VNG Realisatie

HANDLEIDING OPSTELLEN IPV6-NUMMERPLAN

Versie 1.4, 9 juli 2018

COLOFON

Bij de samenstelling van deze handleiding is zijn tekst en tekeningen hergebruik uit het document “Een IPv6-numerplan opstellen”[1] dat door Surfnet is ontwikkeld en gepubliceerd onder de Creative Commons Naamsvermelding 3.0 Nederland licentie.

Bijzondere dank is verschuldigd aan Logius en meer specifiek aan Iljitsch van Beijnum, die heeft bijgedragen om deze handleiding uit te werken en aan te passen voor gebruik door gemeenten en gemeentelijke samenwerkingsverbanden.

Projectgroep IPv6 VNG Realisatie,

Den Haag, 9 juli 2018

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

Inhoud

1. INLEIDING

De IPv4-adressen raken op en steeds meer organisaties zien de noodzaak van het migreren naar IPv6. Migreren naar IPv6 omvat meer dan de huidige IPv4 adressen omzetten naar een nieuw formaat. Vanwege de grotere mogelijkheden die IPv6 biedt, is het raadzaam om voordat alle adressen worden bepaald, na te denken over hoe de IPv6-adressen het beste ingedeeld kunnen worden. Dit document beschrijft hoe dat kan worden gerealiseerd.

De aanbeveling van VNG Realisatie aan gemeenten en samenwerkingsverbanden is eerst te starten met het zekerstellen van de externe bereikbaarheid via IPv6 (websites en mailservers). Vervolgens kan in een later stadium worden verdergegaan met de 'interne uitrol' van IPv6. Daarbij is de aanbeveling om landelijk te werken met een vaste hoofdindeling, waarbij bijvoorbeeld systemen die vertrouwelijke gegevens verwerken een herkenbare adresrange krijgen. Binnen de vaste hoofdindeling hebben gemeenten en samenwerkingsverbanden voldoende ruimte (gelet op het grote aantal beschikbare adressen) om eigen detailindelingen te maken.

Op grond van het voorgaande is een IPv6-nummerplan nodig. Wanneer u een nummerplan gaat maken op basis van IPv6, dan ziet dat er heel anders uit dan een IPv4-nummerplan. Bij het opstellen van een IPv4-nummerplan zijn de keuzemogelijkheden voor verschillende indelingen beperkt. De reden daarvoor is dat een organisatie doorgaans relatief weinig vaste IPv4-adressen ter beschikking krijgt. De IPv4-adresindeling is daarom meestal gebaseerd op efficiënt adresgebruik.

De IPv6-adressenrange, die u als gemeente of samenwerkingsverband ontvangt, is standaard 2^{80} adressen (een /48 prefix). Dit zijn er zoveel, dat er vrijwel geen beperkingen zijn bij het indelen van de adressen binnen uw organisatie. Toch is het zinvol om een IPv6-nummerplan op te stellen: een systeem waarmee u de IPv6-adressen toekent aan locaties en/of gebruikerstypen.

Voor de Nederlandse overheid bestaat een overkoepelend IPv6-nummerplan waarbinnen alle overheidsorganisaties (overheids) IPv6-adressen krijgen. Gemeenten en samenwerkingsverbanden krijgen meerdere opeenvolgende /48-blokken. De verschillende /48-blokken zijn bedoeld om verschillende typen systemen met verschillende beveiligingskenmerken IPv6-adressen te geven.

Door een goed IPv6-nummerplan op te zetten, worden IPv6-adresreeksen op een zinvolle en structurele manier gegroepeerd. Dit heeft onder andere de volgende voordelen:

- Beveiligingsbeleid is gemakkelijker toe te passen, zoals bij het configureren van accesslists en firewalls
- Adressen zijn goed leesbaar: uit het adres is af te leiden in welke gebruiksgroep of locatie het adres in gebruik is
- Een goed nummerplan is schaalbaar: het biedt ruimte voor uitbreidingen in bijvoorbeeld locaties of gebruiksgroepen
- Door een goed IPv6-nummerplan kan netwerkbeheer efficiënter worden uitgevoerd

Bedenk wel dat een efficiënt IPv6-nummerplan grote hoeveelheden IPv6-adressen 'minder efficiënt' gebruikt. In nagenoeg alle gevallen is dat een juiste afweging: schijnbare

inefficiency op lokaal niveau leidt tot meer efficiency elders, bijvoorbeeld, door te voorkomen dat routingtabellen in routers te snel groeien. De adressen zijn er; u kunt ze net zo goed gebruiken.

In deze handleiding leest u hoe u op een gestructureerde manier een goed IPv6-nummerplan kunt opzetten. Hierbij zijn een aantal keuzes van belang, die u stap voor stap doorloopt. Door deze keuzes weloverwogen te maken, zorgt u ervoor dat het nummerplan goed aansluit bij de wensen en eisen van uw organisatie. U krijgt daarbij aanbevelingen voor de te maken keuzes.

1.1 VOOR WIE IS DIT DOCUMENT BEDOELD?

Deze handleiding is bedoeld voor netwerkarchitecten en netwerkbeheerders die IPv6 binnen hun organisatie gaan uitrollen. Er wordt verondersteld dat u ervaring hebt met het inrichten van netwerken op basis van IPv4.

1.2 ONDERSTEUNING VANUIT VNG REALISATIE EN LOGIUS

De implementatie van IPv6 adressen bij gemeenten en gemeentelijke samenwerkings-verbanden is een ingrijpende operatie. Om deze operatie in goede banen te laten lopen is besloten om vanaf het najaar van 2016 een aparte projectorganisatie binnen VNG Realisatie in het leven te roepen, die in nauwe afstemming met de specialisten van Logius proces- en inhoudelijke ondersteuning kan leveren aan gemeenten en samenwerkingsverbanden die daar behoefte aan hebben. Nadere informatie kunt u vinden op de speciale webpagina's van VNG Realisatie: https://da2020.nl/ipv6 .

De toewijzing van IPv6-adressen aan gemeenten en samenwerkingsverbanden van gemeenten vindt plaats door Logius in samenwerking met VNG Realisatie. Zie ook https://www.logius.nl/diensten/ipv6/ .

2. OPBOUW VAN IPV6-ADRESSEN

Voordat we ingaan op IPv6 adressen eerst nog een terugblik naar IPv4. Een IPv4-adres is 32 bits lang en bestaat uit 4 groepen van 8 bits. Die vier groepen van acht bits worden opgeschreven als vier nummers van 0 tot 255 met punten ertussen. Met IPv4 zijn 2^{32} ofwel 4.294.967.296 adressen mogelijk.

IPv6-adressen zijn 128 bits lang, vier keer zo lang als IPv4-adressen. Dit betekent dat ze een heel verschillende notatie hebben, en het grote aantal bits maakt het mogelijk om een IPv6-adres meer interne structuur te geven.

Bij IPv6 zijn er theoretisch 2^{128} adressen beschikbaar, heel veel meer dus dan er met IPv4 beschikbaar zijn. Om een voorstelling te maken: 2^{128} of 340.282.366.920.938.463.463.374.607.431.768.211.456 of 340 miljard miljard miljard miljard is ongeveer gelijk aan het aantal zandkorrels op aarde.

2.1 ADRESNOTATIE

Bij een IPv6-adres (128 bits), kan elk bit de waarde 0 of 1 hebben. Omdat een adres bestaande uit 128 enen en nullen voor mensen niet leesbaar is, wordt het op een handigere manier genoteerd. Hierbij wordt gebruik gemaakt van het hexadecimale stelsel omdat dit goed leesbaar en tegelijkertijd nauw verband houdt met de binaire notatie. Bij hexadecimale notatie worden naast de cijfers 0 – 9 ook de letters A – F gebruikt.

De notatie van IPv6-adressen bestaat uit 8 blokken van telkens 4 tekens, gescheiden voor een ‘:’.Elk cijfer in het hexadecimale stelsel komt overeen met 4 bits; een IPv6-adres van 128 bits bestaat dus uit (128 / 4 =) 32 hexadecimale cijfers. Dit wordt op de volgende wijze genoteerd:

2001:0db8:0000:0000:0000:0000:0000:0001

Omdat het schijven van al deze nullen niet handig is, mogen deze volgens vastgestelde regels weggelaten worden. Van elk groepje cijfers tussen twee dubbele punten mogen de voorloopnullen weggelaten worden. We krijgen dan:

2001:db8:0:0:0:0:0:1

Vervolgens mag één keer (en niet meer) een reeks bestaande uit nullen en dubbele punten afgekort worden tot twee dubbele punten. We krijgen dan:

2001:db8::1

De exacte regels voor het noteren van IPv6-adressen zijn vastgelegd in RFC 5952[2].

2.2 GROEPERING VAN ADRESSEN (PREFIXEN)

Voor het groeperen van IPv6-adressen wordt gebruik gemaakt van de binaire waarde van het adres. De groepering gebeurt met een zogenaamde prefix, vergelijkbaar met het netnummer voor telefoonnummers (bijvoorbeeld, 020 is de "prefix" voor Amsterdam). Dit zijn alle adressen die met dezelfde bits beginnen. Het aantal bits dat hetzelfde is, wordt achter het adres geschreven, gescheiden door een schuine streep (slash).

De prefix

2001:db8::/ 32

bevat dus alle adressen van

2001:0db8:0000:0000:0000:0000:0000:0000

tot en met

2001:0db8:ffff:ffff:ffff:ffff:ffff:ffff

Zoals hierboven te zien is blijven de eerste 32 bits, oftewel de eerste 8 hexadecimale cijfers, gelijk. De prefix

2001:db8:1234::/ 64

bevat alle adressen van

2001:0db8:1234:0000:0000:0000:0000:0000

tot en met

2001:0db8:1234:0000:ffff:ffff:ffff:ffff

(Laat u niet afleiden door de ontbrekende nullen in 2001:db8:1234::/64 in plaats van 2001:db8:1234:0000::/64.)

Prefixen die een veelvoud zijn van vier zijn het makkelijkst in het gebruik, dus deze komen het meest voor. Bijvoorbeeld /32, /48, /52, /56, /60 en /64. Als een prefix een andere grens heeft "hakt" deze door een hexadecimaal cijfer heen, waardoor de adresreeks moeilijker te ontcijferen is (zie kader).

[2] http://tools.ietf.org/html/rfc5952#page-10

Prefix geen veelvoud van vier

Als de prefixlengte geen mooi veelvoud van vier is, ligt de binaire scheiding midden in een hexadecimaal cijfer. Dit zorgt ervoor dat alle hexadecimale cijfers die met dezelfde bits beginnen bij de prefix horen. De prefix

2001:db8::/ 61

bevat daardoor alle adressen van

2001:0db8:0000:0000:0000:0000:0000:0000

tot en met

2001:0db8:0000:0007:ffff:ffff:ffff:ffff

omdat de hexadecimale cijfers 0 tot en met 7 allemaal met de binaire waarde 0 beginnen. Zo bevat de prefix

2001:db8:0:8::/ 61

alle adressen van

2001:0db8:0000:0008:0000:0000:0000:0000

tot en met

2001:0db8:0000:000f:ffff:ffff:ffff:ffff

omdat de hexadecimale cijfers 8 tot en met F allemaal met de binaire waarde 1 beginnen.

Met IPv4 is het theoretisch mogelijk om een niet-aansluitend subnetmasker te hebben. Bijvoorbeeld, bij het subnetmasker 255.255.252.255 vallen de adressen 192.0.2.3 en 192.0.3.3 binnen hetzelfde subnet, maar 192.0.2.3 en 192.0.2.4 niet. Maar niet-aansluitende subnetmaskers hebben geen corresponderende prefixlengte. Gezien het feit dat IPv6-subnetten gedefinieerd worden door middel van een prefixlengte is het niet mogelijk niet-aansluitende subnetten te gebruiken met IPv6.

2.1. /64 subnetten

IPv6-adressen hebben geen vaste structuur zoals het klasse A/B/C-systeem dat oorspronkelijk gebruikt werd met IPv4. Desondanks worden IPv6-subnets geacht /64 prefixen te zijn. Andere subnetgroottes zijn mogelijk, maar kunnen mechanismen zoals stateless address autoconfiguration in de weg zitten (zie paragraaf 5.1). Dus heel kleine subnetten, zoals point-to-pointverbindingen tussen twee systemen, gebruiken een even groot blok IPv6-adressen als heel grote subnetten, zoals een groot Ethernet met verschillende Ethernet-switches.

2.2. Toewijzing adresblokken

De originele aanbeveling voor het toewijzen van IPv6-adresruimte aan eindgebruikers was als volgt:

- **/48** (65 536 subnetten) als standaard, behalve bij zeer grote gebruikers
- **/64** (een enkel subnet) wanneer het duidelijk is dat niet meer dan één subnet nodig is
- **/128** (een enkel adres) wanneer het absoluut zeker is dat maar één systeem aangesloten wordt

Echter, RFC 6177[3] (ook bekend als Best Current Practice 157) verandert dit en adviseert het toewijzen van een adresblokgrootte die aansluit bij de behoeften van de gebruiker. Ook adviseert de RFC om geen losse adressen uit te geven. Bijvoorbeeld: een /48 is veel meer dan een thuisgebruiker nodig heeft, maar een /64 laat maar één subnet toe, wat beperkingen met zich meebrengt, zo niet nu dan in de toekomst. Een /56 of /60 is dus een geschiktere keus voor consumenten.

Daarom is het om naar boven af te ronden, want een tweede adresblok toevoegen of migreren naar een nieuw, groter blok brengt kosten met zich mee. Dit is met name het geval bij middelgrote en grote organisaties die in eerste instantie een /56 toegewezen kregen. Bij een /56 is het netwerk al relatief groot op het moment dat er meer adresruimte nodig is, met als gevolg dat de impact van aanpassingen aanzienlijk is. Als in eerste instantie een /60 toegewezen was, dan zou het netwerk hier veel eerder uitgegroeid zijn, op een moment dat het netwerk nog kleiner was en wijzigingen nog een stuk makkelijker gemaakt konden worden.

Dit betekent dat een /48 toegewezen moet worden wanneer er ook maar enige twijfel is of een /56 voldoende is op lange termijn. ISPs kunnen grotendeels naar eigen inzicht de grootte van adresblokken die ze uitgeven bepalen binnen het maximum van een /48–zelfs in het geval van thuisgebruikers.

ISPs die LIR zijn (Local Internet Registry, ook wel "RIPE lid" in Europa) krijgen minimaal een /29, maar grote ISPs kunnen veel grotere adresblokken / kortere prefixen krijgen, zodat ze een aparte sub-prefix per regio of land waar ze actief zijn kunnen gebruiken.

[3] RFCs zijn beschikbaar op http://tools.ietf.org/html/

Gebaseerd op het bovenstaande staan de eerste 48 bits van uw IPv6-nummerplan vast. In dit document gebruiken we 2001:db8:1234::/48 als voorbeeld. Dat betekent dat u de /64 prefixen

2001:db8:1234:0000::/ 64

tot en met

2001:db8:1234:ffff::/ 64

kan gebruiken binnen uw netwerk–16 bits in totaal.

Voor uw eigen nummerplan dient u de nummers in de voorbeelden te vervangen door de u toegewezen prefix.

2.3. Weergave van onderverdelingen

Gezien het feit dat de eerste 48 bits toegewezen binnen het overheidsbrede IPv6-nummerplankader en de laatste 64 bits gebruikt worden binnen elk subnet, gaat een IPv6-nummerplan over de overblijvende 16 bits die beschikbaar zijn om subnetten te nummeren. In deze handleiding verdelen we die 16 beschikbare bits onder in groepen. We onderscheiden de volgende groepen:

- B: bit is nog beschikbaar voor onderverdeling
- L: bit wordt gebruikt voor onderverdeling naar locatie
- T: bit wordt gebruikt voor onderverdeling naar gebruikstype

De toegewezen bits geven we als volgt weer. De plaatsing van de letters B, L en T is hierbij willekeurig en dient uitsluitend ter illustratie:

2001:db8:1234:	L	L	L	L	T	T	T	T	B	B	B	B	B	B	B	B	::/ 64

Elk vakje representeert een bit. Vier vakjes samen representeren een nibble (vier bits) en dus één hexadecimaal cijfer in het IPv6-adres, wat voor bovenstaand voorbeeld de volgende adresstructuur oplevert:

2001:db8:1234:LTBB::/ 64

Bits 1-4 worden in dit voorbeeld dus gebruikt voor een onderverdeling naar locatie, bits 5-8 voor een onderverdeling naar gebruikstype en bits 9-16 zijn nog beschikbaar voor nadere invulling.

3. BEVEILIGINGSCATEGORIEËN

Onderdeel van het Nederlandse overheidsbrede IPv6-nummerplankader is dat overheden een uniforme indeling van systemen binnen beveiligingscategorieën toepassen. Er zijn vier beveiligingscategorieën gedefinieerd:

- **Van/naar het internet en frontends.** Deze categorie bevat servers die met het publieke internet communiceren en ook computers, tablets en smartphones die niet door een overheidsorganisatie beheerd worden. Dit omvat zowel apparatuur van gasten als ”bring your own device” (BYOD) van medewerkers.
- **Campus en transitzones.** Deze categorie bevat de (vertrouwde) kantooromgeving, waaronder computers, tablets en smartphones die door een overheidsorganisatie beheerd worden en andere kantoorapparatuur zoals printers/scanners. Daarnaast bevat deze categorie transitzones (DMZ) die communicatie tussen frontends en backends faciliteert.
- **Datacenter en backends.** Deze categorie bevat de servers waar (overheids-) interne applicaties op draaien en de backends van publiek bereikbare diensten/applicaties. Adressen binnen deze categorie zijn niet bereikbaar vanaf het internet. Adressen binnen deze categorie worden wel gebruikt voor communicatie tussen overheidsorganisaties over besloten netwerken zoals Diginetwerk.
- Als laatste is er een **categorie zonder voorgedefinieerde functie**. Organisaties kunnen hier naar eigen inzicht zaken in onderbrengen die niet goed in de overige categorieën passen.

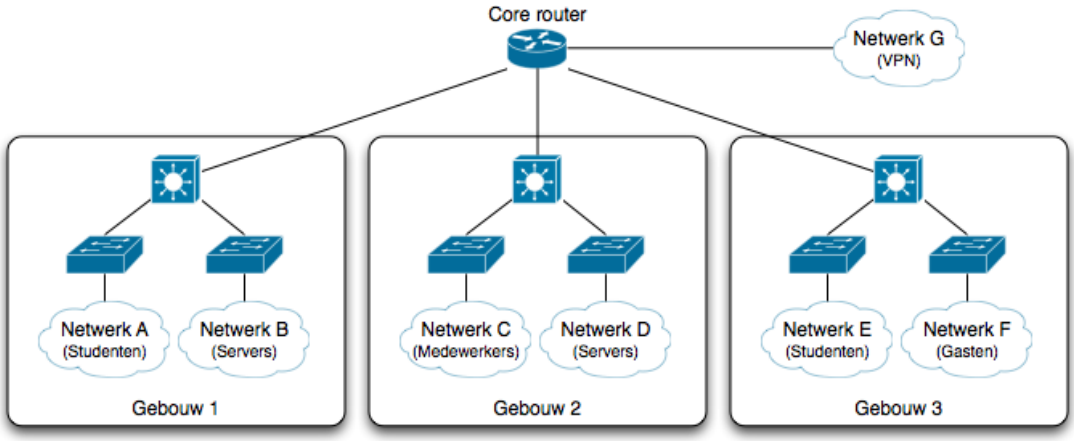
Bij het maken van een nummerplan voor een gemeente is het belangrijk dat alle systemen die IPv6-adressen krijgen een plaats vinden in de juiste categorie. De verdere onderverdeling zal in de meeste gevallen per categorie verschillen.

In feite komt dit neer op het opstellen van drie of vier verschillende nummerplannen, één voor iedere beveiligingscategorie. Samen vormen deze het totale IPv6-nummerplan van de organisatie.

4. EEN NUMMERPLAN OPSTELLEN

Bij het opstellen van een nummerplan bepaalt u volgens welke structuur de beschikbare adressen verdeeld worden over de netwerken binnen uw organisatie. Er is een aantal handige manieren om deze onderverdeling te maken.

In de rest van dit hoofdstuk worden de mogelijke onderverdelingen bekeken. Hierbij maken we gebruik van het volgende voorbeeldnetwerk:



4.1 BASISSTRUCTUUR VAN HET NUMMERPLAN

Met IPv6 hebben we de beschikking over zo veel adressen dat er één of meerdere onderverdelingen gemaakt kunnen worden. Zo kunnen we bijvoorbeeld de adressen onderverdelen per gebruikstype of per locatie. We kunnen ook combinaties maken. Zo kunnen de adressen bijvoorbeeld eerst op gebruikstype en daarna op locatie worden onderverdeeld. Nadat de onderverdeling gemaakt is kunnen er nog bits beschikbaar blijven voor verdere invulling.

Als we kijken naar de voorbeeld uit sectie 2.4:

2001:db8:1234:	L	L	L	L	T	T	T	T	B	B	B	B	B	B	B	B	::/ 64

In dit voorbeeld zijn er 4 bits gebruikt voor de onderverdeling per locatie (L) en 4 bits voor de onderverdeling per gebruikstype (T). Er blijven dan nog 8 bits beschikbaar (B). Met dit nummerplan kunnen 16 locaties genummerd worden, waarbij elke locatie de beschikking heeft over 16 gebruikstypen. Met de overgebleven 8 bits kan elk van deze locaties per gebruikstype 256 subnetten aanmaken.

4.1.1 IPv6, NAT en firewalls

Bij IPv4 wordt Network Address Translation (NAT) zeer algemeen gebruikt om meerdere werkstations toegang tot het publieke internet te geven middels een enkel IPv4-adres. IPv6 beschikt over voldoende adresruimte, waardoor het gebruik van NAT voor dit doel niet langer nodig is.

Een bijeffect van NAT is dat het (grotendeels) voorkomt dat ongevraagde pakketten vanaf het publieke internet werkstations achter het NAT-apparaat bereiken. Dit betekent dat protocollen waarbij twee werkstations die zich achter NATs bevinden rechtstreeks communiceren (peer-to-peer protocollen) extra logica aan boord moeten hebben om communicatie door NAT heen op te kunnen zetten. Maar IPv6 peer-to-peerapplicaties, en ook een aantal applicaties die niet op het eerste gezicht peer-to-peer zijn, zoals FTP, zijn wellicht niet voorzien van NAT-herkenning, of zetten deze logica niet in wanneer ze over IPv6 communiceren. Het gevolg is dat IPv6-netwerken die NAT inzetten waarschijnlijk meer NAT-gerelateerde problemen zullen zien dan een vergelijkbaar IPv4-netwerk. Er is ook geen RFC die IPv6 NAT beschrijft, alleen IPv6 IPv6-to-IPv6 Network Prefix Translation (RFC 6296, met status "experimenteel").

Om te voorkomen dat ongewenste pakketten die binnenkomen vanaf het publieke internet interne systemen bereiken kan het nuttig zijn een "stateful" firewall in te zetten. Deze correleert inkomende pakketten aan communicatiesessies die door interne systemen opgezet zijn. Zie RFC 4864 voor meer informatie.

4.2 ROUTER VS FIREWALL: LOCATIE OF GEBRUIKSTYPE EERST

Om te beginnen moeten we kiezen hoe de adressen als eerste onderverdeeld gaan worden. Als eerste onderverdeling is het aan te raden om te kiezen voor de locatie of de gebruikstype (bijvoorbeeld medewerkers, servers, switches, routers, openbaar, enzovoort). Deze varianten worden verder uitgewerkt.

4.2.1 Locatie eerst

Bij een onderverdeling naar locatie krijgt bijvoorbeeld elk gebouw of elke afdeling een eigen deel van de adressen toegewezen. Hierbij ligt de nadruk op de optimalisatie van de routeringstabellen. Alle netwerken van één locatie kunnen geaggregeerd worden tot één route in de routeringstabel, waardoor deze compact blijft.

Vrijwel alle moderne routers kunnen omgaan met zeer grote routeringstabellen zonder dat dit ten koste van de snelheid gaat, er is dus over het algemeen geen reden om te kiezen voor locatie eerst om routeringstabellen klein te houden.

4.2.2 Gebruikstype eerst

Bij een onderverdeling naar gebruikstype is bovenstaande optimalisatie van de routering niet mogelijk, aangezien de gebruikstypen verdeeld zijn over de locaties

Eerst onderverdelen naar gebruikstype maakt het wel veel eenvoudiger om het beveiligingsbeleid in te richten. De meeste firewall policies zijn gericht op het soort gebruik en niet op de locatie waar het netwerk zich bevindt. Per gebruikstype is daardoor vaak maar één policy nodig in de firewalls.

De binnen de vastgestelde indeling in beveiligingscategorieën in het kader van het overheidsbrede IPv6-nummerplan maakt al een scheiding tussen vier overkoepelende beveiligingscategorieën. Het zal echter vaak gewenst zijn binnen iedere categorie een fijnmaziger onderscheid te maken. Bijvoorbeeld, zowel publieke Wi-Fi als webservers worden geplaatst in de internet/frontend-categorie, maar de firewallregels voor deze verschillende subcategorieën zullen heel verschillend zijn.

4.2.3 Advies

Op basis van het bovenstaande, raden wij aan om de adressen onder te verdelen op basis van gebruikstype, aangezien dit de meeste aansluiting kan bieden bij bestaande policies en procedures. Mogelijke redenen om toch onder te verdelen per locatie, zijn:

- Er zijn locaties die hun eigen nummerplan gaan maken
- De routers kunnen zonder aggregatie het aantal routes niet aan

4.3 BENODIGDE ADRESRUIMTE BEPALEN VOOR DE GEKOZEN ONDERVERDELING

Nu moeten we bepalen welk deel van de 16 bits beschikbare adresruimte (zie sectie 2.4) nodig is voor de gekozen onderverdeling. Eén bit kan twee groepen (2^1) bevatten, 2 bits 4 groepen (2^2), enzovoort. We gaan als volgt te werk om het aantal groepen te bepalen:

1. We bepalen het aantal locaties of gebruikstypen binnen uw organisatie. Tel voor elke locatie of gebruikstype 1 groep.
2. We verhogen dit aantal met 1 groep, ten behoeve van de backbone en andere infrastructuur.
3. Bij een onderverdeling naar locatie nemen we 1 groep extra voor alle netwerken die niet gebonden zijn aan een bepaalde locatie. Dit zijn bijvoorbeeld netwerken voor VPN's en tunnels.
4. We nemen (minimaal) 1 of 2 groepen om rekening te houden met toekomstige uitbreidingen.

Om een handig bruikbare onderverdeling te maken, moet het aantal blokken waarin we de adresruimte onderverdelen een macht van 2 zijn. We ronden daarom het opgetelde aantal bits uit stap 1 tot en met 4 op naar boven af, naar de eerstvolgende macht van 2. Zie de tabel voor het aantal bits dat nodig is voor elk gewenst aantal groepen. De uitkomst is het aantal groepen dat gebruikt wordt voor de eerste onderverdeling, naar locatie of gebruikstype. Deze werkwijze wordt uitgewerkt in een aantal voorbeelden; uitgebreidere voorbeelden vindt u in de appendix.

Bits	Locaties of gebruikstypes
1	2
2	3 of 4
3	5 - 8
4	9 - 16

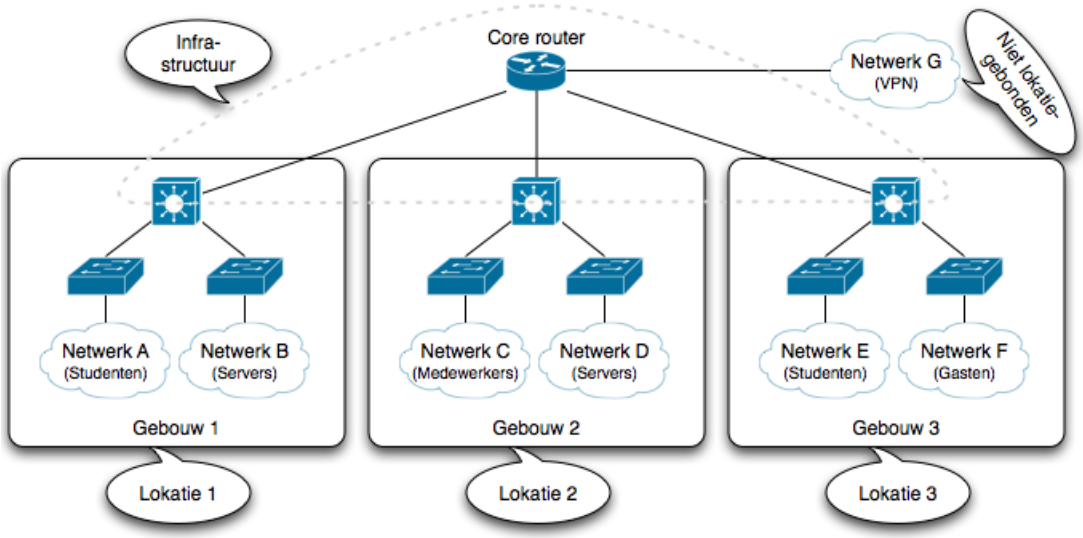
Bits	Locaties of gebruikstypes
5	17 - 32
6	33 - 64
7	65 - 128
8	129 - 256
9	257 - 512
10	513 - 1024
11	1025 - 2048
12	2049 - 4096

Voorbeeld 1: naar locatie

In dit rekenvoorbeeld maken we een onderverdeling naar locatie. Het aantal benodigde groepen wordt als volgt bepaald:

- Aantal locaties: 3 groepen
- Backbone en andere infrastructuur: 1 groep
- Niet-locatiegebonden netwerken: 1 groep
- Toekomstige locaties: 2 groepen
- Totaal: 7 groepen

In het voorbeeldnetwerk krijgen we dan de volgende verdeling:



Na afronding naar de eerstvolgende macht van 2 komen we op een onderverdeling van 8 groepen. Om deze groepen in het IPv6-adres op te nemen, hebben we 3 bits (L) nodig (2^3 = 8; zie ook het overzicht op de vorige pagina). We komen tot de volgende verdeling van de bits:

2001:db8:1234:	L	L	L	B	B	B	B	B	B	B	B	B	B	B	B	B	::/ 64

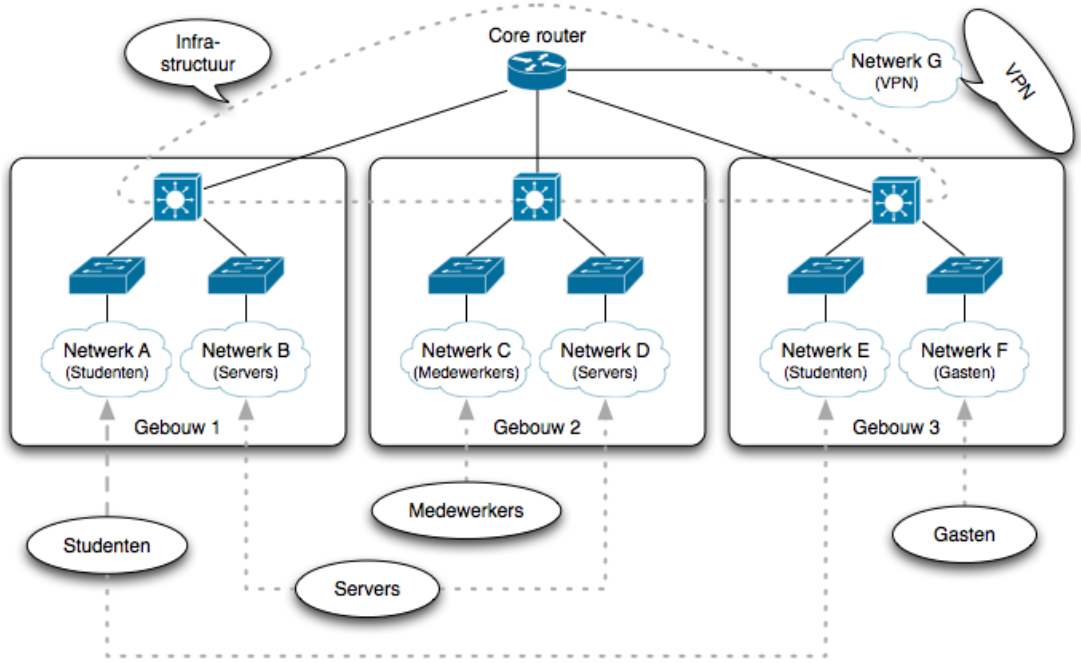
Er zijn nu nog 13 bits beschikbaar (B).

Voorbeeld 2: naar gebruikstype

In dit rekenvoorbeeld maken we een onderverdeling naar gebruikstype. Het aantal benodigde groepen wordt als volgt bepaald:

- Aantal gebruikstypen (medewerkers, gasten, servers en VPNs): 4 groepen
- Backbone en andere infrastructuur: 1 groep
- Toekomstige gebruikstypen: 4 groepen
- Totaal: 9 groepen

In het voorbeeldnetwerk krijgen we dan de volgende verdeling:



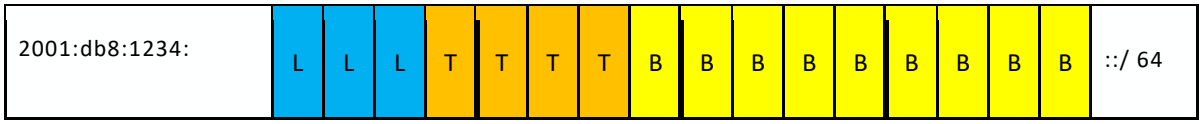
Na afronding naar de eerstvolgende macht van 2 komen we op een onderverdeling van 16 groepen. Om deze groepen in het IPv6-adres op te nemen hebben we 4 bits (T) nodig (2^4 = 16). Er zijn nu nog 12 bits beschikbaar (B):

2001:db8:1234:	T	T	T	T	B	B	B	B	B	B	B	B	B	B	B	B	::/ 64

4.4 OPTIONELE VERDERE ONDERVERDELING

De overgebleven bits kunnen gebruikt worden voor het nummeren van netwerken binnen de gekozen onderverdeling. Bij een onderverdeling op basis van locatie kunnen zo meerdere netwerken op één locatie genummerd worden, en bij een onderverdeling op basis van gebruikstype kunnen bijvoorbeeld meerdere medewerker-netwerken en meerdere server-netwerken genummerd worden.

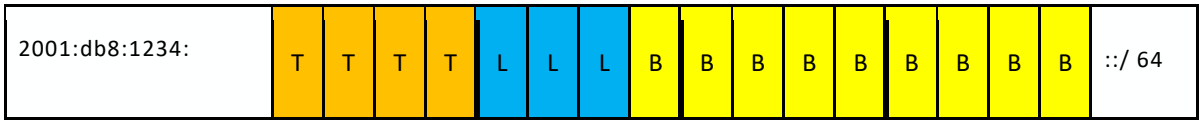
De overgebleven bits kunnen ook gebruikt worden om onderverdelingen naar locatie en gebruikstype te combineren. Als we eerst onderverdelen volgens voorbeeld 1, en een subonderverdeling maken volgens voorbeeld 2, krijgen we het volgende resultaat:



In dit nummerplan is ruimte voor 8 locaties met elk 16 gebruikstypen. Voor elke gebruikstype zijn vervolgens nog 512 (2^9 vanwege de 9 beschikbare bits) netwerken in te richten.

Door de onderverdelingen op deze manier te combineren wordt in eerste instantie onderverdeeld per locatie. Dit maakt het mogelijk om de routeringstabellen te optimaliseren, maar het helpt niet om het beveiligingsbeleid eenvoudiger in te richten. Dit komt doordat het beleid in firewalls alleen in te stellen in gerekend vanaf het begin van het adres, en in dit voorbeeld staat de locatie aan het begin en niet de gebruikstype.

Om het inrichten van het beveiligingsbeleid eenvoudiger te maken kan de combinatie ook andersom gemaakt worden door eerst onder te verdelen volgens voorbeeld 2, en de subonderverdeling te maken volgens voorbeeld 1. We krijgen dan het volgende resultaat:



In dit voorbeeld staat de gebruikstype vooraan. Hierdoor kan het beleid in firewalls eenvoudig ingesteld worden per gebruikstype. Aangezien de gebruikstype vaak relevanter is dan de locatie voor het beveiligingsbeleid raden we aan om op deze manier te werken.

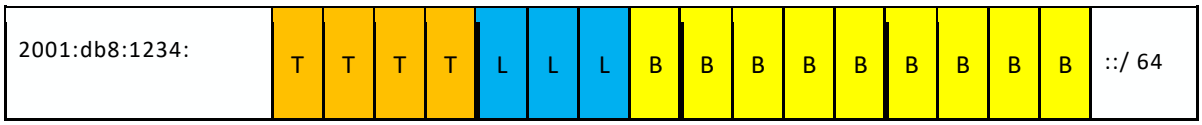
4.5 CONTROLE

We controleren of de gemaakte onderverdeling voldoet, door te kijken of er voldoende bits over zijn na de onderverdeling(en). Zijn er bijvoorbeeld (bij een onderverdeling per gebruikstype gevolgd door een onderverdeling per locatie) meerdere medewerker netwerken per locatie nodig, dan moeten er voldoende bits over zijn om deze in te richten.

In het voorbeeld uit sectie 4.5 zijn er nog 9 bits over, wat nog 512 (2^9) mogelijke waarden per gebruikstype per locatie oplevert. Dit zal meer dan voldoende zijn.

4.6 SPEELRUIMTE

Als de overgebleven bits net niet voldoende zijn, kan dit in de onderverdeling worden opgevangen. In het bovenstaande voorbeeld hebben we 4 bits genomen voor de gebruikstypen en 3 bits voor de locaties. We houden dan 9 bits over waarmee we per soort per locatie 512 (2^9) netwerken in kunnen richten.



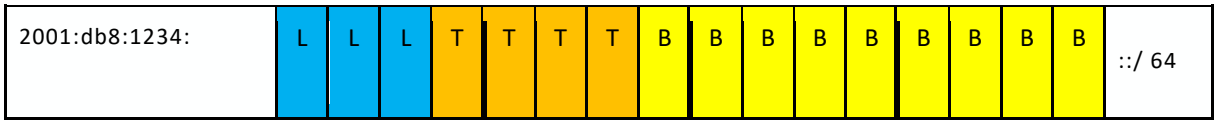
Dit zal in de meeste gevallen voldoende zijn. Maar stel dat we per locatie 2048 VPN-netwerken nodig hebben. We kunnen dan de onderverdeling aanpassen. Deze wordt dan echter lastiger leesbaar in hexadecimale notatie. We kunnen er ook voor kiezen om binnen de gebruikstypen 4 groepen te reserveren voor VPN-netwerken. Als de nummers van deze groep van 4 soorten op een binaire grens (decimaal: 0-3, 4-7, 8-11 of 12-15, hexadecimaal: 0-3, 4-7, 8-B, C-F) gekozen worden dan zijn deze nog steeds met één firewall policy te vangen.

We zouden dan bijvoorbeeld de volgende groepen krijgen:

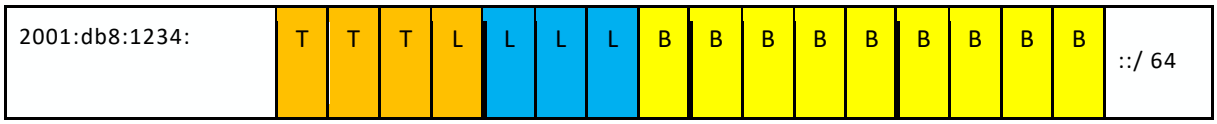
0	Backbone en andere infrastructuur
1	Servers
2	Toekomstige uitbreiding
3	Toekomstige uitbreiding
4	Medewerkers
5	Gasten
6	Toekomstige uitbreiding
7	Toekomstige uitbreiding
8	VPNs A
9	VPNs B
A	VPNs C
B	VPNs D
C	Toekomstige uitbreiding
D	Toekomstige uitbreiding
E	Toekomstige uitbreiding
F	Toekomstige uitbreiding

4.7 LEESBAARHEID

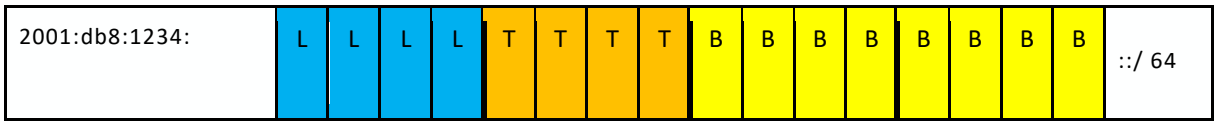
In het voorbeeld in deze sectie gebruikten we 3 bits per locatie en 4 bits per gebruikstype. Als er voldoende bits over zijn, kunnen we dit naar boven afronden om de IPv6-adressen leesbaarder te maken. Elk hexadecimaal cijfer in een IPv6-adres staat voor 4 bits. Door de onderverdeling in veelvouden van 4 bits te maken zal elke groep samenvallen met een cijfer in het IPv6-adres. Bijvoorbeeld:



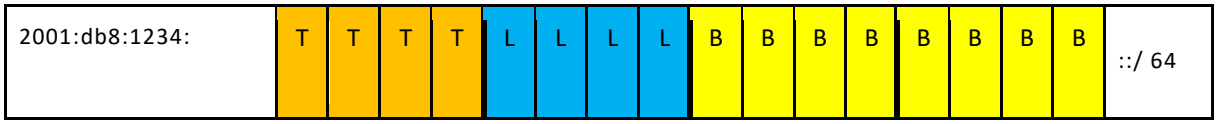
of



wordt:



of



De vier L-bits worden weergegeven als 1 hexadecimaal cijfer in het IPv6-adres. Ook de vier T-bits worden weergegeven als 1 hexadecimaal cijfer. Dit levert de volgende IPv6-adresstructuur op:

2001:db8:1234:LTBB::/ 64

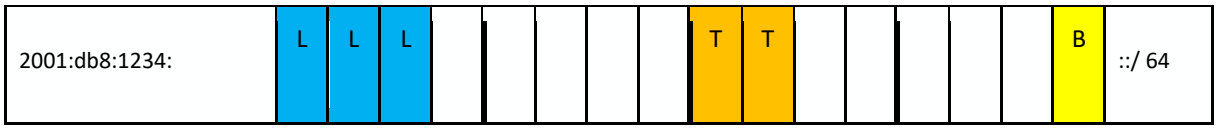
2001:db8:1234:TLBB::/ 64

De locatie en de gebruikstype zijn zo duidelijk terug te vinden in het IPv6-adres. Het eerste teken geeft de locatie aan (L) en het tweede teken de gebruikstype (T).

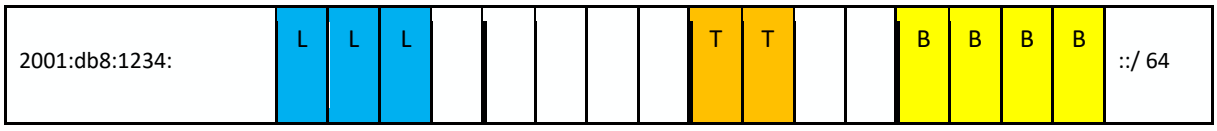
4.8 FLEXIBILITEIT VOOR TOEKOMSTIGE GROEI

Als het aantal locaties en/of gebruikstypes kan groeien op een manier die moeilijk te voorspellen is op het moment dat het nummerplan opgesteld wordt, dan kan het nuttig zijn om de grenzen tussen de verschillende groepen bits zo flexibel mogelijk te houden. Dit kan op de manier die beschreven staat in RFCs 1219 en 3531. Het nadeel van deze aanpak is dat het een goed begrip van bitmanipulatie vereist. Daarnaast is het periodiek, wanneer de grenzen tussen de velden opschuiven, firewallregels en dergelijke aangepast moeten worden. Wanneer de locatie in de bovenste bits gecodeerd wordt en hierna het

gebruikstype volgt dan kan een nummerplan met flexibele grenzen als volgt beginnen, met vijf locaties, drie gebruikstypes en twee subnetten per locatie/gebruikstype:

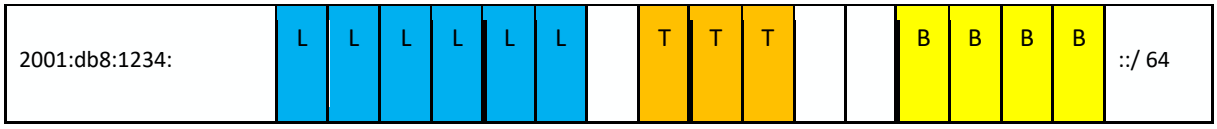


Daarna gaat bijvoorbeeld het aantal subnetten per gebruikstype van twee naar tien, en heeft dus vier bits nodig:

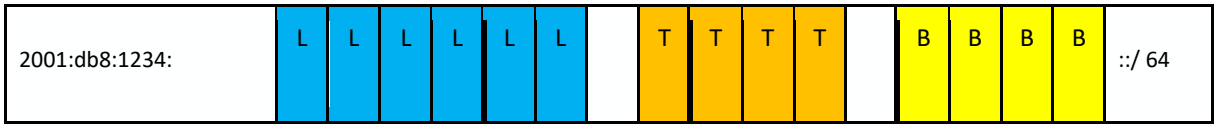


Vervolgens stijgt het aantal gebruikstypes tot vijf, en heeft dit veld een derde bit nodig. Er zijn meer vrije bits aan de linkerkant, dus het gebruikstype-veld groeit in die richting:

Het aantal locaties groeit naar 50 en heeft zes bits nodig:



Het aantal gebruikstypes groeit tot 13 en heeft een vierde bit nodig, wat van rechts komt waar er meer ongebruikte bits zijn:

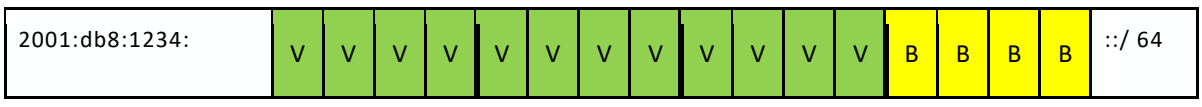


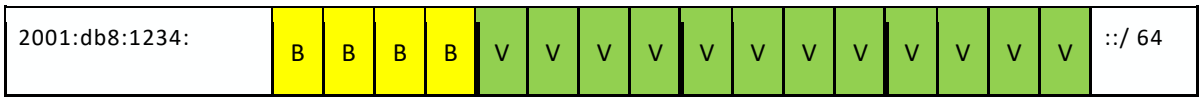
Enzovoort. Let op dat de L- en T-velden bits toegevoegd kregen aan de rechterkant, wat betekent dat om hernummeren te voorkomen, de codering van een nummer in deze bits op een wat ongebruikelijke manier plaats moet vinden. Zie RFC 3531 voor meer informatie.

4.9 GEBRUIK VAN VLAN-NUMMERS

Een andere optie is om VLAN-nummers als subnetnummers te gebruiken. In netwerken waar de meeste subnetten VLANs zijn en dus al een VLAN-nummer hebben maakt dit het bijhouden van VLAN- en subnetnummers makkelijker, omdat nu maar één nummer bijgehouden hoeft te worden.

VLAN-nummers zijn 12 bits groot, terwijl subnetnummers 16 bits zijn (uitgaande van een /48 prefix voor de organisatie). Het is dus mogelijk om simpelweg één van de twee volgende methodes te gebruiken:





Alleen worden IPv6-adressen hexadecimaal geschreven, maar VLAN-nummers decimaal. De bovenstaande methodes vereisen dus een conversie tussen hex en decimaal die de relatie tussen het VLAN- en het subnetnummer een stuk ingewikkelder en onduidelijker maakt.

Een betere aanpak is om het decimale VLAN-nummer als het hexadecimale subnetnummer te gebruiken. Dus VLAN 2783 wordt simpelweg subnet 2001:db8:1234:2783::/64. Let op dat dit de subnetnummers boven de 4096 en ook alle subnetnummers waar een letter in voorkomt vrijlaat voor extra subnetten die niet aan een VLAN gebonden zijn

Het in het IPv6-subnet overnemen van het VLAN ID is minder geschikt voor overheidsorganisaties. Binnen het overheidsbrede IPv6-nummerplankader krijgt iedere overheidsorganisatie meerdere /48-prefixen krijgt binnen verschillende beveiligingscategorieën. Als het VLAN ID in het subnet-deel van het IPv6-adres opgenomen wordt, dan zal ieder VLAN een adresreeks binnen elke beveiligingscategorie krijgen. Mocht er dan een fout gemaakt worden met het activeren van deze adressen, dan kan het relatief makkelijk gebeuren dat vertrouwde systemen via adressen binnen een minder vertrouwde beveiligingscategorie, die dus zeer waarschijnlijk minder strikt gefirewalled zal zijn, bereikbaar worden.

Om die reden raden wij het één-op-één overnemen van de VLAN-indeling in het IPv6-nummerplan af voor overheidsorganisaties. In het document “Een IPv6-nummerplan opstellen”[5] van Surfnet beschrijven secties 4.10 en 4.11 het gebruik van het VLAN ID in het subnet-deel van het IPv6-adres in meer detail.

4.10 ADRESGEBRUIK OP POINT-TO-POINT VERBINDINGEN

Als u gebruik maakt van point-to-point verbindingen kan het gebruik van een /64 voor zulke verbindingen problemen opleveren bij bepaalde routerimplementaties. Adressen uit de /64 die niet in gebruik zijn worden door de routers aan beide kanten van de verbinding naar de andere kant gestuurd. Hierdoor gaan pakketten die aan zo’n adres gericht zijn pingpongen tussen de routers. Dit levert een ongewenste belasting op voor het netwerk. Daarom is het in sommige gevallen nuttig om een prefix langer dan /64 op deze verbindingen te configureren.

- Let op: het gebruik van een subnetgrootte anders dan /64 is niet in overeenstemming met RFC 4291[6].

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

[6] http://tools.ietf.org/html/rfc4291#section-2.5.4

Maar als een subnet geen /64 is, wat is dan wel een gepaste subnetgrootte voor point-to-point verbindingen?

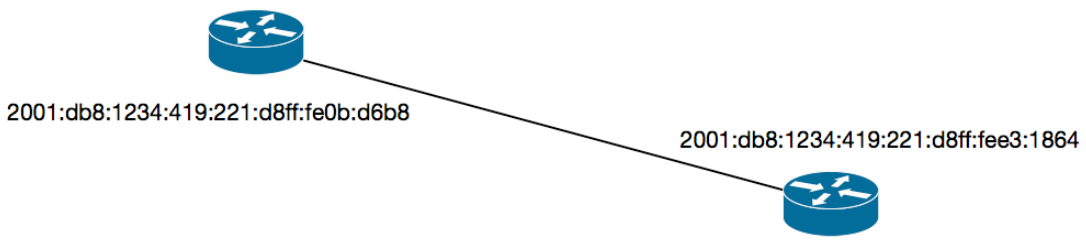
- **/127** is mogelijk omdat IPv6 geen broadcastadres heeft. Maar het laagste adres in elk subnet (waarvan alle bits volgend op de prefix 0 zijn) is het "all routers anycast address", wat betekent dat alle routers geacht worden pakketten aan dat adres te ontvangen. Sommige routerleveranciers implementeren dit niet, dus een /127 subnet werkt op hun routers. Maar problemen kunnen ontstaan wanneer apparatuur vervangen wordt door die van een andere leverancier.
- **/126** maakt het mogelijk het laagste adres over te slaan. Maar de hoogste 128 adressen in elk subnet zijn ook gereserveerd voor verschillende anycastadressen (RFC 2526). Maar in praktijk levert dat gewoonlijk geen problemen op.
- **/120** maakt het mogelijk alle gereserveerde anycastadressen over te slaan.
- **/112** maakt het mogelijk alle gereserveerde anycastadressen over te slaan en heeft het voordeel dat de hele viercijferige hexadecimale waarde na de laatste dubbele punt in het IPv6-adres het subnet systemen binnen het subnet identificeert.

Dus /112 lijkt het beste niet-/64 alternatief. Maar het kan ook nuttig zijn het aantal adressen binnen een subnet te beperken om zo "neighbor cache exhaustion attacks", waar een aanvaller alle adressen in een subnet scant waardoor routers Neighbor Discovery moeten uitvoeren voor al die adressen, wat hun capaciteiten te boven kan gaan. Dus een alternatief kan zijn een /126 of /120 waarbij een /112 gereserveerd wordt om de leesbaarheid te bevorderen, of zelfs een volledige /64 zodat het mogelijk is later naar /64 over te gaan.

4.11 EUI-64-ADRESSERING

Op subnetten waar alleen routers aanwezig zijn kan het nuttig zijn de routers de laagste 64 bits van hun IPv6-adres automatisch te laten genereren. Op deze manier is het niet nodig om bij te houden welke router welk adres heeft. Hiervoor kan een instelling aanwezig zijn om "EUI-64" (de 64-bit representatie van een Ethernet MAC-adres) -adressering te configureren. Routers genereren dan een IPv6-adres op basis van hun MAC-adres op dezelfde manier als werkstations de laagste 64 bits van hun IPv6-adres uit hun MAC-adres genereren wanneer stateless address autoconfiguration gebruikt wordt. Net als stateless address autoconfiguration is EUI-64-adressering alleen mogelijk op /64 subnetten.

Het onderstaande plaatje laat een subnet zien met twee Cisco routers geconfigureerd met de configuratiecommando's "ipv6 address 2001:db8:1234:419::/64 eui-64" op het interface dat met het subnet verbonden is. Ondanks de identieke configuratie heeft iedere router een uniek adres.



5. BEHEER VAN WERKSTATIONS

Nu er een plan ligt voor het nummeren van de IPv6-netwerken, kunnen we kijken naar de nummering van de werkstations en servers (hosts) binnen het netwerk. Hiervoor zijn drie gangbare methoden beschikbaar:

- Stateless address autoconfiguration
- Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- Handmatige configuratie

Voor de meeste werkstations raden we het gebruik van automatische configuratie aan, via stateless address autoconfiguration (soms onofficieel afgekort tot SLAAC) of DHCPv6. Dit vereenvoudigt het beheer aanzienlijk. Mits goed geïmplementeerd verhoogt het ook de privacy van de gebruikers. Alleen voor apparatuur zoals routers, switches, firewalls en servers wordt aangeraden handmatige, statische configuratie toe te passen.

5.1 STATELESS ADDRESS AUTOCONFIGURATION

Stateless address autoconfiguration (SLAAC) is de meest eenvoudige manier om werkstations op een IPv6-netwerk aan te sluiten. De router verstuurt zogenaamde Router Advertisements (RA's) en de werkstations gebruiken de informatie in de RA in combinatie met hun MAC-adres om een IPv6-adres in te stellen. Ethernet MAC-adressen zijn 48 bits, maar deze worden verlengd tot 64 bits door in het midden de bits FFFE toe te voegen. Dit levert een 64-bit Extended Unique Identifier (EUI-64) op. Dan wordt het unique/local bit in het MAC-adres omgedraaid om te voorkomen dat handmatig geconfigureerde adressen op adressen lijken die gegenereerd op basis van een wereldwijd uniek MAC-adres. De laagste 64 bits in een IPv6-adres staan bekend als de "interface identifier". Bijvoorbeeld het MAC-adres 04:0c:ce:e9:38:60 resulteert in de interface identifier 60c:ceff:fee9:3860.

Een RA kan meerdere prefixen bevatten. Als meerdere routers op hetzelfde subnet RAs uitzenden zullen werkstations naar alle RAs van alle routers luisteren en adressen configureren op basis van alle prefixen in alle RAs. Dit kan gebruikt worden om een zekere mate van redundantie te bereiken.

5.2 PRIVACY-ADRESSEN

De laatste versies van veelgebruikte operating systemen gebruiken privacyextensies naast EUI-64-gebaseerde stateless address autoconfiguration. Deze privacyextensies voorkomen de situatie waarbij een werkstation gevolgd zou kunnen worden wanneer het verbonden is met verschillende IPv6-netwerken doordat servers elders het MAC-adres dat steeds hetzelfde is herkennen. De privacyextensies gebruiken een willekeurig nummer als interface identifier in plaats van een EUI-64. Een nieuw willekeurig nummer wordt elke 24 uur gegenereerd of wanneer het systeem (opnieuw) een verbinding met een netwerk maakt.

Normaliter genereren werkstations een op een MAC-adres gebaseerd IPv6-adres en ook een privacy adres, en gebruiken dan het privacy adres voor uitgaande verbindingen. Het MAC-adres gebaseerde adres kan dan gebruikt worden als stabiel adres om inkomende verbindingen op te ontvangen.

5.3 DYNAMIC HOST CONFIGURATION PROTOCOL FOR IPV6 (DHCPV6)

Het gebruik van privacy adressen kan problematisch zijn als netwerkbeheerders willen traceren wie wel IPv6-adres gebruikt op welk moment. De oplossing daarvoor is centraal de adresuitgifte coördineren door middel van DHCPv6. Tot een paar jaar geleden ondersteunde Mac OS X geen DHCPv6, maar in Mac OS X 10.7 werd DHCPv6 toegevoegd. Windows ondersteunt DHCPv6 vanaf Windows Vista. Op dit moment ondersteunen alle wijdgebruikte operating systemen DHCPv6, maar DHCPv6 software is niet altijd standaard geïnstalleerd in alle Linux en BSD distributies.

DHCPv6 kan naast IPv6-adressen ook andere informatie uitgeven, zoals nameserver adressen, vergelijkbaar met hoe IPv4 DHCP werkt. Het kan op twee manieren gebruikt worden:

- DHCPv6 wordt gebruikt om IPv6-adressen uit te geven en daarnaast andere informatie
- Stateless address autoconfiguration wordt gebruikt om IPv6-adressen te configureren, DHCPv6 wordt gebruikt om overige informatie uit te geven

Twee bits in router advertisements bepalen welke optie werkstations gebruiken. Om deze reden, en ook omdat DHCPv6 geen default gateway-adres uitgeeft, moeten IPv6-routers altijd router advertisements sturen naar hosts, zelfs wanneer er geen gebruik wordt gemaakt van stateless address autoconfiguration.

Let op dat, afhankelijk van hoe RAs geconfigureerd zijn, DHCPv6 en stateless address autoconfiguration allebei actief kunnen zijn, waardoor werkstations twee adressen configureren, drie als er gebruik wordt gemaakt van privacy adressen.

Als adressen door DHCPv6 worden uitgedeeld, is het aan te raden om de switches er voor te laten zorgen dat werkstations alleen de adressen gebruiken die ze via DHCPv6 hebben gekregen.

ⓘ Let op: dit is voor zowel IPv4 als IPv6 niet gestandaardiseerd. Voor IPv4 hebben meerdere leveranciers eigen beveiligingsmaatregelen geïmplementeerd. Er zijn nog weinig switches die deze beveiliging met IPv6 kunnen bieden. De enige remedie bij problemen is dan het traceren van het MAC-adres van het zich misdragende systeem.

5.4 HANDMATIGE ADRESCONFIGURATIE

Het toekennen van statische IPv6-adressen raden we alleen aan voor apparatuur zoals routers, switches, firewalls en servers. Automatische configuratie zorgt bij dit soort apparatuur op de lange termijn mogelijk voor problemen. Als bijvoorbeeld van een server de netwerkadapter wordt vervangen zal het met stateless address autoconfiguration geconfigureerde adres van de server ook veranderen, en de kans is groot dat degene die de netwerkadapter vervangt vergeet om de DNS-informatie voor de server aan te passen.

Om de herkenbaarheid van belangrijke apparatuur te vergroten, raden we aan om (delen van) het IPv4-adres in het IPv6-adres te verwerken. Hierover leest u meer in sectie 3.1 en sectie 3.2.

5.5 ROUTER ADVERTISEMENT GUARD

Het komt voor dat (thuis-)routers of werkstations IPv6 router advertisements uitzenden en zo niet-werkende IPv6-connectiviteit adverteren. Aangezien veel werkstations IPv6 (wanneer beschikbaar) prefereren boven IPv4, betekent dit dat bestemmingen die een IPv6-adres in de DNS hebben onbereikbaar worden. Als dit per ongeluk gebeurt is dat onwenselijk. Maar het is ook mogelijk dat RAs met boze opzet geïnjecteerd worden om verkeer om te leiden zodat het geïnspecteerd of gemanipuleerd kan worden.

RFC 6105 beschrijft Router Advertisement Guard, een systeem dat ervoor zorgt dat ongewenste RAs hosts niet bereiken. RA Guard is een functie van apparatuur die op laag 2 werkt (zoals Ethernetswitches). Deze filteren RAs uit die komen van aangesloten apparaten die niet geacht worden RAs te genereren, terwijl RAs van de "echte" IPv6-router of IPv6-routers doorgelaten worden.

ⓘ Let bij het aanschaffen van Ethernetswitches en Wi-Fi basisstations op of deze RA Guard ondersteunen.

5.6 DNS-ADRESSEN

DNS-adressen zijn de adressen die het vaakst ingetypt worden. Het is daarom nuttig als ze kort zijn. Ze komen voor in veel lokale configuratiebestanden, en als een DNS-server één of meer domeinen draait, dan staat zijn adres ook in de configuraties van servers elders. Zodoende is het belangrijk dat DNS-adressen stabiel zijn. Gebaseerd op deze twee overwegingen is het nuttig om elke DNS-server zijn eigen /64 subnet te geven met een kort handmatig geconfigureerd adres. Bijvoorbeeld:

DNS1: 2001:db8:1234:a::53

DNS2: 2001:db8:1234:b::53

Handmatige configuratie van statische adressen zorgt dat er geen afhankelijkheid van DHCPv6, stateless address autoconfiguration en de server's MAC-adres is. Het gebruik van een eigen /64 maakt het mogelijk de server fysiek te verplaatsen zonder deze te hernummeren; het hele subnet verhuist gewoon mee met de server.

Bij IPv4 is het standaard om een DNS zone file te genereren met daarin een naam voor ieder mogelijk adres. Dus zodra een systeem op het netwerk aangesloten wordt heeft het een naam in de DNS–hoewel vaak een lelijke.

Met IPv6 is dit niet langer mogelijk, het aantal adressen per adresblok is simpelweg veel te groot. In het geval van handmatige adresconfiguratie is het natuurlijk geen probleem om het adres in de DNS te zetten. Met DHCPv6 kan de DHCPv6-server ingesteld worden zodat deze steeds hetzelfde adres uitgeeft aan hetzelfde systeem zodat dit adres in de DNS toegevoegd kan worden. Dat is wel flink wat werk. Een betere oplossing is om de DHCPv6-server een dynamic DNS update te laten uitvoeren wanneer deze een adres uitdeelt. Wel is het simpel om voor de volledige adresreeks waaruit de DHCPv6-server adressen uitgeeft DNS-namen te genereren.

Bij stateless address autoconfiguration genereren werkstations hun eigen adres. Voor MAC-adres gebaseerde adressen is het mogelijk deze handmatig in de DNS te zetten. Maar voor mobiele systemen en privacy adressen is dat niet werkbaar. Het is mogelijk een dynamic DNS (RFC 2136) cliënt op zulke systemen te draaien, maar die cliënt moet de juiste instellingen krijgen en zal misschien niet de reverse DNS bijwerken.

Gezien het bovenstaande is het heel gebruikelijk voor IPv6-systemen om geen geldige reverse DNS-naam te hebben. Het is dus niet verstandig om DNS-namen te controleren bij toegangscontrole.

APPENDIX 1: UITGEWERKTE VOORBEELDEN

Deze appendix geeft een aantal uitgewerkte voorbeelden van de nummerplanopties die uitgelegd worden vanaf sectie 4.1.

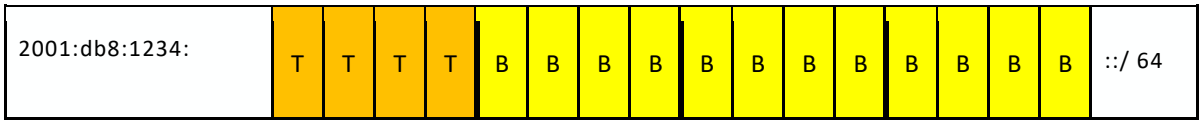
Indeling naar gebruikstypen

Er is gekozen voor een onderverdeling per gebruikstype, waarbij de volgende groepen worden onderscheiden:

- Aantal gebruikstypen (medewerkers, gasten, servers): 4 groepen
- Backbone en andere infrastructuur: 1 groep
- Totaal: 5 groepen

Na afronding naar de eerstvolgende macht van 2 komen we op een onderverdeling van 8 groepen. Om deze groepen in het IPv6-adres op te nemen hebben we 3 bits nodig ($2^3 = 8$).. We hebben met 3 ongebruikte groepen nog enige groeimogelijkheid.

Van de beschikbare 16 bits hebben we er nu 3 gebruikt; er blijven er nog 13 over. We besluiten deze niet verder onder te verdelen. Voor de leesbaarheid gebruiken we 4 bits voor de gebruikstype, waardoor er 12 bits overblijven. We houden daardoor ruimte voor 4096 (2^{12}) mogelijke netwerken per gebruikstype. Er zijn nu nog 12 bits beschikbaar:



Dit levert de volgende adresstructuur op:

2001:db8:1234:TBBB::/ 64

We kunnen dit weergeven in de volgende tabel:

Gebruikstype (T)	Vrij te kiezen (B)	Netwerk
Infrastructuur (0)	0	2001:db8:1234:**0**000::/ 64
Infrastructuur (0)	1	2001:db8:1234:**0**001::/ 64
Infrastructuur (0)	12	2001:db8:1234:**0**00c::/ 64
Infrastructuur (0)	100	2001:db8:1234:**0**064::/ 64
Medewerkers (1)	0	2001:db8:1234:**1**000::/ 64
Medewerkers (1)	12	2001:db8:1234:**1**00c::/ 64
Medewerkers (1)	321	2001:db8:1234:**1**141::/ 64

Gebruikstype (T)	Vrij te kiezen (B)	Netwerk
Etc.		

Indeling naar gebruikstypen en locaties

Er is gekozen voor een onderverdeling per gebruikstype en per locatie.

Voor de gebruikstypen worden de volgende groepen onderscheiden:

- Aantal gebruikstypen (medewerkers, gasten, servers): 4 groepen
- Backbone en andere infrastructuur: 1 groep
- Totaal: 5 groepen

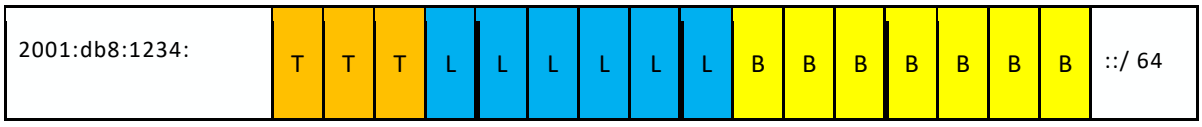
Na afronding naar de eerstvolgende macht van 2 komen we op een onderverdeling van 8 groepen. Om deze groepen in het IPv6-adres op te nemen hebben we 3 bits nodig ($2^3 = 8$). We hebben met 3 ongebruikte groepen nog enige groeimogelijkheid.

In dit voorbeeld gaan we verder uit van 35 locaties. Met 6 bits hebben we ruimte voor 64 (2^6) locaties, wat ruim voldoende is.

Er zijn nu 9 bits gebruikt voor de onderverdeling; er blijven er 7 te gebruiken. Daarmee kunnen we per gebruikstype, per locatie tot 128 (2^7) netwerken van dezelfde categorie inrichten.

We kiezen er in dit voorbeeld voor om geen aanpassingen te doen voor de leesbaarheid. Dit raden we in de praktijk niet aan, maar in dit voorbeeld willen we laten zien wat de invloed op de leesbaarheid is van een minder optimaal nummerplan.

We hebben nu de volgende IPv6-adresstructuur:



Dit levert de volgende voorbeeldadressen op, waarin duidelijk wordt dat de groepen niet in het adres terug te lezen zijn:

Gebruikstype	Locatie	Vrij te kiezen	Netwerk
Infrastructuur (0)	Niet locatie-gebonden (0)	0	2001:db8:1234:**0000**::/ 64
Infrastructuur (0)	Niet locatie-gebonden (0)	1	2001:db8:1234:**0001**::/ 64
Infrastructuur (0)	Niet locatie-gebonden (0)	2	2001:db8:1234:**0002**::/ 64
Infrastructuur (0)	Stadhuis	0	2001:db8:1234:**0080**::/ 64

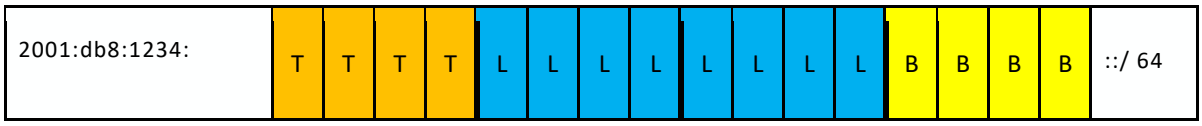
Gebruikstype	Locatie	Vrij te kiezen	Netwerk
Infrastructuur (0)	Stadskantoor	0	2001:db8:1234:**1180**::/ 64
Medewerkers (1)	Niet locatie-gebonden (0)	0	2001:db8:1234:**2000**::/ 64
Medewerkers (1)	Stadhuis	12	2001:db8:1234:**208c**::/ 64
Medewerkers (1)	Stadskantoor	9	2001:db8:1234:**3189**::/ 64
Etc.			

De leesbaarheid verbeteren

Hoewel de onderverdeling in het vorige voorbeeld goed kan werken, is het niet makkelijk om de adressen te lezen. Om de leesbaarheid te verbeteren gaan we nu de onderverdelingen maken in groepen van 4 bits, zoals beschreven in sectie 4.8.

We nemen 4 bits voor de gebruikstypen en 8 bits voor de locaties. We houden nu nog 4 bits over om per soort per locatie netwerken in te richten. Controleer wel of deze 4 bits genoeg zijn. Een situatie waar 4 bits niet genoeg zou zijn is bijvoorbeeld als er meer dan 16 (2^4) medewerker netwerken per locatie nodig zijn. We kunnen dan de extra speelruimte die we gecreëerd hebben door een extra bit voor de gebruikstypen te nemen gebruiken zoals omschreven in sectie 2.5.

We krijgen de volgende verdeling:



Dit levert de volgende adresstructuur op:

2001:db8:1234:TLLB::/ 64

Dit is in het volgende voorbeeld terug te zien:

Gebruikstype	Locatie	Vrij te kiezen	Netwerk
Infrastructuur (0)	Niet locatie-gebonden (0)	0	2001:db8:1234:**0**000::/ 64
Infrastructuur (0)		1	2001:db8:1234:**0**001::/ 64

Gebruikstype	Locatie	Vrij te kiezen	Netwerk
Infrastructuur (0)		2	2001:db8:1234:0002::/ 64
Infrastructuur (0)	Stadhuis	0	2001:db8:1234:0010::/ 64
Infrastructuur (0)	Stadskantoor	0	2001:db8:1234:0230::/ 64
Medewerkers (1)	Niet locatie-gebonden (0)	0	2001:db8:1234:1000::/ 64
Medewerkers (1)	Stadhuis	12	2001:db8:1234:101c::/ 64
Medewerkers (1)	Stadskantoor	9	2001:db8:1234:1239::/ 64
Etc.			

APPENDIX 2: CONCEPT HOOFDINDELING IP NUMMERING

[wordt later toegevoegd]