminaliteit. [50] [51] Volgens Europol betreft dit ook gevallen van zware criminaliteit, zoals wapenhandel, kinderporno en terrorisme. [52]

De eerste sporen van een online misdrijf zijn vaak e-mails, 'nicknames' op chatsites, verbindingen met websites of logfiles op aangevallen computers. Vervolgens wordt er bij Internet Content Providers (ICP), zoals webhosters en webmaildiensten, een IP-adres en tijdstip opgehaald. Met deze informatie wordt bij een ISP een persoon geïdentificeerd of gelokaliseerd. Wanneer een Internet Content Provider geen poortnummer kan aanleveren, betekent dit in het geval van CG-NAT dat een persoon niet kan worden geïdentificeerd of dat om identificatie mogelijk te maken de privacy van andere gebruikers moet worden geschonden.

Europol stelt de volgende oplossingsrichtingen voor: uiteindelijk is IPv6 dankzij de ongelimiteerde pool aan IP-adressen de meest gewenste oplossing. IPv6 neemt de noodzaak voor CG-NAT (de schaarste aan IPv4-adressen) weg. De transitie naar IPv6 verloopt echter niet zo snel als verwacht. Daarom stelt Europol als oplossingsrichting een vergelijkbare aanpak als België voor, zijnde het limiteren van het aantal gebruikers achter één IP-adres tot een bepaald aantal. Deze vereiste lijkt (al is causaliteit in dit geval lastig vast te stellen) de uitrol van IPv6 te stimuleren: België kent (relatief) het grootste aantal IPv6-gebruikers ter wereld.

4.2 Adoptie van IPv6

De adoptie van IPv6 verschilt enorm tussen landen. Er zijn twee landen waarbij meer dan 50% van de gebruikers IPv6 heeft: India en België. Figuur 19 toont IPv6-gebruik per land als gemeten door Google. Een tweede datapunt is Facebook (Figuur 20) – zij meten een iets hoger gebruik van IPv6 voor Nederland dan Google.

Figuur 19. Percentage gebruikers IPv6 per land als gemeten door Google [53]. Van wit (0%), lichtgroen (Nederland; 15%) tot donkergroen (Duitsland; 42%), rood: regio's waar IPv6 op relatief grote schaal wordt gebruikt, maar waar gebruikers betrouwbaarheidsproblemen of vertraging ondervinden.

Figuur 20 Gebruik van IPv6 gemeten door Facebook (donkerblauw is 100%; Nederland scoort circa 18%). [54]

Nederland behoort, zowel absoluut als relatief naar bevolkingsomvang, tot een van de landen met de meeste IPv4-adressen. Nederland staat op plek 12 met meeste IPv4-adressen wereldwijd (absoluut) en op plek 4 wanneer het aantal IPv4-adressen wordt afgezet tegen de bevolkingsomvang.[60] Alleen de VS, Zweden en Noorwegen hebben relatief meer IPv4-adressen dan Nederland wanneer het aantal adressen wordt afgezet tegen de bevolkingsomvang. In Tabel 8 is de top 15 landen met de hoogste IPv4-ratio weergegeven.

Binnen de top 15 hebben alleen de VS, Zwitserland en het VK een IPv6-adoptiepercentage van meer dan 25%. Het lijkt erop dat tekorten van IPv4-adressen één van de drivers zijn voor IPv6-adoptie.

Tabel 8 Adoptie van IPv6 ten opzichte van de ratio IPv4 adressen/populatie.

Rank	Land	% IPv6 [55]	IP/populatie ratio [42]
1	Verenigde Staten	43,95%	4,91
2	Zweden	7,43%	3,34
3	Noorwegen	14,63%	3,24
4	**Nederland**	**12,72%**	**2,77**
5	Zwitserland	32,72%	2,73
6	Finland	23,22%	2,58
7	Canada	21,32%	2,33
8	Zuid Korea	10,73%	2,30
9	Denemarken	4,27%	2,22
10	Australië	16,37%	2,16
11	Verenigd koningkrijk	27,33%	1,96

[60] Hierbij zijn landen met minder dan 500.000 inwoners niet meegerekend. Denk hierbij aan stadstaten zoals Vaticaanstad en San Marino maar ook eilanden groepen in de stille oceaan.

Rank	Land	% IPv6 [55]	IP/populatie ratio [42]
12	Hong Kong	0,44%	1,65
13	Nieuw Zeeland	15,97%	1,61
14	Japan	28,00%	1,59
15	Taiwan	9,01%	1,53

4.3 Verschillen binnen internationale ISP-concerns

Zoals hierboven is beschreven verschilt de mate adoptie van IPv6 sterk tussen landen. Een vraag die rijst is of het verschil te verklaren is door de nationale context, of sterker vanuit de strategie van ISP's. Een groot deel van de ISP's die in Nederland actief zijn, zijn (deels) eigendom van internationaal conglomeraten: VodafoneZiggo is in handen van Vodafone Group en Liberty Global; T-Mobile Nederland is in handen van Deutsche Telekom. Een vergelijking van de ISP's binnen eenzelfde moederbedrijf, maar in verschillende landen, geeft antwoord op deze vraag.

4.3.1 Vodafone Group

De Vodafone Group is actief in meer dan 20 landen. We zien een sterk verschil tussen de Vodafone-ISP's in de verschillende landen op het gebied van IPv6-adoptie. Tabel 9 toont het aandeel IPv6-verkeer ten opzichte van het totaal, uitgesplitst naar AS-nummer (en daarmee naar ISP), gemeten en geschat door APNIC in 2019.

Tabel 9 Percentage IPv6 voor Vodafone dochtenondernemingen op basis van AS-blokken [55]

Operator	AS	Land	% IPv6
Vodafone	AS9500	Nieuw-Zeeland	57,78
Vodafone	AS38266	India	48,54
Vodafone	AS12353	Portugal	2,76
Vodafone	AS25135	Groot-Brittannië	0,45
Vodafone	AS15480	Nederland	0,27
Vodafone	AS133612	Oostenrijk	4,90
Vodafone	AS21334	Hongarije	0,12
Vodafone	AS15502	Iran	0,12
Vodafone	AS16019	Tsjechië	0,12
Vodafone	AS12302	Roemenië	0,05
Vodafone	AS30722	Italië	0,02
Vodafone	AS12430	Spanje	0,01
Vodafone	AS15897	Turkije	0,01
Vodafone	AS38442	Fiji	0,01
Vodafone	AS30722	Albanië	0,01
Vodafone	AS12663	Duitsland	0,00
Vodafone	AS36935	Egypte	0,00
Vodafone	AS48728	Qatar	0,00

Waar de meeste dochtenondernemingen van Vodafone vrijwel geen IPv6 aanbieden, zijn er twee uitschieters: Nieuw-Zeeland en India.

Nieuw-Zeeland

In Nieuw-Zeeland voert de overheid sinds 2008 een actief beleid om de adoptie van IPv6 te stimuleren. Zo heeft de Nieuw-Zeelandse overheid een *IPv6-taskforce* opgericht. Deze taskforce bestaat uit vertegenwoordigers van verschillende vendors (Huawei, Juniper, Cisco, etc.) en ISP's. De taskforce houdt zich bezig met educatie en training op het gebied van IPv6. De IPv4-schaarste wordt aangemerkt als de primaire reden voor het oprichten van de taskforce, om zo ISP's klaar te stomen voor de toekomst.

Medewerkers van Vodafone raakten overtuigd van het nut van IPv6 om het tekort aan IPv4-adressen op te lossen. [55] In 2016 heeft Vodafone Nieuw-Zeeland IPv6 uitgerold binnen haar mobiele netwerken.

India

In India zien we dat ISP Reliance Jio de overstap naar IPv6 maakte toen het lokale RIR geen IPv4-adressen meer uit gaf. Daarmee was Reliance Jio noodgedwongen om IPv4-adressen aan te schaffen, maar koos ervoor om dit vanuit financiële overwegingen niet te doen. Reliance Jio heeft vervolgens in 9 maanden tijd meer dan 200 miljoen gebruikers overgezet naar IPv6, mede doordat de grote contentproviders beschikbaar zijn over IPv6 en er dus maar weinig IPv4-adressen nodig zijn om verkeer te tunnelen naar content die niet beschikbaar is over IPv6. [56]

De Indiase overheid heeft na het succes van Reliance Jio actief IPv6-adoptie gestimuleerd. [57] Als een gevolg hiervan zien we nu ook een relatief hoog IPv6-adoptiepercentage voor de Indiase tak van Vodafone.

4.3.2 Deutsche Telekom (T-Mobile)

Deutsche Telekom is met T-Mobile als merk (en separate dochterondernemingen) in diverse landen actief. Ook hier zien we sterke verschillen (Tabel 10). We lichten er twee landen uit met een percentage van meer dan 50% IPv6-adoptie op netwerken van Deutsche Telekom: de Verenigde Staten en Griekenland.

Tabel 10 Percentage IPv6 voor Deutsche Telekom dochtenondernemingen op basis van AS-blokken [55]

Operator	AS	Land	% IPv6
T-Mobile	AS21928	Verenigde Staten	98,67
T-Mobile	AS3320	Duitsland	71,35
T-Mobile	AS6799	Griekenland	55,49
T-Mobile	AS5483	Hongarije	37,78
T-Mobile	AS13036	Tsjechië	7,61
T-Mobile	AS8412	Oostenrijk	1,16
T-Mobile	AS12912	Polen	0,02
T-Mobile	AS6855	Slowakije	0,02
T-Mobile	AS31615	Nederland	0,01
T-Mobile	AS5391	Kroatië	0,00
T-Mobile	AS6821	Macedonië	0,00

Verenigde Staten

In de VS liep T-Mobile tegen een tekort aan IPv4-adressen aan. Met het oog op een groeiende markt werd de overstap naar IPv6 gezien als oplossing. Op datzelfde moment was IPv6 nog niet geschikt voor alle mobiele applicaties. Met alleen DNS64 en NAT64 konden diensten zoals WhatsApp en Skype niet functioneren. Niet veel later werd 464XLAT geïntroduceerd en

bleek dit ook geen probleem meer. Daarnaast is 464XLAT een manier om IPv6 uit te rollen zonder grote investeringen in hardware. Door IPv4 NAT-apparatuur te upgraden kan 464XLAT worden gerealiseerd. Er zijn hiermee geen *sunk costs*[61] als een ISP in het verleden CG-NAT boven dual-stack oplossingen prefereerde om het tekort aan IPv4-adressen te overbruggen. Naarmate meer CPE 464XLAT gingen ondersteunen, ging het IPv6-adoptiepercentage gestaag omhoog.

Griekenland

OTE (Deutsche Telekom dochter) heeft eveneens een hoog IPv6-adoptiepercentage. OTE heeft eerst voor breedbandklanten (oftewel, vaste aansluitingen) IPv6 geactiveerd. [55] Later heeft de mobiele tak van OTE, COSMOTE, besloten om IPv6 uit te rollen. COSMOTE is in 2010 begonnen met plannen voor IPv6 en heeft inmiddels een IPv6-adoptiepercentage van ongeveer 77%. [58]

COSMOTE geeft aan dat, ondanks een gebrek aan commerciële prikkel, *vendor push*, of mogelijkheden voor dienstendifferentiatie richting klanten, de volgende overwegingen speelden bij de overstap naar IPv6: [59]

- Publiek tekort aan IPv4-adressen
- Sterke groei in aantal mobiele gebruikers
- Kortlevende kapitaalinvesteringen in CG-NAT voorkomen
- Ondersteuning voor opkomende technologieën als VoLTE en IoT
- Regulatory compliance

Deze motivatie lijkt erop te wijzen dat de verwachte groei van de markt in combinatie met beperkte middelen (geld en IPv4-adressen) de grootste driver waren voor IPv6-adoptie. Zo heeft COSMOTE voor IPv6 gekozen om de groeiende markt op de lange termijn te kunnen bedienen, en werd CG-NAT als kortstondige kapitaalinvestering gezien.

4.3.3 Kenmerken ISP's met een hoog IPv6-adoptiepercentage

De houding ten opzichte van CG-NAT is een belangrijk kenmerk van ISP's met een hoog IPv6-adoptiepercentage. Sommige ISP's zien CG-NAT als een duurzame oplossing waarmee geen drastische aanpassingen in de organisatie of het netwerk hoeven te worden gemaakt, andere ISP's vinden het vooral een kortstondige oplossing en zien de noodzaak om uiteindelijk over te stappen naar IPv6.

APNIC concludeert dat een van de kernmerken die bepalend is voor IPv6-adoptie voor vaste netwerken de hardware is die de gebruikers van de ISP hebben. [55] Zo heeft Comcast in de VS een IPv6-adoptiepercentage van 74%, terwijl alle diensten over IPv4 worden aangeboden. Dit komt doordat de gebruikers hardware inzetten die alleen IPv4 ondersteunt. De adoptie van nieuwere technologieën door de gebruiker kost tijd, met name wanneer de noodzaak voor overschakelen bij de ISP en gebruiker niet aanwezig is. De adoptie van IPv6 is voor deze ISP's slechts een kwestie van tijd: wanneer CPE wordt geüpgraded om IPv6 te kunnen ondersteunen, zal de adoptie van IPv6 vanzelf toenemen.

Internationaal gezien ligt de adoptie van IPv6 hoger voor mobiele netwerken dan voor vaste netwerken. In de VS ligt de adoptie van IPv6 voor alle mobiele ISP's hoger dan 50%. [55] T-Mobile is uitschieter en verwerkt meer dan 90% van het verkeer over IPv6. Ook Verizon Wireless biedt internet over 4G LTE aan en heeft een IPv6-adoptiepercentage van 85%. Het

[61] Kosten die al gemaakt zijn en niet meer ongedaan te maken zijn.

Indiase Reliance Jio is een van de ISP's met het hoogste IPv6-adoptiepercentage, en is tevens een van de snelst groeiende ISP's. [55] Het mobiele netwerk van Reliance Jio is volledig gebaseerd op LTE.

Ten opzichte van modems hebben mobiele apparaten een kortere levensduur. Hierdoor zijn er meer IPv6-compatibele apparaten dan dat er IPv6-compatibele modems zijn. Mobiele ISP's hoeven dus weinig hardware in het netwerk te upgraden om IPv6 aan te kunnen bieden.

Reliance Jio heeft een sterke groei in gebruikers meegemaakt. Deze ISP heeft een hybride ('dual stack') oplossing geïntroduceerd, waarbij IPv4 en IPv6 naast elkaar worden gebruikt. IPv4 is echter niet compatibel met IPv6. Daarom worden ISP's die deze dual-stack oplossing aanbieden na verloop van tijd 'gedwongen' om over te stappen naar IPv6. Een snelle groei in gebruikers leidt alleen tot een groei in IPv6-adoptie wanneer de ISP geen IPv4-adressen meer heeft. Het is dus niet noodzakelijk dat een snelle groeier gebruik moet maken van een dual-stack oplossing. Met name op mobiel wordt er vaak voor gekozen om alle klanten met voor IPv6-geschikte toestellen op IPv6-only te zetten; en om NAT64 en DNS64 te gebruiken om IPv4-only bestemmingen te bereiken en 464XLAT in te zetten om applicaties die IPv4 willen via een IPv6-tunnel naar het IPv4-internet te verbinden.

Vaak wordt de adoptie van IPv6 geassocieerd met hoge kosten. Met name wanneer de ISP genoeg IPv4-adressen heeft, kan de overschakeling naar IPv6 als een 'luxe' worden gezien: de ISP kan in dit geval zijn diensten nog aanbieden over IPv4. Wanneer we echter kijken naar de 20 'rijkste' ISP's ter wereld zien we dat slechts 13 van de 20 ISP's een IPv6-adoptie heeft van meer dan 35%. Er is geen duidelijke correlatie tussen de waarde van een ISP tegenover de adoptie van IPv6.

Wereldwijd worden er geen verbanden gevonden tussen het aantal IPv4-adressen dat een ISP heeft en het percentage gebruikers op IPv6. Vanwege CG-NAT kan een IPv4-adres eenvoudig worden gedeeld met andere gebruikers. Niet alleen vanuit de theorie wordt dit verband in twijfel getrokken, ook empirisch zien we niet dat het aantal gebruikers op één IPv4-adres verband houdt met het aantal gebruikers op IPv6.

4.4 Conclusie: wat betekent dit voor Nederland?

Uit de internationale vergelijking zijn op hoofdlijnen drie lessen te trekken voor de Nederlandse situatie:

1. Het nationaal tekort aan IPv4-adressen is één van de drivers voor IPv6-adoptie. Nederland heeft een relatief zeer groot aantal IPv4-adressen, waardoor er een kleinere prikkel bestaat voor ISP's om IPv6 uit te rollen.

2. De adoptie van IPv6 lijkt niet te worden gedreven door de strategie van de moederbedrijven van de ISP's. Nationale factoren, zoals nationaal beleid, zijn bepalend(er) voor en succesvol geweest bij het al dan niet adopteren van IPv6 door ISP's.

3. Internationaal zien we IPv6 op mobiele netwerken vaak eerder uitgerold worden dan op vaste. We concluderen hieruit dat de technologie volwassen is en dat operators (ook 'incumbents') IPv6 binnen 1-2 jaar op mobiele netwerken kunnen uitrollen.

5 Conclusies

5.1 Beantwoording onderzoeksvragen

In dit onderzoek beantwoorden wij drie deelvragen.

1. Wat zijn mogelijkheden om, tot twaalf maanden na een communicatie, een individuele gebruiker of abonnee van een publiek IP-adres te kunnen identificeren, op basis van een datum- en tijdsaanduiding van de communicatie, en hoe bruikbaar zijn deze voor opsporing en vervolging?

De huidige stand van zaken is als volgt:

- Identificatie van abonneehouders op basis van IP-adres is op de Nederlandse vaste netwerken over het algemeen goed mogelijk. IP-adressen worden relatief statisch uitgedeeld en de informatie over toewijzing wordt gelogd. Er zijn enkele randgevallen, zoals klanten met een IPv6-aansluiting, waarbij IPv4-verkeer via NAT verloopt.

- De mogelijkheden voor identificatie op basis van IP-adres verschillen sterk tussen de mobiele operators. Bij één operator is 1:1-identificatie (tot abonneehouder) mogelijk wanneer de gebruikte bronpoort bekend is. Zo niet, dan is identificatie mogelijk tot tussen 84 en 84.000 abonnees. Dit leidt tot problemen voor opsporingsinstanties.

Om identificatie te verbeteren, zien we verschillende oplossingen. De oplossingen verschillen netto nauwelijks in kosten voor de operators, maar wel sterk als het gaat om de bruikbaarheid voor opsporing en de mate van (mogelijke) privacyschending/juridische proportionaliteit van het bijhouden van informatie.

De meest voor de hand liggende oplossing om 1:1-identificatie te realiseren is uitrol van IPv6. Daarnaast is de sector het erover eens dat (om meer redenen dan identificatie alleen) uiteindelijk zal moeten worden gemigreerd naar IPv6. Er bestaat op dit moment echter nauwelijks een prikkel bij de Nederlandse mobiele internetproviders om dit nu te doen. Een enkele ISP is er reeds mee bezig. Mogelijk kan een sterkere druk vanuit de overheid (als 'klant' van telecommunicatiediensten) een laatste zet in de juiste richting geven. Hoewel IPv6-adoptie enige tijd zal duren, en het IPv4-verkeer waarschijnlijk nooit volledig zal vervangen, leidt het wel tot een lagere druk op CG-NAT en daarmee ook tot verbeterde identificatiemogelijkheden op basis van een IPv4-adres.

Binnen enkele jaren zou ook *zonder* IPv6 identificatie tot een kleinere groepsgrootte haalbaar moeten zijn. We zien het toevoegen van IPv4-adressen als de meest eenvoudige oplossing hiervoor. De ISP's lijken nog over een grote hoeveelheid IPv4-adressen te beschikken die zij zouden kunnen inzetten op hun mobiele netwerk (naar schatting zo'n 4,2 miljoen in totaal). Wanneer voor alle abonnees CG-NAT wordt toegepast, betekent dit identificatie tot een groepsgrootte van vijf abonnees. Wanneer een ISP de eigen IPv4-adressen niet anders kan of wil indelen, zou deze IPv4-adressen kunnen inkopen. Hierbij spelen (eenmalige) kosten en de vraag of deze IPv4-adressen in de gevraagde hoeveelheid beschikbaar zijn.

Een alternatieve oplossing is om terug te keren naar een vorm van logging van verkeersgegevens, waarbij de gegevens worden gemaskeerd. Er is dan niet meer exact te achterhalen met wie een verbinding werd opgezet, maar het is wel mogelijk een (kleinere) groep abonnees te identificeren gegeven een bepaald IP-adres. Of deze oplossingsrichting voldoende verbetering biedt gegeven de te maken kosten, is echter twijfelachtig. De privacy-inbreuk

wordt (vanwege de kleinere groepsgrootte bij identificatie) enerzijds verlaagd, maar (afhankelijk van de invulling van het maskeren) verhoogd.

2. Welke gegevens van een gebruiker zouden per geïdentificeerde mogelijkheid onder de voorgenomen wettelijke bewaarplicht voor telecomaanbieders moeten vallen?

Om de genoemde oplossingen te laten functioneren, zouden ISP's de volgende informatie moeten bijhouden:

1. *Het uitrollen en adopteren van IPv6*: informatie over de toewijzing van publieke IPv6-adressen (naar verwachting semi-statisch toegewezen) en publieke IPv4-adressen (al dan niet via een 464-NAT-oplossing) verbijzonderd naar datum/tijd.

2. *Vergroten van het aantal publieke IPv4-adressen*: informatie over de toewijzing van publieke IPv4-adressen naar abonnees, verbijzonderd naar datum/tijd, zowel bij CG-NAT als bij semi-statische toewijzing.

3. *Source port logging*: informatie over de toewijzing van publiek IP-adres naar abonnee naar datum/tijd (wanneer geen NAT wordt toegepast) en informatie over de toewijzing van de combinatie van publiek IPv4 en uitgaand poortnummer naar abonnee en datum/tijd.[62]

4. *Gemaskeerd loggen van verkeersgegevens*: verkeersgegevens (datum, tijd, abonnee, bestemmingsadres), op een vooraf bepaalde manier gemaskeerd (bijvoorbeeld door alleen bepaalde bits van het bestemmingsadres op te slaan).[63]

5. *Verhogen werkhoeveelheid politie:* in dit geval blijft de huidige retentie van gegevens ongewijzigd. Dat betekent dat de koppeling van IP-adres naar abonnee wordt opgeslagen voor zover deze bekend is, in sommige gevallen aangevuld met bronpoortinformatie.

De datum/tijd moet met zodanige precisie worden opgeslagen dat hergebruik van hetzelfde IP-adres (dan wel dezelfde poort) niet kan leiden tot verwarring tussen abonnees.

3. Wat zijn de kosten om de geïdentificeerde mogelijkheden te implementeren, uitgaande van een implementatietermijn van één, twee of drie jaar, waarbij rekening wordt gehouden met de reguliere/geplande kosten voor afschrijving en vervanging van hardware en software door de aanbieders? In hoeverre speelt het tijdselement daarin een rol?

De ISP's zijn terughoudend in het geven van kostenschattingen voor de genoemde oplossingen. Desondanks verschillen de kosten sterk tussen ISP's als gevolg van de verschillen in infrastructuur en gekozen oplossing voor CG-NAT. Zo zijn de kosten voor de enkele mobiele operator die reeds source port logging toepast uiteraard nihil, maar kunnen deze (zoals toegelicht in het rapport) substantieel zijn indien dit nog niet is gerealiseerd. Ditzelfde geldt voor herverdeling van de IPv4-adressen die een operator reeds ter beschikking heeft.

---

[62] Of dit juridisch haalbaar is, zal afhangen van de huidige discussie over of een IP-adres wel of geen persoonsgegeven is. Poortnummers kunnen gezien worden als verlenging van een IP-adres.

[63] Een juridische toets moet uitwijzen hoeveel en wat voor gegevens daadwerkelijk bijgehouden mogen worden.

Wanneer het gaat om de aankoop van IP-adressen zien we relatief beperkte vaste kosten. We rekenen hierbij op 5 á 6 miljoen euro per operator, waarbij we een budget van circa een half miljoen meerekenen als implementatiekosten. De prijzen stellen tevens 'opportunity cost' voor in het herverdelingsscenario (het geld dat een ISP anders had kunnen verdienen bij de verkoop van de ongebruikte IPv4-adressen).

We constateren dat de hardware die de operators gebruiken zeer waarschijnlijk reeds beschikt over de gevraagde functionaliteiten, en dus niet hoeft te worden vervangen. De tijdsperiode voor uitrol van de hier besproken mogelijkheden speelt dus nauwelijks een rol. Dit geldt in mindere mate voor de oplossing waarin IPv6 wordt uitgerold – hierbij kan het nodig zijn om ook ondersteunende systemen geschikt te maken.

Ten aanzien van de uitrol van IPv6 constateren we daarnaast dat migratie om meerdere redenen voor de hand ligt en de kosten dus niet volledig kunnen worden bepaald noch toegerekend aan het identificatievraagstuk. Om IPv6 uit te rollen over de gehele internetketen, kan het best worden gestart bij de mobiele internetproviders. Als zij overgaan, zal de druk op IPv4 sterk dalen. Daarnaast zal IPv6 gangbaarder worden en volgt de rest van de keten vanzelf. De ISP's hebben echter tot op heden geen urgente redenen gehad om IPv6 uit te rollen.

5.2 Beleidsopties

Er bestaat nauwelijks twijfel over het nut en de noodzaak van eenduidige identificatie op basis van IP-adressen. Steeds vaker zijn er (en als het gaat om cybercrime, steeds vaker alléén) IP-adressen beschikbaar als spoor in een opsporingsonderzoek. De huidige situatie is echter dat IP-adressen in sterke mate worden gedeeld op mobiele netwerken, en dat het bijhouden van verkeersgegevens ten behoeve van identificatie juridische bezwaren kent. Wanneer er niet eenduidig kan worden geïdentificeerd moeten opsporingsdiensten extra identificatiewerk verrichten op een grotere groep (onschuldige) personen, wat een aanvullende en ongewenste privacy-inbreuk met zich meebrengt.

Om in deze context tot verbeterde identificatie op basis van IP-adressen te komen zien we een aantal beleidsopties.

5.2.1 Beleidsoptie 1: Een functionele verplichting tot 1:1-identificatie

IPv6 is, zoals eerder toegelicht, technisch gezien de meest voor de hand liggende oplossing om eenduidige identificatie te realiseren. Deze oplossing heeft echter niet de voorkeur van (alle) mobiele ISP's. Initieel (tot maximaal de komende vijf jaar) zullen sommige operators oplossingen als logging en het toevoegen van IPv4-adressen verkiezen boven uitrol van IPv6. Uiteindelijk verwachten we echter (gezien het stijgende aantal apparaten) dat ook deze operators zullen overgaan naar IPv6.

Door niet direct een verplichting tot uitrol van IPv6 te stellen, worden operators in staat gesteld een migratiepad te kiezen dat aansluit bij de eigen situatie. Investeringen in CG-NAT hoeven niet vervroegd te worden afgeschreven en complexe migratietrajecten van ondersteunende systemen kunnen over langere tijd worden uitgesmeerd. De beleidsoptie zou uiteraard wel kunnen worden gecombineerd met een sterke prikkel om al eerderIPv6 te kiezen als invulling.

Beleidsinstrumenten

De meest voor de hand liggende implementatie van deze beleidsoptie betreft het wettelijk vastleggen van een verplichting voor ISP's om, wanneer zij hiertoe worden verzocht, dermate specifieke gegevens op te leveren dat deze kunnen leiden tot de identificatie van één persoon op basis van (één of meerdere) IP-adressen en tijdstippen.

Aangezien de ISP's waarschijnlijk niet direct kunnen voldoen aan dit verzoek (daar is hun techniek immers nog niet klaar voor), kan overwogen worden om de 1:1-eis pas na een aantal jaar in te laten gaan, en in de tussentijd een hogere grens toe te staan. Uit gesprekken met de politie kwam naar voren dat een groepsgrootte van 25 werkbaar zou zijn. In België is gekozen voor een maximale groepsgrootte van 16.

Verwacht effect

ISP's die ervoor hebben gekozen om niet te investeren in IPv6 worden in deze beleidsoptie niet harder geraakt dan andere ISP's. Het is waarschijnlijk dat ISP's, bij invoering van deze beleidsoptie, een business case zullen maken waarin logging, herverdeling/vergroting van de IPv4-voorraad (indien mogelijk) en IPv6-uitrol zullen worden vergeleken. Afhankelijk van de tijdshorizon die daarbij wordt gehanteerd zal dit in het voordeel van IPv6 (lang) of logging (kort) uitslaan.

5.2.2 Beleidsoptie 2: IPv6-uitrol stimuleren of verplichten

Gelet op het aantal apparaten dat in de toekomst op internet zal zijn aangesloten, is uiteindelijke uitrol en adoptie van IPv6 onafwendbaar. CG-NAT kan het omslagpunt uitstellen, maar blijft (gezien de technische bezwaren en de kosten, die zullen stijgen naarmate het dataverbruik en aantal apparaten groeit) een tussenoplossing. Van overheidswege zouden de Nederlandse ISP's dan ook verplicht kunnen worden tot het uitrollen van IPv6.

Zoals aangegeven is IPv6 op vaste netwerken in sommige gevallen reeds beschikbaar, of verwachten we dat het in de komende twee á drie jaar zal worden uitgerold (eigen opgaaf van de ISP's). Op mobiele netwerken is uitrol van IPv6 (door een kleinere diversiteit in apparatuur) voor consumenten technisch gezien realistisch binnen twee á drie jaar. Eén mobiele ISP geeft aan reeds bezig te zijn met uitrol van IPv6. Alle mobiele ISP's geven aan dat zij met een hoge mate van complexiteit te maken krijgen, doordat systemen die zijn gekoppeld aan de mobiele netten (ten behoeve van bijvoorbeeld facturering) moeten worden bijgewerkt om IPv6 te ondersteunen. Daarnaast zullen niet alle apparaten IPv6 ondersteunen, waarbij met name oudere M2M-apparaten een belangrijke onzekere factor zijn.

Een argument dat de keuze voor deze beleidsoptie zou kunnen onderbouwen, is dat het uitrollen van IPv6 de Nederlandse digitale economie klaarstoomt voor de toekomst. In de context van ontwikkelingen als IoT, 5G en smart mobility biedt het voorop lopen ten aanzien van IPv6 mogelijk een verbeterde concurrentiepositie ten opzichte van andere landen.

Beleidsinstrumenten

In de internationale vergelijking zagen we dat overheden diverse beleidsopties kunnen inzetten om de uitrol van IPv6 te stimuleren. [48] [49] Een voor de hand liggende is wetgeving, welke IPv6 verplicht stelt. We zien dit instrument echter niet in andere landen terug. Het heeft de voorkeur om de keuze van techniek bij de ISP's te laten liggen en het achterliggende doel (betere identificatie) te benadrukken in beleid. Een 'zachter' instrument is het als overheid optreden als launching customer met IPv6-vereiste voor overheidswebsites. We zien dat dit in een aantal landen een positief effect heeft gehad op de uitrol van IPv6.

Onder de aanname dat uitrol van IPv6 onafwendbaar is, ligt het bij deze beleidsoptie niet voor de hand om de ISP's te compenseren voor de kosten die zij hiervoor dienen te maken. De ISP's hebben er immers zelf, vanuit strategische overwegingen, voor gekozen om de uitrol uit te stellen of juist naar voren te halen.

In deze beleidsoptie wordt uitrol, maar niet het *gebruik* van IPv6 verplicht. Omdat er waarschijnlijk nog lange tijd gebruik zal worden gemaakt van IPv4 ligt het voor de hand om dit beleid te combineren met stimulatie van gebruik van IPv6 (onder o.a. dienstenaanbieders) en een functionele verplichting tot identificatie bij IPv4.

Verwacht effect

Zodra is overgestapt op IPv6 zal direct de helft of meer van het internetverkeer (naar volume) via IPv6 verlopen – naar verwachting zal dan ook minimaal de helft van de sporen een IPv6-adres betreffen, en is eenduidige identificatie hiervoor mogelijk. Het overige verkeer zal vervolgens langzaam maar zeker overgaan naar IPv6.

Verkeer dat niet via IPv6 wordt afgewikkeld, wordt afgehandeld via technieken als 464XLAT. Hoewel hier nog steeds sprake is van het delen van IPv4-adressen is het aantal abonnees per adres in principe kleiner, doordat er minder (en steeds minder) poorten per abonnee nodig zullen zijn.

5.2.3 Beleidsoptie 3. Een functionele verplichting tot 1:N-identificatie

In deze beleidsoptie worden, net als bij de vorige beleidsoptie, ISP's verplicht om abonnees te kunnen identificeren op basis van een publiek IP-adres. Anders dan bij de voorgaande beleidsoptie hoeft deze identificatie niet eenduidig te zijn, maar wordt een maximum gesteld aan de 'groepsgrootte' (het aantal abonnees dat wordt gevonden bij een bepaald IP-adres).

Beleidsinstrumenten

Zie boven. In aanvulling zal de gewenste groepsgrootte moeten worden vastgesteld in overleg met opsporingsdiensten en het OM.

Een mogelijkheid is om voor een bepaalde periode een maximum groepsgrootte te hanteren, en binnen een bepaalde termijn over te gaan naar een vereiste tot 1:1-identificatie. Wanneer vooraf wordt aangegeven wanneer deze verplichting van kracht zal worden, hebben de ISP's vrijheid om zelf een strategie te kiezen.

Verwacht effect

Deze beleidsoptie heeft de kleinste impact op de ISP's. Alle ISP's zullen (ofwel voor hun CG-NAT-oplossing, ofwel voor hun 464XLAT-oplossing) logging moeten realiseren. Daarnaast kan met een implementatie van CG-NAT waarbij met 'pools' van IP-adressen wordt gewerkt mogelijk niet aan de verplichting worden voldaan zonder verkeersgegevens te loggen.

Hoe groter de groepsgrootte, hoe moeilijker identificatie is voor opsporingsdiensten, en hoe groter de potentiële inbreuk op privacy van de onschuldige abonnees.

5.2.4 Beleidsoptie 4: Geen nieuw specifiek beleid voeren, 'nudging'

De laatste logische beleidsoptie is om geen nieuw beleid te voeren ten aanzien van identificatie. Het uitgangspunt is dat de markt uiteindelijk IPv6 zal adopteren, waarmee 1:1-identificatie uiteindelijk vaker mogelijk wordt.

Beleidsinstrumenten

Eventueel kunnen 'zachtere' instrumenten worden ingezet om identificatie te verbeteren. Zo kunnen websites/online diensten worden aangespoord om source ports te loggen, en kunnen ISP's worden aangesproken op hun (morele) verantwoordelijkheid. De overheid zou daarnaast een actieve rol kunnen spelen in het herverdelen van IPv4-adressen tussen organisaties die over veel IPv4-adressen beschikken (universiteiten en enkele overheidsinstellingen) en de ISP's. Tot slot zou beleid ter stimulatie van IPv6-uitrol kunnen worden gehanteerd (zie hieronder).

Verwacht effect

Bij een aantal ISP's zal (volgens eigen opgaaf door de ISP's) binnen twee tot drie jaar IPv6 beschikbaar zijn op vaste en mobiele aansluitnetwerken. We verwachten dat het nog minimaal vijf jaar zal duren voordat IPv6 bij alle ISP's uit eigen beweging beschikbaar is gekomen. Zoals eerder aangegeven zal het beschikbaar komen van IPv6 initieel leiden tot 1:1 identificatie voor circa de helft van de sporen en een verkleinde groepsgrootte voor IPv4-sporen. Binnen vijf tot tien jaar zal dan sprake zijn van eenduidige identificatie voor het overgrote deel van de gevallen.

Bij andere ISP's zou de uitrol van IPv6 naar verwachting nog minimaal vijf jaar op zich kunnen laten wachten. Als gevolg van het toenemend aantal op internet aangesloten apparaten zal de identificeerbaarheid van abonnees ten opzichte van de huidige situatie licht afnemen (er zullen meer abonnees een IPv4-adres delen).

Referenties

[1] Justid, (2014). *Factsheet CIOT: Telecomgegevens voor opsporing* [www.justid.nl]

[2] VVD, CDA, D66 en ChristenUnie (10 oktober 2017). *Vertrouwen in de toekomst - regeerakkoord 2017-2021.*

[3] Grapperhaus, F. (2018). *Wijziging van de Telecommunicatiewet en het Wetboek van Strafvordering in verband met de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare telecommunicatiediensten en openbare telecommunicatienetwerken [kamerbrief]* [zoek.officielebekendmakingen.nl]

[4] Vyncke, E. (2018). *What can only be done with IPv6...* [www.ipv6council.be]

[5] Richter, P., Wohlfart, F., Vallina-Rodriguez, N., Allman, M., Bush, R., Feldmann, A., Kreibich, C., Weaver, N., en Paxson, V. (2016). *A Multi-perspective Analysis of Carrier-Grade NAT Deployment* [arxiv.org]

[6] O'Reilly, D. (2018). *The Carrier-Grade NAT Information Gap and Source Port Logging*FRT Solutions.

[7] Europol (2017). *Are you sharing the same IP address as a criminal? Law enforcement call for the end of carrier grade NAT (CGN) to increase accountability online* [www.europol.europa.eu]

[8] StackExchange Skeptics (2015). *Can every grain of sand be addressed in IPv6?* [skeptics.stackexchange.com]

[9] Google (2019). *Per-Country IPv6 adoption* [www.google.com]

[10]Tweede Kamer (12-04-2017). *Overzicht moties en toezeggingen. Prepaid SIM-kaarthouders (p.5)* [zoek.officielebekendmakingen.nl]

[11]Eurpol (2018). *The Internet Organised Crime Threat Assessment 2018* [www.europol.europa.eu]

[12]Rathenau Instituut & Dialogic (2017). *Een nooit gelopen race. Over cyberdreigingen en versterking van weerbaarheid* [www.nctv.nl] Den Haag: Rathenau Instituut.

[13]Europol, (2017). *Carrier-Grade Network Address Translation (CGN) and the Going Dark Problem* []

[14]Wet bewaarplicht van telecommunicatiegegevens (jaargang 2009). *nr. 333.*

[15]Rechtbank Den Haag C/09/480009 / KG ZA 14/1575 (11 maart 2015). *ECLI:NL:RBDHA:2015:2498*

[16]Grapperhaus, F. (26 maart 2018). *Dataretentie [Kamerbrief]* [www.rijksoverheid.nl]

[17]Arrest van het Europees Hof van Justitie in de gevoegde zaken C-203/15 en C-698/15, (21 december 2016). *document 62015CJ0203*

[18]Minister van Justitie en Veiligheid (2018). *Dataretentie. Brief aan de Voorzitter van de Tweede Kamer.* [www.rijksoverheid.nl] Den Haag,

[19]ACM (2019). *Geregistreerde telecom- en postbedrijven* [www.acm.nl]

[20]CBS, (2018). *Huishoudens: samenstelling, grootte, regio, 1 januari* [statline.cbs.nl]

[21]Tweakers.net (2012). *UPC schuift introductie ipv6 door naar medio 2013* [tweakers.net]

[22](2015). *Ziggo zet uitrol ipv6 tijdelijk op lager pitje* [tweakers.net]

[23]de Vries, J. . *Ziggo: 'Uitrol ipv6 gaat nog de nodige jaren duren'* [tweakers.net]

[24]KPN (2019). *IPv6: wat is het en wat kun je ervan verwachten?* [www.kpn.com]

[25]ETSI. *IPv6-Based 5G Mobile Wireless Internet; Deployment of IPv6-Based 5G Mobile Wireless Internet* [www.etsi.org] Sophia Antipoulis, Frankrijk: ETSI.

[26]Cisco. *Statistics per country* [6lab.cisco.com]

[27]Grundemann, C. (2012). *Carrier Grade NAT - Observations and Recommendations*CableLabs.

[28]Vyncke, Eric (2019). *IPv6 Deployment Status* [www.vyncke.org]

[29]Apple (2016). *Supporting IPv6-only Networks* [developer.apple.com]

[30]. *464XLAT -- A Solution for Providing IPv4 Services Over and IPv6-only Network* [sites.google.com]

[31](2012). *Nexus S Android ICS Top Free Apps on T-Mobile USA IPv6-only Network* [docs.google.com]

[32]iPhoned (2018). *'iOS heeft samen met Android volledige smartphonemarkt in handen'* [www.iphoned.nl]

[33]iCulture (2018). *Weinig keuze meer: iOS en Android hebben 99,9% van de markt* [www.iculture.nl]

[34]IETF (2011). *RFC6333: Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion* [tools.ietf.org]

[35]IETF (2013). *RFC6877: 464XLAT: Combination of Stateful and Stateless Translation* [tools.ietf.org]

[36]IETF (2010). *RFC 5771: IANA Guidelines for IPv4 Multicast Address Assignments* [tools.ietf.org]

[37]IETF (2010). *RFC 5735: Special Use IPv4 Addresses* [tools.ietf.org]

[38]IETF (1984). *RFC 919: Broadcasting internet datagrams* [tools.ietf.org]

[39]Provost, M.A. S. (2017). *MIT sells IPv4 addresses* [gist.github.com]

[40]Bort, J. (2011). *Microsoft pays Nortel $7.5 million for IPv4 addresses* [www.networkworld.com] Network World.

[41]RIPE. *IPv4 Transfer Statistics* [www.ripe.net]

[42]Finder, I. (2019). *Top 50 organizations with the largest IP allocations in Netherlands* [ipfinder.io]

[43]ACM, (2018). *Telecommonitor 2018*

[44]Nishizuka, K. . *Carrier-Grade-NAT (CGN) Deployment Considerations* [datatracker.ietf.org]

[45]Dialogic (2016). *The wireless Internet of Things: Spectrum utilisation and monitoring*

[46]IETF (2011). *RFC6302: Logging Recommendations for Internet-Facing Servers* [tools.ietf.org]

[47]W3Techs (2019). *Usage of web servers* [w3techs.com]

[48]Howard, L., en Horton Sowell, J. (2014). *A Comparison of Public Policy Approaches to the IPv4-IPv6 Transition*TPRC Conference Paper.

[49]Levin, S.L., en Schmidt, S. (2014). *IPv4 to IPv6: Challenges, solutions, and lessons* vol. 38, Telecommunications Policy.pp. 1059-1068.

[50]Europol (2016). *The Internet Organised Crime Thread Assessment (IOCTA)* [www.europol.europa.eu]

[51]Europol (2014). *The Internet Organised Crime Threat Assessment (IOCTA) 2014* [www.europol.europa.eu]

[52](Europol), G.M. (2017). *Carrier Grade NAT (CGN) and crime attribution online* [ripe74.ripe.net]

[53]Google (2019). *IPv6 Statistics* [www.google.com]

[54]Facebook (2019). *IPv6 Per-country adoption map* [www.facebook.com]

[55]APNIC, (2019). [stats.labs.apnic.net]

[56]Internet Society (2018). *State of IPv6 Deployment 2018* [www.internetsociety.org]

[57]Government of India, Ministry of Communications, Department of Telecommunications (2018). *National Digital Communications Policy 2018* [dot.gov.in]

[58]Internet Society (2016). *Cosmote introduces IPv6* [www.internetsociety.org]

[59]Manousakis, G. (2017). *IPv6 deployment (challenges) for mobile* [www.ipv6.org.uk] COSMOTE.

[60]Jackson, M. (2018). *Mobile Network Operator EE UK Sees Surge in IPv6 Deployment* [www.ispreview.co.uk]

[61]HvJ EU (16 oktober 2016). *C-582/14*ECLI:EU:C:2016:779,

[62](2019). *6lab - The place to monitor IPv6 adoption* [6lab.cisco.com]

[63]IETF (2014). *Deterministic Address Mapping to Reduce Logging in Carrier-Grade NAT Deployments* [tools.ietf.org]

[64]IETF. *RFC 4941. Privacy Extensions for Stateless Address Autoconfiguration in IPv6* [tools.ietf.org]

Bijlage 1. Overzicht gesprekspartners

Naam	Organisatie	Functie
Anne van Otterlo	Nokia	Account CTO KPN
Caroline Hendriks	Politie	Afdeling IenS
Dennis de Bruin	T-Mobile	Security analytics information lead
Dirk Hakkesteegt	Digivox	Projectmanager
Edwin Groen	Politie	Politie, afdeling IenS
Emile Mons	T-Mobile	Security support engineer
Frank van Berkel	T-Mobile	Senior regulatory counsel
Gerrit-Jan Zwenne	Universiteit Leiden Pels Rijcken	Hoogleraar recht en de informatiemaatschappij Advocaat
Gert Wabeke	KPN	Manager lawful intercept
Hessel Schut	Politie	Team High Tech Crime
Loek Weerd	Politie	Afdeling IenS
Mat Ford	Internet Society	Technology programme manager
Paul Knol	KPN	Senior regulatory officer
Raoul Deijn	T-Mobile	Transport network engineer
René Blankestein	VodafoneZiggo	Government security affairs manager
Wouter Reynders	Nokia	IP network engineer

Contact:
Dialogic innovatie & interactie
Hooghiemstraplein 33-36
3514 AX Utrecht
Tel. +31 (0)30 215 05 80
www.dialogic.nl