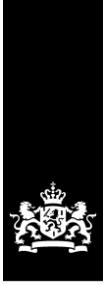

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Overheidsbreed IPv6-nummerplankader

Versie 1.0

Datum 19 oktober 2016
Status Definitief

Inhoud

Versiehistorie

Datum	Versie	Auteur	Opmerkingen
10-12-2015	0.1	Iljitsch van Beijnum	Eerste concept
3-2-2016	0.2	Iljitsch van Beijnum	
2-5-2016	0.9	Iljitsch van Beijnum	Verwerking opmerkingen KING
27-7-2016	0.99	Iljitsch van Beijnum	Verwerking opmerkingen IPO/UVW
19-10-2016	1.0	Iljitsch van Beijnum	Kleine aanpassingen

Begrippenlijst

BGP: Border Gateway Protocol, het systeem waarmee de routers van ISPs en sommige eindgebruikers doorgeven waar welke IP-adressen gebruikt worden

Global unicast adres: adres waarmee wereldwijde één-op-één-communicatie mogelijk is; ofwel een "gewoon" (publiek) adres.

IP: Internet Protocol, de technologie die de basis vormt voor het internet

IP-adres: een IPv4-adres of een IPv6-adres; een IP-adres is nodig voor communicatie over het internet

IPv4-adres: een adres voor gebruik van IPv4, 32 bits lang

IPv6-adres: een adres voor gebruik van IPv6, 128 bits lang

IPv4: Internet Protocol versie 4 (sinds 1981 in gebruik)

IPv6: Internet Protocol versie 6 (wordt nu ingevoerd)

LIR: Local Internet Registry, een organisatie, meestal een ISP, die "lid" is van het RIPE NCC of een andere LIR en op basis daarvan IP-adressen aan kan vragen en verder kan distribueren

Multihoming: tegelijkertijd verbinden met twee of meer internet service providers

NAT: Network Address Translation, een techniek waarbij meerdere systemen één (publiek) adres kunnen delen.

PA: LIRs krijgen van het RIPE NCC één of meer Provider Aggregatable prefixen toegewezen voor eigen gebruik en verdere distributie aan hun klanten

PI: een Provider Independent prefix maakt het mogelijk van ISP te wisselen zonder te hoeven hernummeren; dit is een porteerbaar adresblok

Prefix: een reeks IP-adressen, geïdentificeerd aan de hand van het deel dat alle adressen in de reeks gemeenschappelijk hebben en hoe groot dat gemeenschappelijke deel is

Prefixlengte: de grootte van een reeks IP-adressen. Hoe lager het getal, hoe groter de reeks

RIPE: Réseaux IP Européens, een organisatie die zichzelf beschrijft als "a forum open to all parties with an interest in the technical development of the Internet"

RIPE NCC: RIPE Network Coordination Centre, de RIR die IP-adressen uitgeeft in Europa, het Midden-Oosten en de voormalige Sovjet-Unie

RIR: Regional Internet Registry. De vijf RIRs (AFRINIC, APNIC, ARIN, LACNIC en RIPE NCC) geven IP-adressen uit in verschillende delen van de wereld

Site local adres: zie unique site local adres

Unique site local adres (ULA): een adres dat alleen voor interne communicatie gebruikt kan worden; onderdeel van de eigen (unieke) reeks interne adressen van de organisatie

1. Samenvatting

De overgang van het huidige IPv4 naar het nieuwe IPv6 biedt de mogelijkheid om een overheidsbreed IPv6-nummerplankader op te stellen. Hiermee krijgen alle overheidsorganisaties binnen Nederland IPv6-adressen uit één reeks of een klein aantal reeksen IPv6-adressen en gebruiken zij deze adressen op een gestandaardiseerde manier. Dit maakt het mogelijk om IP-pakketten snel in firewalls te identificeren als komende van een overheidsorganisatie en een globale inschatting van het gewenste beveiligingsniveau te maken.

Logius vraagt bij het RIPE NCC, de organisatie die in Europa IP-adressen uitdeelt, voldoende IPv6-adresruimte aan voor alle Nederlandse overheidsorganisaties. Grote blokken worden gedelegeerd aan ministeries, die intern kleinere blokken IPv6-adressen uitgeven aan deelorganisaties. Gemeenten, provincies, waterschappen, ZBOs en andere overheidsorganisaties die niet onder een ministerie vallen vragen hun adresreeks rechtstreeks bij Logius aan.

Dit document beschrijft de achtergrond en de implementatie van het overheidsbrede IPv6-nummerplankader. Binnen dit kader stelt elke organisatie een eigen IPv6-nummerplan op.

2. Inleiding

In opdracht van het ministerie van BZK heeft TNO onderzocht in hoeverre een overheidsbreed IPv6-nummerplankader kan bijdragen tot leveranciersonafhankelijkheid, informatieveiligheid en financieel voordeel.[1] Het onderzoek trekt de volgende conclusie:

> "Uit het onderzoek komt naar voren dat een beperkte set afspraken een bijdrage kan leveren aan leveranciersonafhankelijkheid, informatieveiligheid en efficiënt beheer van de ICT-infrastructuur van de overheid. Dit kan worden bereikt door het in gebruik nemen van overheidseigen IPv6-adressen. Met overheidseigen adressen kan de overheid zelf haar IPv6-adressen op internet beter beschermen tegen misbruik, kunnen omnummerkosten bij een leverancierswissel worden voorkomen en wordt het mogelijk om overheden redundant via verschillende internetproviders aan te sluiten. Het gebruik van één overheidsadresblok maakt adressen herkenbaarder en eenvoudiger te registreren wat kan helpen bij detectie van misbruik en het maken van onderscheid tussen overheidsverkeer en niet-overheidsverkeer."

Dit document voorziet in de implementatie van een overheidsbreed IPv6-nummerplankader.

Ten tijde van het opstellen van de eerste versie van dit document beschikte het Ministerie van Defensie al over een eigen IPv6-blok. Defensie zal dat blok blijven gebruiken en valt dus buiten het overheidsbrede IPv6-nummerplankader.

Het overheidsbrede IPv6-nummerplankader stelt een kader voor het gebruik van IPv6-adressen binnen de Nederlandse overheid. Dit kader heeft twee aspecten:

1. Iedere overheidsorganisatie binnen Nederland krijgt IPv6-adresruimte uit twee overkoepelende blokken IPv6-adressen.

2. Iedere overheidsorganisatie binnen Nederland krijgt zestien blokken IPv6-adressen, waarbij ieder blok bestemd is voor doeleinden binnen een voorgeschreven beveiligingscategorie. (Er zijn bijvoorbeeld categorieën voor servers die met het publieke internet communiceren en servers die alleen binnen besloten overheidsnetwerken communiceren.) Het gebruik van deze beveiligingscategorieën wordt in een apart document beschreven.

Met inachtneming van het bovenstaande is iedere organisatie verder zelf verantwoordelijk voor haar interne IPv6-nummerplan.

[1] Overheidsbrede beleidskaders voor IPv6-nummerplannen https://www.rijksoverheid.nl/documenten/rapporten/2015/04/03/overheidsbrede-beleidskaders-voor-ipv6-nummerplannen

Het Nationaal Beraad Digitale Overheid heeft in september 2015 het advies overgenomen aan "overheidsorganisaties buiten de Rijksoverheid om zoveel mogelijk gebruik te maken van overheidseigen IPv6-adressen." (De Rijksoverheid heeft alreeds beleid om overheidseigen adressen te gebruiken.)[2]

Het overheidsbrede IPv6-nummerplankader voorziet zowel in IPv6-adressen voor gebruik over het internet als IPv6-adressen voor besloten gebruik. Overheidsorganisaties kunnen zelf kiezen via welke leverancier of leveranciers van toegang tot het internet zij hun IPv6-adressen bereikbaar maken. Ondanks het gebruik van een tweetal overkoepelende IPv6-adresblokken is er dus geen sprake van gezamenlijke inkoop van internet-connectiviteit.

Zie de begrippenlijst voor de beschrijving van de gebruikte terminologie en de appendix voor meer achtergrondinformatie over IPv6.

[2] https://digitaleoverheid.pleio.nl/file/download/41685692

3. Doel en achtergrond

Het gebruik van een uniek overheidsbreed IPv6 nummerplan stelt de overheid in staat om omnummering bij het wisselen van leveranciers te voorkomen. Een vaste indeling in verschillende beveiligingscategorieën maakt het afdwingen van restricties simpeler; vanuit beheerperspectief wordt het maken van fouten beperkt en het opsporen van fouten wordt vergemakkelijkt. Overheidsorganisaties hoeven niet zelf kosten te maken om rechtstreeks IPv6-adresruimte bij het RIPE NCC aan te vragen.

3.1. Bestaande situatie IPv4

Bij de invoering van IPv4 de afgelopen tientallen jaren hebben verschillende overheidsorganisaties zich gericht op organisatienummerplannen maar was er geen gelegenheid om een overheidsbreed nummerplan of nummerplankader te introduceren. Als gevolg hiervan worden bij de verschillende overheidsorganisaties IPv4-adresblokken van verschillende ISPs en dienstverleners gebruikt en/of zijn zij LIR (lid van het RIPE NCC) en krijgen daarmee rechtstreeks IPv4-blokken toegewezen door het RIPE NCC.

Het gebruik van adressen van ISPs en dienstverleners is over het algemeen in eerste instantie simpel en kosteneffectief, maar brengt extra werk en kosten met zich mee bij het overstappen naar een andere leverancier; dan moeten systemen adressen van de nieuwe leverancier krijgen (omnummeren). Om die reden is het gebruik van niet-leveranciersgebonden (porteerbare / provider independent) adressen wenselijk. Vóór het opraken van de IPv4-adressen was het lid worden van RIPE NCC de aangewezen manier om aan grotere aantallen leveranciersonafhankelijke IPv4-adressen te komen. Dit ging in de vorm van één of meer eigen provider aggregateable (PA) adresblokken (het soort adresblokken dat uitgegeven wordt aan ISPs om verder te delegeren naar hun klanten). Voor die tijd was het ook mogelijk om provider independent (PI) adresblokken aan te vragen en tot en met de vroege jaren ’90 waren alle IPv4-adressen die uitgegeven werden de facto provider independent.

3.2. Nieuwe situatie IPv6

De introductie van IPv6 biedt de mogelijkheid om het gebruik van IPv6-adressen overheidsbreed te standaardiseren. Alle overheidsorganisaties beschikken zo over leveranciersonafhankelijke (PI) adresblokken zonder dat het nodig is om en masse kosten te maken om LIR te worden. De directe kosten van het LIR-schap zijn relatief beperkt, maar de inwerktijd om bekend te worden met de door het RIPE NCC gehanteerde procedures en de tijd benodigd voor het in stand houden van die kennis is aanzienlijk.

De grootte van de IPv6-adresruimte maakt het mogelijk om de adressen die toegewezen worden aan iedere overheidsorganisatie volgens een vast stramien onder te verdelen in verschillende beveiligingscategorieën. De combinatie van een overheidsbrede reeks IPv6-adressen en een gestandaardiseerde encodering van beveiligingscategorieën in die

adressen maakt het beperken van communicatie tot geautoriseerde systemen met firewallregels aanzienlijk makkelijker en vooral ook minder foutgevoelig.

Een overheidsbreed IPv6-nummerplankader heeft dus voordelen op het gebied van leveranciersonafhankelijkheid en informatiebeveiliging, en heeft financiële voordelen boven de situatie waarbij veel overheidsorganisaties zelf LIR worden.

3.3. Kader van het overheidsbreed IPv6-nummerplan

Het overheidsbreed IPv6-nummerplankader beperkt zich tot het clusteren van de IPv6-adresblokken die verschillende overheidsorganisaties gebruiken onder één (of een zeer beperkt aantal) overkoepelend IPv6-adresblok of -blokken en het gecoördineerd op een vaste plek binnen elk IPv6-adres opnemen van een beveiligingsniveau. Binnen dit kader is het aan iedere deelnemende organisatie om autonoom een eigen IPv6-adresplan op te stellen en te implementeren. Zie hiervoor ook het SURFnet Whitepaper IPv6-nummerplan opstellen.[3] In het najaar van 2016 zal Logius een handleiding opstellen IPv6 nummerplan voor overheidsorganisaties publiceren.

3.4. IPv6-adressen voor intern gebruik

Het overheidsbreed IPv6-nummerplankader voorziet zowel in adressen voor gebruik over het publieke internet, voor het gebruik tussen overheidsorganisaties onderling als ook voor puur intern gebruik. Er wordt dus in alle gevallen gebruik gemaakt van “global unicast” (publieke) adressen. Het gebruik van unique site local adressen (ULA), de IPv6-versie van RFC 1918-adressen, is om onderstaande redenen ongewenst.

Een organisatie komt aan een reeks unique site local adressen (ULA) door deze zelf te genereren op basis van een willekeurig getal.[4] Het is dus mogelijk dat twee organisaties intern dezelfde ULA-reeks gebruiken, hoewel het risico hierop minimaal is vanwege de grootte van de willekeurige getallen. Het is niet mogelijk een reeks ULAs bij het RIPE NCC of een andere registry aan te vragen.

Een risico bij het gebruik van ULAs is dat ze niet herkenbaar zijn als overheidsadressen, een eventuele andere gebruiker heeft een even legitieme claim op een ULA-reeks. Het verdient daarom de voorkeur om global unicast overheidsadressen te gebruiken voor alle toepassingen: zowel communicatie over het publieke internet als communicatie binnen besloten overheidsnetwerken en ook voor puur interne systemen. Bij het gebruik van de juiste beveiligingscategorie kunnen adressen voor intern gebruik simpel uitgefilterd worden aan de rand van het netwerk. Tevens kunnen de adresblokken die overeenkomen met hogere beveiligingscategorieën simpelweg niet aan de rest van de wereld geadverteerd worden, waardoor ze niet vanaf het internet bereikbaar zijn.

---

[3] https://www.surf.nl/kennisbank/2013/whitepaper-ipv6-nummerplan-opstellen.html

[4] Unique Local IPv6 Unicast Addresses (RFC 4193) https://tools.ietf.org/html/rfc4193

De ervaring leert dat systemen waarvan voorzien was dat ze alleen intern benaderbaar hoefden te zijn toch vaak later ook voor andere organisaties toegankelijk gemaakt moeten worden. Onder andere om in die gevallen omnummering van ULA naar overheidsadressen te voorkomen wil de overheid alleen gebruikmaken van overheids- (global unicast) adressen.

Let ook op dat bij IPv6 NAT zelden of nooit toegepast wordt; het is dus niet mogelijk intern ULAs te gebruiken en die naar global unicast-adressen te vertalen aan de rand van het netwerk.

3.5. Niet-overheidsorganisaties

Een overheidsorganisatie kan bij het uitbesteden van een functie een adresreeks delegeren aan de dienstverlener voor het uitvoeren van deze functie. Dit heeft als voordelen dat de betreffende functie aan de gebruikte adressen herkenbaar blijft als overheidsfunctie en ook dat bij het overgaan op een andere dienstverlener de adressen kunnen overgaan op de nieuwe dienstverlener zonder hernummeren (portabiliteit).

Als een dienstverlener optreedt voor meerdere overheidsorganisaties en het niet nodig is dat de uitgevoerde functie aan het adres herkenbaar is als behorende bij een specifieke overheidsorganisatie, maar het is wel gewenst dat de gebruikte adressen herkenbaar zijn als overheidsadressen en/of er over een besloten overheidsnetwerk gecommuniceerd moet worden, dan kan de betreffende dienstverlener een eigen adresblok krijgen binnen het overheidsbrede IPv6-nummerplankader. Hiervoor is een specifieke reeks adressen binnen het nummerplan gereserveerd.

Dienstverleners mogen adressen uit het overheidsnummerplankader alleen gebruiken voor de door een overheidsorganisatie uitbestede functie of functies.

4. Deelnemende overheden

In principe geldt dit nummerplankader voor alle Nederlandse overheidsorganisaties. Vooralsnog is alleen het Ministerie van Defensie hiervan uitgezonderd.

4.1. Overzicht overheidsorganisaties

Op standaarden.overheid.nl[5] is het volgende overzicht van overheidsorganisaties te vinden:

Type overheidsorganisatie	Aantal
Adviescollege	37
Deelgemeente	34
Dienst	53
Gemeente	587
Hoog College Van Staat	6
Koepelorganisatie	3
Koninklijk Huis	1
Ministerie	16
Openbaar Lichaam	33
Politiekorps	27
Provincie	12
Rechterlijke Macht	41
Regering	1
Regionaal Samenwerkingsorgaan (GGD, Milieudienst, Plusregio, Recreatieschap, SocialeDienst, Veiligheidsregio)	264
Rijksinspectie	17
Staten-Generaal	3
Tuchtrechtelijke Instantie	48
Waterschap	31
Zelfstandig Bestuursorgaan	183
Totaal	1397

Deze aantallen zijn echter niet volledig actueel; na fusies wordt de nieuwe organisatie aan de lijst toegevoegd, maar oude organisaties blijven staan. Naar schatting is het daadwerkelijke totaal ongeveer 20% lager dan de genoemde 1397 overheidsorganisaties.

De volgende typen overheidsorganisaties hebben vooral een nationaal karakter:

[5] http://standaarden.overheid.nl/owms/4.0/doc/waardelijsten

Type overheidsorganisatie	Aantal
Adviescollege	37
Dienst	53
Hoog College Van Staat	6
Koepelorganisatie	3
Koninklijk Huis	1
Ministerie	16
Openbaar Lichaam	33
Regering	1
Rijksinspectie	17
Staten-Generaal	3
Zelfstandig Bestuursorgaan	183
Totaal	353

De volgende typen overheidsorganisaties hebben met name een lokaal of regionaal karakter:

Type overheidsorganisatie	Aantal
Deelgemeente	34
Gemeente	587
Politiekorps	27
Provincie	12
RechterlijkeMacht	41
RegionaalSamenwerkingsorgaan (GGD, Milieudienst, Plusregio, Recreatieschap, SocialeDienst, Veiligheidsregio)	264
TuchtrechtelijkeInstantie	48
Waterschap	31
Totaal	1044

Het is altijd mogelijk dat er nieuwe overheidsorganisaties in het leven geroepen worden die ook adresruimte nodig hebben, of dat er na fusies nieuwe adressen nodig zijn en de adressen van de oude deelorganisaties pas later geretourneerd worden. Als zodanig geven de bovenstaande aantallen een indicatie, maar geen volledige zekerheid over de hoeveelheid organisaties die IPv6-adressen nodig hebben.

5. Ontwikkeling IPv6-nummerplankader

Bij het ontwikkelen van het Nederlandse overheidsbrede IPv6-nummerplankader is gekeken naar het Duitse IPv6-nummerplan.

De Duitse federale overheid beschikt over een /26 IPv6-prefix (64 /32s), waaruit /32s gedelegeerd zijn aan "sub-LIRs". De 16 deelstaten zijn sub-LIRs en tevens zijn er twee /32s voor landelijke netwerken en vier /32s aan defensie uitgegeven. De deelstaten geven als sub-LIR op hun beurt IPv6-adressen uit aan overheidsorganisaties binnen hun grondgebied.

De Duitse indeling in sub-LIRs kan in Nederland in enigszins gewijzigde vorm ook toegepast worden. Maar in plaats van deelstaten (die Nederland niet heeft) zouden dan de ministeries sub-LIR worden, in overeenstemming met de positie van ministeries in het Nederlandse staatsbestel.

In Nederland zijn de provincies een laag tussen het landelijke en lokale/regionale niveau. Maar gezien het feit dat Nederland geen federale structuur kent en de provincies geen ICT-gerelateerde taken uitvoeren ten behoeve van lagere overheden op hun grondgebied ligt het niet voor de hand om de provincies sub-LIR te maken. Hierbij komt nog het feit dat veel waterschappen provincie-overschrijdend zijn. In plaats van het Duitse hiërarchische model worden daarom twee aparte blokken gereserveerd voor lokale/regionale overheidsorganisaties (gemeenten, provincies, waterschappen, enzovoort).

Het model voor het overheidsbrede IPv6-nummerplankader voor de Nederlandse situatie ziet er dan als volgt uit:

Overige organisaties (grotere adresblokken)	/32
Ministerie van Financiën (Fin)	/32
Ministerie van Infrastructuur en Milieu (I&M)	/32
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK)	/32
Ministerie van Veiligheid en Justitie (V&J)	/32
Ministerie van Algemene Zaken (AZ)	/32
Ministerie van Buitenlandse Zaken (BuZa)	/32
Ministerie van Economische Zaken (EZ)	/32
Ministerie van Onderwijs, Cultuur en Wetenschap (OCW)	/32
Ministerie van Sociale Zaken en Werkgelegenheid (SZW)	/32
Ministerie van Volksgezondheid, Welzijn en Sport (VWS)	/32
Lokale overheidsorganisaties	/32
Regionale overheidsorganisaties	/32
Overige organisaties (kleinere adresblokken)	/32
Gereserveerd	2 x /32
Totaal	**/28**

Omdat de gewenste plaats van de beveiligingscategorie in het IPv6-adres verschilt afhankelijk van de grootte van het toegewezen adresblok worden

hier twee verschillende /32-blokken voor gereserveerd waar de beveiligingscategorie op een andere plaats opgenomen wordt.

5.1. Aanvangssituatie

Bij aanvang van het opstellen van dit document bestond de volgende situatie:

- Defensie is LIR en beschikt over het blok 2a04:8f80::/29
- Logius is LIR en beschikt over het blok 2a04:9a00::/29 ten behoeve van de Rijksoverheid

De reeks van Logius is als volgt onderverdeeld:

- Logius: Overige organisaties Rijk 2a04:9a00::/32
- Ministerie van Financiën (Fin) 2a04:9a01::/32
- Ministerie van Infrastructuur en Milieu (I&M) 2a04:9a02::/32
- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) 2a04:9a03::/32
- Ministerie van Veiligheid en Justitie (V&J) 2a04:9a04::/32
- Gereserveerd 2a04:9a05::/32
- Gereserveerd 2a04:9a06::/32
- Gereserveerd 2a04:9a07::/32

5.2. Aanvraag/toewijzing RIPE NCC

Onder de geldende regels van het RIPE NCC was het niet mogelijk om de prefix 2a04:9a00::/29 van Logius uit te breiden naar 2a04:9a00::/28 om het eerder genoemde model voor de Nederlandse situatie te realiseren.

Als alternatief hiervoor is een extra /29 prefix aangevraagd op naam van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties; de prefix 2a07:3500::/29 is toegewezen.

Voor het overheidsbrede IPv6-nummerplankader zijn hiermee de volgende prefixen beschikbaar:

2a04:9a00::/29
2a07:3500::/29

6. Indeling overheidsbrede IPv6-nummerplankader

Na toewijzing van het decentrale blok door het RIPE NCC is de indeling van de overheids-IPv6-adressen als volgt:

Prefix	**Gebruikt door**	**Beveiligingsbits**
2a04:8f80::/29	*Defensie*	*Niet van toepassing*
2a04:9a00::/32	Overige organisaties (grotere blokken)	32 – 35
2a04:9a01::/32	Financiën	32 – 35
2a04:9a02::/32	Infrastructuur en Milieu	32 – 35
2a04:9a03::/32	Binnenlandse Zaken en Koninkrijksrelaties	32 – 35
2a04:9a04::/32	Veiligheid en Justitie	32 – 35
2a04:9a05::/32	Gereserveerd (ministerie)	32 – 35
2a04:9a06::/32	Gereserveerd (ministerie)	32 – 35
2a04:9a07::/32	Gereserveerd (ministerie)	32 – 35
2a07:3500::/32	Vrij	Nader te bepalen
2a07:3501::/32	Vrij	Nader te bepalen
2a07:3502::/32	Vrij	Nader te bepalen
2a07:3503::/32	Vrij	Nader te bepalen
2a07:3504::/32	Gemeenten	44 – 47
2a07:3505::/32	Provincies / waterschappen	44 – 47
2a07:3506::/32	Overige organisaties (kleinere blokken)	44 – 47
2a07:3507::/32	Gereserveerd	44 – 47

De prefix 2a04:8f80::/29 van het Ministerie van Defensie maakt geen onderdeel uit van het overheidsbrede IPv6-nummerplankader.

De prefix 2a04:9a00::/32 wordt gebruikt door overheidsorganisaties die behoefte hebben aan minder adresruimte dan een /32 maar meer dan een /44.

De prefixen 2a07:3500::/32 – 2a07:3503::/32 worden vrijgehouden. De plaats van de beveiligingsbits binnen deze prefixen zal vastgesteld worden wanneer deze prefixen in gebruik genomen worden.

De prefix 2a07:3504::/32 wordt gebruikt door gemeenten en samenwerkingsverbanden tussen gemeenten.

De prefix 2a07:3505::/32 wordt gebruikt door provincies en waterschappen en hun samenwerkingsverbanden.

De prefix 2a07:3506::/32 wordt gebruikt door overheidsorganisaties die behoefte hebben aan een /44.

7. Toewijzing IPv6-adressen

Logius delegeert naar de ministeries met grote uitvoeringsorganisaties een prefix ter grootte van een /32. De organisatie binnen het betreffende ministerie die deze delegatie ontvangt is verantwoordelijk om IPv6-adressen uit te delen aan overige organisaties binnen het betreffende ministerie met inachtneming van de RIPE-regels.

Om het mogelijk te maken dat iedere overheidsorganisatie met een eigen IPv6-adresblok zelf via één of meerdere ISPs naar keuze met het publieke internet verbonden kan worden is de maximale prefixlengte (minimale grootte van het adresblok) een /48. Dit is de minimale grootte van een adresblok dat ISPs algemeen accepteren om via het internet te routeren.

Landelijk opererende organisaties krijgen adresruimte uit het adresblok 2a04:9a00::/29, ofwel via het ministerie waar ze onder vallen ofwel rechtstreeks van Logius. Bij adressen uit dit blok wordt de beveiligingscategorie gecodeerd in bits 32 – 35, met als gevolg dat de zestien /48s die voor een individuele organisatie gereserveerd worden geen aaneengesloten reeks vormen.

Voorbeeld: V&J heeft adresblok 2a04:9404::/32, waarbinnen 2a04:9404:**3**000::/36 het deel is met beveiligingscategorie 3.

Gemeenten, provincies, waterschappen en andere decentrale overheidsorganisaties krijgen adresruimte uit het adresblok 2a07:3500::/29. Binnen dit adresblok wordt de beveiligingscategorie in bits 44 – 47 gecodeerd. Als gevolg hiervan vormen de zestien /48s die per organisatie gereserveerd worden *wel* een aangesloten blok, ter grootte van /44.

Voorbeeld: een decentrale overheidsorganisatie heeft 2a07:3506:1000::/44. Hiervan is 2a07:3506:100**3**::/48 het deel met beveiligingscategorie 3.

Overheidsorganisaties die kunnen onderbouwen dat ze niet genoeg hebben aan één /48 per beveiligingscategorie kunnen één of meer extra reeksen van 16 /48s aanvragen.

7.1. Beveiligingscategorieën

Om in de communicatie tussen verschillende overheidsorganisaties effectief en efficiënt te kunnen filteren op basis van beveiligingscategorieën is het van belang dat beveiligingscategorieën op een gecoördineerde wijze toegepast worden.

De indeling van de beveiligingscategorieën zal in een apart document beschreven worden. Hierop vooruitlopend kan beveiligingscategorie 1 gebruikt worden voor servers die over het externe internet communiceren.

7.2. Delegeren adressen aan dienstverleners

Het heeft sterk de voorkeur dat adressen uit het overheidsbrede IPv6-nummerplankader gebruikt worden voor alle systemen binnen een overheidsorganisatie en voor alle diensten die door of namens een overheidsorganisatie uitgevoerd worden.

Voor uitbestede diensten kan een overheidsorganisatie adresruimte van de organisatie aan een dienstverlener delegeren om te gebruiken voor het bereikbaar maken van de betreffende dienst. De dienstverlener zorgt er dan voor dat de gedelegeerde adressen over het internet gerouteerd worden.

Er kunnen bepaalde waarden in de beveiligingsbits beschikbaar zijn om aan dienstverleners gedelegeerd te worden, zie hiervoor het betreffende document. Als er niet zo'n waarde beschikbaar is kan er voor dit doel extra IPv6-adresruimte aangevraagd worden door de organisatie.

De dienstverlener mag adressen uit het overheidsbrede IPv6-nummerplankader alleen gebruiken voor de verlening van de betreffende overheidsdiensten en niet voor overige eigen bedrijfsdoeleinden of ten behoeve van andere klanten. Mocht de dienst op een later moment bij een andere aanbieder ondergebracht worden dan kunnen de gedelegeerde IPv6-adressen meeverhuizen naar de nieuwe aanbieder.

8. Aanvraag- en uitgifteprocedures

8.1. Algemeen

Uitgegeven adresblokken dienen in de RIPE whois-database[6] geregistreerd te worden, waarbij een administratief en technisch contact opgenomen wordt. Het administratief contact is de "eigenaar" van de adressen, het technisch contact zal benaderd worden bij technische problemen. Let op dat de RIPE database publiekelijk te raadplegen is; het gebruik van een rol-contact in plaats van een persoonscontact wordt daarom sterk aanbevolen.

8.2. Ministeries

Aan ministeries wordt een /32 toegewezen voor gebruik door dat ministerie en organisaties die onder de verantwoordelijkheid van dat ministerie vallen.

Het verdient aanbeveling dat een ministerie een plan opstelt voor het toewijzen van adressen uit die /32 aan onderdelen en andere organisaties. Dit plan kan naar eigen inzicht vormgegeven worden zolang de eerder beschreven indeling in beveiligingscategorieën toegepast wordt.

Mochten er in de toekomst organisaties naar een ander ministerie verhuizen, dan is ofwel migratie/omnummering naar een nieuw adresblok nodig, ofwel de betreffende organisatie blijft de bestaande adressen gebruiken. In het laatste geval zal de strikte hiërarchische verdeling van adressen per ministerie verwateren. Ervaring leert dat een dergelijke verwatering niet of nauwelijks te voorkomen is omdat het omnummeren van IP-adressen een potentieel kostbare en langdurige aangelegenheid is.

Gezien het kleine aantal ministeries zal er geen formele aanvraagprocedure opgesteld worden; aanvragers kunnen contact opnemen met het Logius Servicecentrum.

De betreffende adresblokken zullen in de RIPE-database geregistreerd worden.

8.3. Ministeriële organisaties

Overheidsorganisaties die onder de verantwoordelijkheid van een ministerie vallen vragen hun IPv6-adressen aan bij het betreffende ministerie. Dat ministerie zal adressen toekennen uit zijn /32. Ministeries zullen hiervoor aanvraagprocedures opstellen. Neem in geval van twijfel contact op met het Logius Servicecentrum.

De betreffende adresblokken zullen in de RIPE-database geregistreerd worden.

[6] RIPE whois https://apps.db.ripe.net/search/query.html

8.4. Rijk/nationaal overig

Overheidsorganisaties met een nationaal karakter die niet onder de verantwoordelijkheid van een ministerie vallen kunnen IPv6-adresruimte aanvragen bij Logius.

De betreffende adresblokken zullen in de RIPE-database geregistreerd worden.

8.5. Regionaal/lokaal

Overheidsorganisaties met een regionaal of lokaal karakter zoals provincies en waterschappen en hun samenwerkingsverbanden en gemeenten en samenwerkingsverbanden tussen gemeenten kunnen IPv6-adresruimte aanvragen bij Logius.

In samenwerking met IPO, UVW en KING zullen wellicht IPv6-adresreeksen proactief aan provincies, waterschappen en gemeenten toegewezen worden zonder dat zij hiervoor zelf een aanvraag hoeven te doen. Uiteraard kunnen deze toewijzingen op verzoek gewijzigd worden, neem hiervoor contact op met het Logius Servicecentrum.

De betreffende adresblokken zullen in de RIPE-database geregistreerd worden.

8.6. DNS

Voor systemen die in de DNS een IPv6-adres hebben is het zeer wenselijk dat er ook een reverse mapping van het betreffende IPv6-adres naar de naam in de DNS is. Om dit mogelijk te maken dient de reverse DNS gedelegeerd te worden aan de houder van de IPv6-adressen. Hiermee is de houder van de adressen verantwoordelijk voor de invulling van de reverse DNS.

Bij de aanvraag van IPv6-adressen bij Logius dienen dus wanneer mogelijk minimaal twee nameservers opgegeven te worden op het IPv6-aanvraagformulier. In dat geval kan Logius de reverse DNS naar deze nameservers delegeren zodra deze nameservers geconfigureerd zijn om antwoorden te geven voor de reverse mapping van de betreffende adresreeks. Het IPv6-aanvraagformulier kan ook gebruikt worden om op een later moment delegatie van de reverse DNS of een wijziging hierin aan te vragen.

Het is ook mogelijk voor organisaties die hun eigen maintainer-object in de RIPE database beheren om de betreffende maintainer te autoriseren domain-objecten voor de reverse DNS mapping aan te maken zodat de betreffende organisatie dit zelf kan doen.

8.7. Contactgegevens Logius Servicecentrum

Het Logius Servicecentrum is per email bereikbaar op servicecentrum@logius.nl en op werkdagen van 8:00 tot 17:00 per telefoon op 0900 555 4555 (10 cent per minuut). Zie www.logius.nl voor verdere contactinformatie.

Het formulier voor het aanvragen van IPv6-adresruimte bij Logius en voor het doorgeven van wijzigingen is beschikbaar op
www.logius.nl/diensten/ipv6/

9. Appendix: achtergrond IPv6

Alle communicatie over het internet vindt plaats in de vorm van pakketten die ingedeeld zijn volgens het Internet Protocol (IP). Het eerste deel van ieder pakket bevat besturingsinformatie volgens een vaste indeling. Het belangrijkste deel van die besturingsinformatie wordt gevormd door het adres van het systeem dat het pakket verstuurd heeft (het afzendadres of source address) en het adres van het systeem waarvoor het pakket bedoeld is (het bestemmingsadres of destination address).

9.1. IPv4 en IPv6

Volgens de oorspronkelijke specificatie van het Internet Protocol zijn deze adressen 32 bits lang, waarmee maximaal ca. 4 miljard (2^{32}) adressen uitgegeven kunnen worden. Op dit moment zijn nagenoeg al deze adressen uitgegeven en is het zeer moeilijk tot onmogelijk om nog aan nieuwe IP-adressen te komen.

Om toekomstige groei van het internet mogelijk te maken is een nieuwe versie van IP gedefinieerd die adressen van 128 bits gebruikt. Hiermee zijn 2^{128} adressen mogelijk, ofwel 340.282.366.920.938.463.463.374.607.431.768.211.456.

De oorspronkelijke versie van IP staat bekend als Internet Protocol versie 4 (IPv4) en de nieuwe als Internet Protocol versie 6 (IPv6). Om via IPv4 te communiceren dienen zowel de zender als de ontvanger over een IPv4-adres te beschikken en alle tussenliggende routers en firewalls moeten IPv4 ondersteunen. Om via IPv6 te communiceren dienen zowel de zender als de ontvanger over een IPv6-adres te beschikken en moeten alle tussenliggende routers en firewalls IPv6 te ondersteunen.

Er zijn op dit moment nog veel systemen die alleen over IPv4 beschikken. Systemen die over IPv6 beschikken hebben over het algemeen ook nog de beschikking over IPv4 en zijn "dual stack" waardoor ze zowel over IPv4 als IPv6 kunnen communiceren. In de toekomst zullen steeds meer systemen alleen over IPv6 beschikken. Een IPv6-only systeem kan dan alleen met IPv4 systemen communiceren via een gateway of proxy die vertaalt tussen IPv4 en IPv6.

9.2. Uitgifte van IP-adressen

In Europa is het RIPE NCC (Réseaux IP Européens Network Coordination Centre) in Amsterdam verantwoordelijk voor de uitgifte van IPv4- en IPv6-adressen. Het RIPE NCC is één van de vijf Regional Internet Registries (RIRs). Het RIPE NCC geeft adressen uit aan Local Internet Registries (LIRs). In principe kan iedere organisatie LIR worden, maar de meeste LIRs zijn internetproviders die op hun beurt adressen uitgeven aan hun klanten.

IP-adressen worden uitgegeven in de vorm van een prefix. Een prefix is een reeks bits die de linkerkant van een IP-adresreeks identificeert. Bijvoorbeeld, bij de prefix 172.16.0.0/16 of 172.16/16 zijn de linker 16

bits gegeven. De overige 16 bits maken 2^{16} = 65.536 adressen mogelijk, ofwel de adresreeks 172.16.0.0 tot en met 172.16.255.255.

De notatie van IPv6-adressen is iets anders dan IPv4-adressen. Bij IPv4 worden de 32 bits gesplitst in vier groepen van acht bits en iedere groep van acht bits wordt als een normaal decimaal getal tussen 0 en 255 opgeschreven, met punten tussen de vier getallen.

Bij IPv6 worden de 128 bits gesplitst in acht groepen van 16 bits en wordt iedere groep opgeschreven als een hexadecimaal getal van 0 tot en met FFFF. Iedere hexadecimale cijfer/letter staat voor vier bits ofwel een getal tussen de 0 en 15:

Hexadecimaal	Decimaal	Bits (binair)
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
A	10	1010
B	11	1011
C	12	1100
D	13	1101
E	14	1110
F	15	1111

Tussen de acht hexadecimale getallen staan dubbele punten. Verder is het mogelijk om één reeks nullen weg te laten, bijvoorbeeld 2001:4f8:0:2:0:0:0:69 wordt 2001:4f8:0:2::69 en 2a04:9a00:0:0:0:0:0:0 wordt 2a04:9a00::. Maar 2001:4f8:0:2:0:0:0:69 of zelfs 2001:04f8:0000:0002:0000:0000:0000:0069 zijn ook acceptabele variaties. Er wordt geen verschil gemaakt tussen hoofd- en kleine letters (case insensitive).

Bij IPv6 is het gebruikelijk om aan ieder subnet (zoals een Ethernet, een Wi-Fi-netwerk of een verbinding tussen twee routers) een /64 toe te kennen. Over het algemeen blijft de grootte van een subnet beperkt tot één gebouw of een deel van een gebouw en er worden ook meerdere subnetten per locatie gebruikt om verkeersstromen te scheiden om beveiligingsredenen.

LIRs krijgen normaliter een /29 prefix van het RIPE NCC, tenzij ze aannemelijk kunnen maken dat ze meer nodig hebben. ISPs kunnen in hoge mate zelf bepalen hoeveel adressen ze uitgeven aan hun klanten, over het algemeen varieert dit van een /64 - /56 voor consumenten of mobiele gebruikers tot een /48 voor zakelijke gebruikers en organisaties. Bij een /64 heeft de eindgebruiker voldoende adressen voor één subnet. Bij een /56 zijn 256 subnetten ($2^{64-56} = 2^8$) en bij een /48 zijn er 16 bits

(48 - 64) beschikbaar om subnetten te nummeren en zijn er 65.536 subnetten mogelijk. Uit een /29 kan een LIR 34 miljard /64s uitgeven, 134 miljoen /56s, een half miljoen /48s of een combinatie.

Het is ook mogelijk om bij het RIPE NCC zogenaamde "provider independent" (PI) adresruimte aan te vragen. Dit wordt veel gedaan door organisaties die onafhankelijk van hun ISP willen zijn en zo met behoud van hun IP-adressen van ISP kunnen wisselen en/of via meerdere ISPs tegelijk met het internet verbonden willen zijn (multihoming). PI-prefixen zijn /48 of korter (lager getal achter de schuine streep, groter adresblok). /48 is de langste prefix (kleinste blok) wat over het algemeen onafhankelijk over het internet gerouteerd kan worden. Voor multihoming is dus minimaal een /48 vereist. Er is echter geen garantie dat een onafhankelijke /48 vanaf het hele internet bereikbaar zal zijn.

De volgende tabel laat de structuur van een IPv6-adres zien bij een LIR die een /29 prefix van het RIPE NCC heeft en /48s aan klanten uitdeelt.

Bits	**Doel**
/0 - /3 (3)	Bits die global unicast adressen identificeren
/3 - /29 (26)	Bits die de LIR identificeren
/29 - /48 (19)	Bits die de klant van LIR/ISP identificeren
/48 - /64 (16)	Bits die het subnet identificeren
/64 - /128 (64)	Bits die het individueel systeem identificeren