

# **IPv6-nummerplan opstellen**

## ***Handleiding***

# Inhoud

<b>1</b>	<b>Inleiding.....</b>	<b>3</b>
<b>2</b>	<b>Opbouw IPv6-adressen .....</b>	<b>4</b>
<b>3</b>	<b>Mogelijkheden zonder nummerplan.....</b>	<b>7</b>
<b>4</b>	<b>Nummerplan voor netwerken opstellen.....</b>	<b>8</b>
<b>5</b>	<b>Uitgewerkte voorbeelden.....</b>	<b>16</b>
<b>6</b>	<b>Beheer van hosts .....</b>	<b>19</b>



# 1 Inleiding

## 1.1 Waarom dit document?

De IPv4-adressen raken op en steeds meer bedrijven en instellingen zien de noodzaak van het overstappen naar een IPv6-adresstructuur. Een IPv6-adres heeft 128 bits, waardoor er theoretisch  $2^{128}$  adressen beschikbaar zijn, heel veel meer dan de  $2^{32}$  (=4,3 miljard) adressen die met IPv4 beschikbaar zijn. Om een voorstelling te maken:  $2^{128}$  is ongeveer het aantal zandkorrels op de aarde.

Bij het opstellen van een IPv4-nummerplan zijn de keuzemogelijkheden voor verschillende indelingen beperkt doordat een organisatie relatief weinig IPv4-adressen ter beschikking krijgt. De IPv4 adresindeling is daarom meestal gebaseerd op efficiënt adresgebruik. Als u een IPv6-adresrange aanvraagt bij SURFnet, krijgt u standaard  $2^{80}$  adressen ter beschikking. Dit zijn er zoveel dat efficiëntie bijna geen rol meer speelt. Het is daarom zinvol om een IPv6-nummerplan op te stellen: een systeem volgens welk u de IPv6-adressen toekent aan locaties en/of gebruikerstypen.

Door een goed IPv6-nummerplan op te zetten, worden IPv6-adresranges 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 access lists 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.

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.

## 1.2 Voor wie?

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.

## 2 Opbouw IPv6-adressen

### 2.1 Adresnotatie

Een IPv6-adres bestaat uit 128 bits, die elk de waarde 0 of 1 kunnen 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.

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
```

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

```
2001:db8:0:0:0:0:0:0
```

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

```
2001:db8::
```

De exacte regels voor het noteren van IPv6 adressen zijn vastgelegd in RFC 5952<sup>1</sup>.

### 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. Dit zijn alle adressen die met dezelfde bits beginnen. Het aantal bits dat hetzelfde is, wordt achter het adres geschreven, gescheiden door een slash. De prefix

```
2001:db8::/32
```

bevat dus alle adressen van

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

tot en met

```
2001:0db8: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
```

tot en met

---

<sup>1</sup> <http://tools.ietf.org/html/rfc5952#page-10>

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

Het is gebruikelijk om de scheiding tussen groepen aan te brengen tussen twee hexadecimale cijfers in een adres, dus per veelvoud van vier bits. Dit verhoogt de leesbaarheid van de adressen. Daarom worden de prefixen /48, /52, /56, /60 en /64 veel gebruikt. Ligt de scheiding niet tussen twee hexadecimale cijfers, dan worden de adressen minder leesbaar, zie kader.

**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.

**2.3 Toewijzing adresblokken**

IPv6-adresranges worden op de volgende wijze toegewezen:

Prefix	Toegewezen aan	Aantal adressen
/32	LIR (Local Internet Registry, meestal een internetprovider)	2 <sup>96</sup>
/48	Organisatie	2 <sup>80</sup>
/64	Netwerk binnen organisatie	2 <sup>64</sup>
/128	Host (PC, server, printer, router)	1

Deze handleiding gaat ervan uit dat alle netwerken gebruik gaan maken van een /64 adresblok. Hiervan kan afgeweken worden, maar wij raden dit niet aan omdat niet alle apparatuur op dezelfde manier omgaat met adresblokken van een ander formaat.

Daarnaast wordt aangenomen dat uw organisatie een /48 adresblok ter beschikking heeft gekregen, en dat er dus 16 bits (64 - 48) beschikbaar zijn voor de onderverdeling van de adressen in netwerken. Is dat in uw geval anders, dan moet u de berekeningen uit deze handleiding daarop aanpassen.

Uitgaande van het bovenstaande liggen de eerste 48 bits van uw IPv6-adressen vast. We gebruiken in dit document 2001:db8:1234::/48 als voorbeeld. Dit betekent dat u de /64 prefixen

2001:db8:1234:0000::/64

tot en met

2001:db8:1234:ffff::/64

voor uw netwerken kunt gebruiken, in totaal 16 bits.

Deze voorbeeldnummers moet u in uw eigen nummerplan vervangen door de aan u toegewezen prefix.

## 2.4 Weergave van onderverdelingen

In deze handleiding gaan we de 16 beschikbare bits onderverdelen in groepen. We onderscheiden de volgende typen groepen:

- B: bit is nog beschikbaar voor onderverdeling
- L: bit wordt gebruikt voor onderverdeling naar locatie
- G: bit wordt gebruikt voor onderverdeling naar gebruiksoort

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

2001:db8:1234: 

L	L	L	L	G	G	G	G	B	B	B	B	B	B	B	B
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

 ::/64

Elk vakje representeert 1 bit. 4 vakjes samen representeren dus 1 hexadecimaal cijfer in het IPv6-adres, wat voor bovenstaand voorbeeld de volgende adresstructuur oplevert:

2001:db8:1234:**LGBB**::/64

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

## 3 Mogelijkheden zonder nummerplan

### 3.1 Geen nummerplan

Voor kleine, platte organisaties zonder interne organisatorische (er zijn meerdere afdelingen binnen de organisatie die een gedelegeerde bevoegdheid hebben om IP-adressen toe te kennen) of technische (er worden verschillende typen gebruikers en netwerken onderscheiden) structuur is het mogelijk zonder nummerplan te werken en bij het inrichten van een netwerk een willekeurig vrij IPv6-adresblok aan een netwerk toe te kennen.

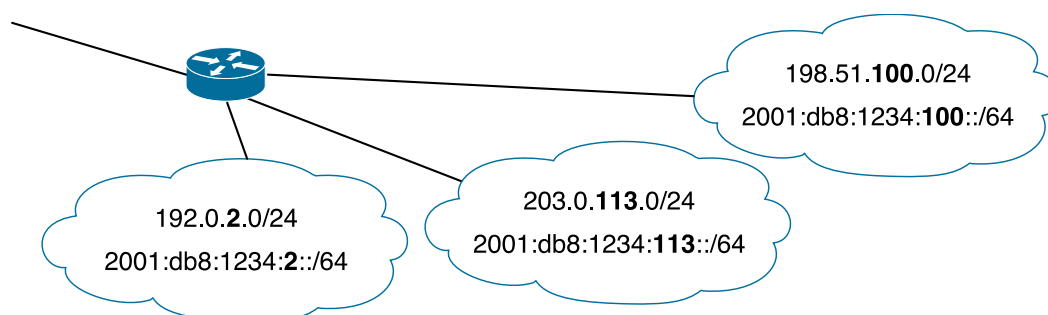
Een nadeel is echter dat het lastig kan zijn om netwerken te herkennen aan de hand van hun adres, omdat er geen structuur in de nummering zit. We raden daarom aan om altijd een nummerplan op te stellen.

Kiest u er toch voor om zonder nummerplan te werken, dan is het raadzaam om op een centrale plaats, bijvoorbeeld een Excel-spreadsheet, een interne wiki-pagina of in de reverse DNS-configuratie, een lijst van toegekende netwerken bij te houden.

### 3.2 Directe relatie tussen IPv4- en IPv6-adressen

Als de bestaande IPv4-netwerken uitsluitend gebruik maken van /24-subnetten (bijvoorbeeld van 203.0.113.0 tot 203.0.113.255), kan een directe relatie worden aangebracht tussen de bestaande IPv4-adressen en de nieuwe IPv6-adressen. Verwerk het voorlaatste getal van het IPv4-adres (113 in bijvoorbeeld 203.0.**113**.0/24) in het IPv6 subnet. Dat wordt dan 2001:db8:1234:**113**::/64.

Een dergelijke nummering kan er als volgt uit zien:



Op deze manier is de relatie tussen de bestaande IPv4-netwerken en de IPv6-netwerken direct zichtbaar.

Voor belangrijke apparatuur, zoals servers en routers, kan het ook handig zijn om het laatste getal van het IPv4-adres in het IPv6-adres te gebruiken. Zo zou het IPv4-adres 192.0.2.**123** bijvoorbeeld IPv6-adres 2001:db8:1234:2::**123** kunnen krijgen. Het is ook mogelijk om het hele IPv4 adres in het IPv6 adres op te nemen. Zo krijgt u bijvoorbeeld IPv6-adres 2001:db8:1234:2:192:0:2:123.

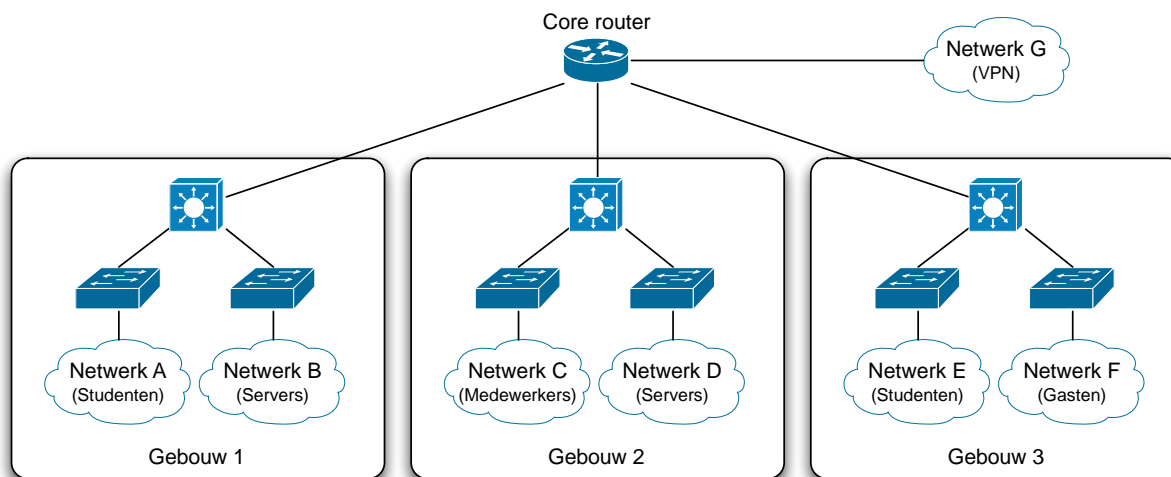
Kiest u voor deze optie, dan is het raadzaam om op een centrale plaats, bijvoorbeeld een Excel-spreadsheet, een interne wiki-pagina of in de reverse DNS-configuratie, een lijst van toegekende netwerken bij te houden.

## 4 Nummerplan voor netwerken opstellen

### 4.1 Inleiding

Bij het opstellen van een nummerplan bepaalt u volgens welke structuur de beschikbare adressen verdeeld worden over de netwerken binnen de organisatie. Er zijn 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:



### 4.2 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 gebruiksoort of per locatie. We kunnen ook combinaties maken. Zo kunnen de adressen bijvoorbeeld eerst op gebruiksoort 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	G	G	G	G	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 gebruiksoort (G). Er blijven dan nog 8 bits beschikbaar (B). Met dit nummerplan kunnen  $16^2$  locaties genummerd worden, waarbij elke locatie de beschikking heeft over  $16^3$  gebruiksoorten. Elk van deze locaties kan per gebruiksoort  $256^4$  netwerken aanmaken.

### 4.3 Eerste onderverdeling maken

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 **gebruiksoort**

<sup>2</sup> aantal mogelijke combinaties van de 4 locatiebits

<sup>3</sup> aantal mogelijke combinaties van de 4 gebruiksoort bits

<sup>4</sup> aantal mogelijke combinaties van de 8 beschikbare bits



(bijvoorbeeld studenten, medewerkers, servers, switches, routers, openbaar, enzovoort). Deze varianten worden verder uitgewerkt.

### **Locatie**

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 routingstabellen. Alle netwerken van één locatie kunnen geaggregeerd worden tot één route in de routingstabel, waardoor deze compact blijft.

### **Gebruikssoort**

Bij een onderverdeling naar gebruikssoort is bovenstaande optimalisatie van de routing niet mogelijk, aangezien de gebruikssoorten verdeeld zijn over de locaties. Dit zal voor de meeste routers echter geen probleem zijn.

Deze onderverdeling 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 gebruikssoort is daardoor vaak maar één policy nodig in de firewalls.

### **Advies**

Op basis van het bovenstaande, raden wij aan om de adressen onder te verdelen op basis van gebruikssoort, 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.

#### **4.4 Benodigde adresruimte bepalen voor de gekozen onderverdeling**

Nu moeten we bepalen welk deel van de 16 bits beschikbare adresruimte (zie paragraaf 2.3) nodig is voor de gekozen onderverdeling. Het aantal groepen van de onderverdeling bepaalt het aantal benodigde bits. 1 bit kan 2 groepen herbergen ( $2^1$ ), 2 bits kunnen 4 groepen herbergen ( $2^2$ ), enzovoort (zie ook pagina 21).

We gaan als volgt te werk om het aantal groepen te bepalen:

1. We bepalen het aantal locaties of gebruikssoorten binnen uw organisatie. Tel voor elke locatie of gebruikssoort 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 1 of 2 groepen om rekening te houden met toekomstige uitbreidingen.
5. 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.

De uitkomst is het aantal groepen dat gebruikt wordt voor de eerste onderverdeling, naar locatie of gebruikssoort.

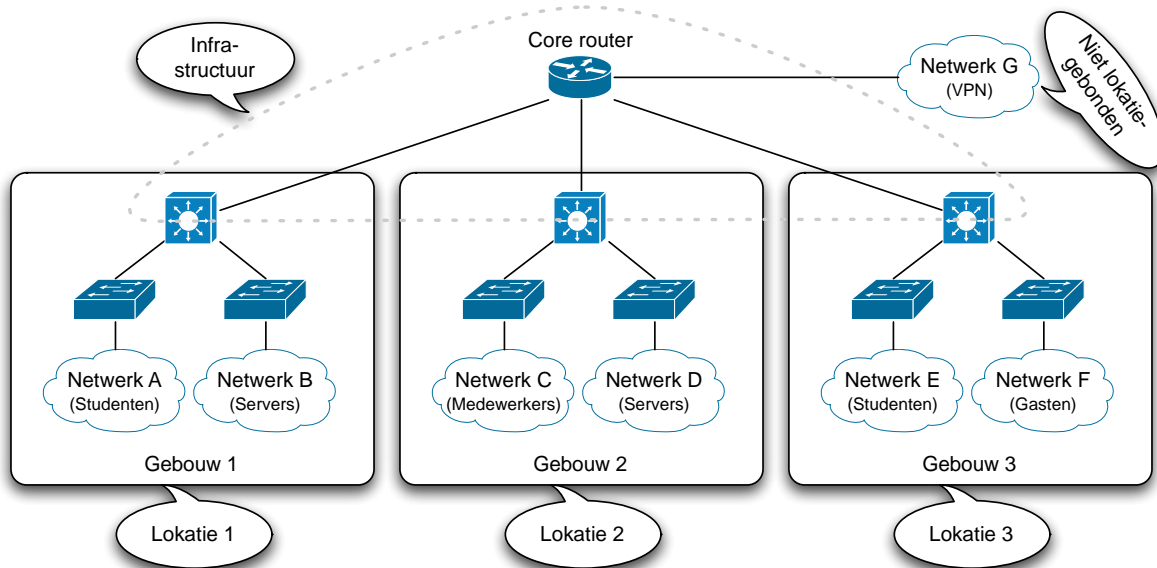
Deze werkwijze wordt uitgewerkt in een aantal voorbeelden; uitgebreidere voorbeelden vindt u in hoofdstuk 5.

### 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 pagina 21). 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

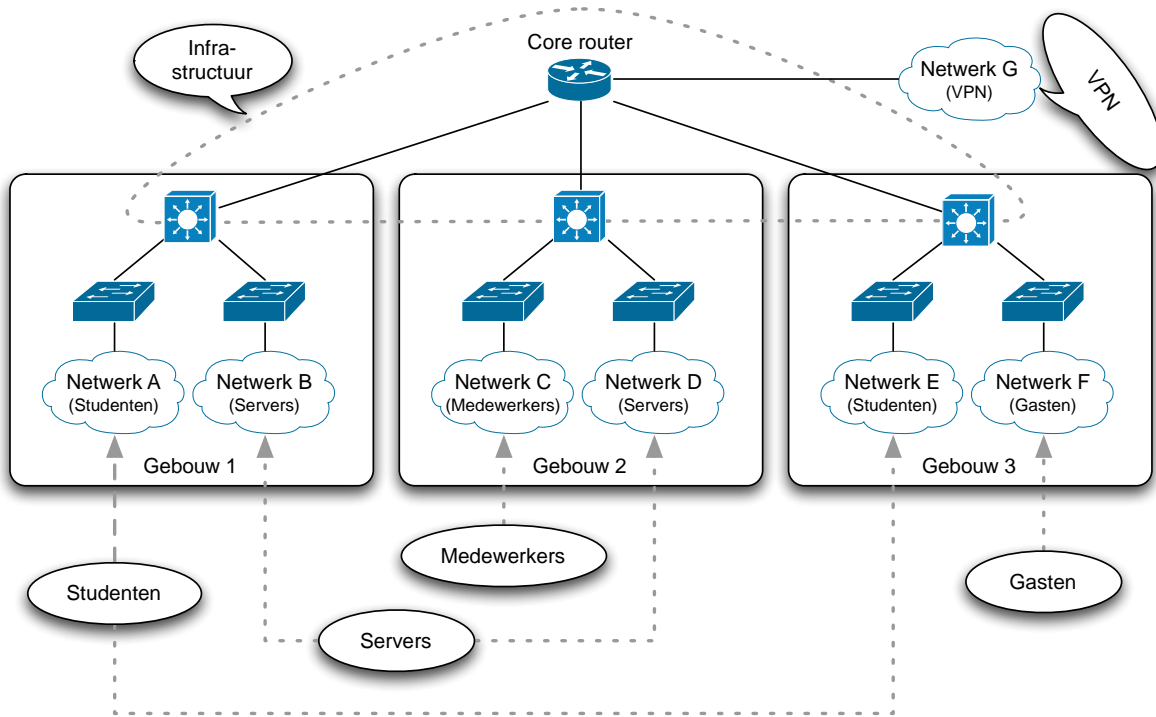
Er zijn nu nog 13 bits beschikbaar (B).

### Voorbeeld 2: naar gebruiksoort

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

- Aantal gebruiksoorten (medewerkers, studenten, gasten, servers en VPN's): 5 groepen
- Backbone en andere infrastructuur: 1 groep
- Toekomstige gebruiksoorten: 4 groepen
- Totaal: 10 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 (G) nodig ( $2^4 = 16$ ). Er zijn nu nog 12 bits beschikbaar (B):

2001:db8:1234: 

G	G	G	G	B	B	B	B	B	B	B	B	B	B	B	B
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

 ::/64

#### 4.5 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 gebruiksoort kunnen bijvoorbeeld meerdere studenten netwerken en meerdere server netwerken genummerd worden.

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

2001:db8:1234: 

I	I	I	G	G	G	G	B	B	B	B	B	B	B	B	B
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

 ::/64

In dit nummerplan is ruimte voor 8 locaties met elk 16 gebruiksoorten. Voor elke gebruiksoort 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 routingstabellen 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 gebruiksoort.

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 sub onderverdeling te maken volgens voorbeeld 1. We krijgen dan het volgende resultaat:

2001:db8:1234: 

G	G	G	G	I	I	I	B	B	B	B	B	B	B	B
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

 ::/64

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

#### 4.6 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 gebruiksoort gevolgd door een onderverdeling per locatie) meerdere studentennetwerken per locatie nodig, dan moeten er voldoende bits over zijn om deze in te richten.

In het voorbeeld uit paragraaf 4.5 zijn er nog 9 bits over, wat nog 512 (2<sup>9</sup>) mogelijke waarden per gebruiksoort per locatie oplevert. Dit zal meer dan voldoende zijn.

#### 4.7 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 gebruiksoorten en 3 bits voor de locaties. We houden dan 9 bits over waarmee we per soort per locatie 512 (2<sup>9</sup>) netwerken in kunnen richten.

2001:db8:1234: 

G	G	G	G	I	I	I	B	B	B	B	B	B	B	B
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

 ::/64

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 gebruiksoorten 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	Studenten
6	Gasten
7	Toekomstige uitbreiding
8	VPN's
9	VPN's
A	VPN's

B	VPN's
C	Toekomstige uitbreiding
D	Toekomstige uitbreiding
E	Toekomstige uitbreiding
F	Toekomstige uitbreiding

#### 4.8 Leesbaarheid

Als er voldoende bits over zijn, kunnen we bits gebruiken om de IPv6-adressen leesbaarder te maken. Elk hexadecimaal cijfer in een IPv6-adres staat voor 4 bits. Door de onderverdeling in veelvoud van 4 bits te maken, zal elke groep samenvallen met een cijfer in het IPv6-adres.

In het volgende voorbeeld gebruiken we 3 bits per locatie en 4 bits per gebruiksoort. Door 4 bits voor de locatie te nemen vergroten we de leesbaarheid, omdat dan zowel de locatie als de gebruiksoort netjes in een bij elkaar horende groep van 4 bits vallen:

2001:db8:1234: 

I	I	I	G	G	G	G	B	B	B	B	B	B	B	B
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

 ::/64

Dit wordt:

2001:db8:1234: 

I	I	I	I	G	G	G	G	B	B	B	B	B	B	B
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

 ::/64

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

2001:db8:1234:**LG**BB::/64

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

#### 4.9 Gebruik van VLAN-nummers

Er zijn organisaties die in hun VLAN-nummering al een locatie- en/of gebruiksoortaanwijzing hebben opgenomen. In dat geval kunt u overwegen om deze nummering een-op-een over te nemen in de IPv6-adresnummering, in plaats van de bovenstaande methode te gebruiken.

Als de VLAN-nummering niet gedaan is op basis van locatie of gebruiksoort is het mogelijk om het VLAN-nummer een-op-een over te nemen in het IPv6 adres. Dit maakt het voor beheerders makkelijk om de relatie te zien tussen het VLAN en het IPv6 adres. Omdat de gebruiksoort en locatie echter niet meer terugkomen in het IPv6 adres is het niet mogelijk om de security policies of de routing te optimaliseren. We raden deze manier van nummeren dan ook niet aan.

Een VLAN-nummer is 12 bits lang, terwijl we met IPv6 16 bits tot onze beschikking hebben. Als we uitsluitend het VLAN-nummer gebruiken voor het nummerplan leidt dit tot een verspilling van 15/16e deel van de IPv6-adressen. Binnen kleinere organisaties zal dit waarschijnlijk geen probleem zijn, en kan het handig zijn.

Er zijn twee manieren om dit aan te pakken:

1. We kunnen het VLAN-nummer decimaal in het IPv6-adres opnemen. De hexadecimale tekens A tot en met F worden dan nergens gebruikt. Deze notatie is makkelijk te lezen, maar is minder handig voor het opstellen van firewall policies. Deze werken op basis van de bits in het adres, wat overeenkomt met de hexadecimale notatie.
2. We kunnen het VLAN-nummer hexadecimaal in het IPv6-adres opnemen, waarbij 1 hexadecimaal teken in het IPv6-adres ongebruikt blijft. Als bijvoorbeeld wordt gekozen om het linker teken 0 te laten dan kunnen 1 tot en met F nog gebruikt worden voor andere onderverdelingen als daar behoefte aan mocht zijn.

Bijvoorbeeld:

VLAN-nummer	IPv6 decimaal	IPv6 hexadecimaal
<b>1</b>	2001:db8:1234:000 <b>1</b> ::/64	2001:db8:1234:000 <b>1</b> ::/64
<b>12</b>	2001:db8:1234:00 <b>12</b> ::/64	2001:db8:1234:000 <b>c</b> ::/64
<b>4094</b>	2001:db8:1234: <b>4094</b> ::/64	2001:db8:1234:0 <b>ffe</b> ::/64

### ***VLAN-nummerindeling omwisselen in IPv6-structuur***

Ook hier zijn nog varianten mogelijk. Als bijvoorbeeld de VLAN-nummers eerst per locatie en vervolgens per gebruiksoort onderverdeeld zijn is het nog steeds mogelijk om de IPv6-adressen eerst per gebruiksoort en daarna per locatie te verdelen.

We nemen als voorbeeld de volgende VLAN indeling, waarbij de hexadecimale notatie van het VLAN-nummer, locatie en gebruiksoort tussen haakjes staat:

VLAN-nummer	Locatie	Gebruik
0001 ( <b>001</b> )	0 ( <b>0</b> )	1 ( <b>01</b> )
0529 ( <b>211</b> )	2 ( <b>2</b> )	17 ( <b>11</b> )
4094 ( <b>FFE</b> )	15 ( <b>F</b> )	254 ( <b>FE</b> )

In dit voorbeeld geven de eerste 4 bits van het VLAN-nummer de locatie aan. De overige 8 bits geven de gebruiksoort aan. Als we dit rechtstreeks over zouden nemen in het IPv6 adres dan kunnen we de routing optimaliseren, maar niet het beveiligingsbeleid. Dit komt omdat de locatie vooraan staat en de gebruiksoort daarachter. Als we de IPv6 adressen willen gebruiken voor optimalisatie van het beveiligingsbeleid dan zal echter de gebruiksoort vooraan moeten staan.

Om dit te bewerkstelligen kunnen we de eerste 4 bits van het VLAN-nummer (die de locatie aangeven) achteraan plaatsen als de laatste 4 bits van het IPv6 netwerk. De laatste 8 bits van het VLAN-nummer (die de gebruiksoort aangeven) kunnen dan daar voor geplaatst worden.

### ***Hexadecimale notering***

Dit is in het onderstaande voorbeeld verder uitgewerkt. De hexadecimale notatie van VLAN-nummer, locatie en gebruik staat tussen haakjes.

VLAN-nummer	Locatie	Gebruik	IPv6 hexadecimaal
0001 ( <b>001</b> )	0 ( <b>0</b> )	1 ( <b>01</b> )	2001:db8:1234:00 <b>10</b> ::/64

VLAN-nummer	Locatie	Gebruik	IPv6 hexadecimaal
0529 (211)	2 (2)	17 (11)	2001:db8:1234:0112::/64
4094 (FFE)	15 (F)	254 (FE)	2001:db8:1234:0fef::/64

### ***Decimale notering***

Een soortgelijke nummering kan gebruikt worden als het VLAN-nummer op een decimale grens is opgedeeld. Als bijvoorbeeld de eerste twee cijfers de locatie aangeven en de laatste twee cijfers het gebruik, dan kan dat in het IPv6-adres omgedraaid worden. Bijvoorbeeld:

VLAN-nummer	Locatie	Gebruik	IPv6 decimaal
0001	00	01	2001:db8:1234:0100::/64
0529	05	29	2001:db8:1234:2905::/64
4094	40	94	2001:db8:1234:9440::/64

### **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 router implementaties. 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 packets 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 geen /64 maar een /127 op deze verbindingen te configureren.

Let wel op: dit werkt vaak wel, maar is niet in overeenstemming met de IPv6 standaarden!

We raden daarom aan dat u in het nummerplan een /64 reserveert voor dergelijke verbindingen, ook al gebruikt u maar een /127. Zodra de router implementatie gecorrigeerd is door de leverancier kunt u dan alsnog een /64 configureren zonder het nummerplan aan te hoeven passen.

## 5 Uitgewerkte voorbeelden

### 5.1 Indeling naar gebruiksoorten

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

- Aantal gebruiksoorten (studenten, 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 gebruiksoort, waardoor er 12 bits overblijven. We houden daardoor ruimte voor 4096 ( $2^{12}$ ) mogelijke netwerken per gebruiksoort. Er zijn nu nog 12 bits beschikbaar:

2001:db8:1234 

G	G	G	G	B	B	B	B	B	B	B	B	B	B	B	B
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

 ::/64

Dit levert de volgende adresstructuur op:

2001:db8:1234:**GBBB**::/64

We kunnen dit weergeven in de volgende tabel:

Gebruiksoort (G)	Vrij te kiezen (B)	Netwerk
Infrastructuur (0)	0	2001:db8:1234: <b>0000</b> ::/64
Infrastructuur (0)	1	2001:db8:1234: <b>0001</b> ::/64
Infrastructuur (0)	12	2001:db8:1234: <b>000c</b> ::/64
Infrastructuur (0)	100	2001:db8:1234: <b>0064</b> ::/64
Studenten (1)	0	2001:db8:1234: <b>1000</b> ::/64
Studenten (1)	12	2001:db8:1234: <b>100c</b> ::/64
Studenten (1)	321	2001:db8:1234: <b>1141</b> ::/64
etc.		

### 5.2 Indeling naar gebruiksoorten en locaties

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

Voor de gebruiksoorten worden de volgende groepen onderscheiden:

- Aantal gebruiksoorten (studenten, 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 ( $2^3$ ). We hebben met 3 ongebruikte groepen nog enige groeiemogelijkheid.

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 gebruiksoort, 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:

2001:db8:1234 

G	G	G	L	L	L	L	L	L	B	B	B	B	B	B	B
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

 ::/64

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

Gebruiksoort	Locatie	Vrij te kiezen	Netwerk
Infrastructuur (0)	Niet locatie-gebonden (0)	0	2001:db8:1234: <b>0000</b> ::/64
Infrastructuur (0)	Niet locatie-gebonden (0)	1	2001:db8:1234: <b>0001</b> ::/64
Infrastructuur (0)	Niet locatie-gebonden (0)	2	2001:db8:1234: <b>0002</b> ::/64
Infrastructuur (0)	Locatie 1	0	2001:db8:1234: <b>0080</b> ::/64
Infrastructuur (0)	Locatie 35	0	2001:db8:1234: <b>1180</b> ::/64
Studenten (1)	Niet locatie-gebonden (0)	0	2001:db8:1234: <b>2000</b> ::/64
Studenten (1)	Locatie 1	12	2001:db8:1234: <b>208c</b> ::/64
Studenten (1)	Locatie 35	9	2001:db8:1234: <b>3189</b> ::/64
etc.			

### 5.3 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.

We nemen 4 bits voor de gebruiksoorten 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 ( $2^4$ ) studentennetwerken per locatie nodig zijn. We kunnen dan de extra speelruimte die we gecreëerd hebben door een extra bit voor de gebruiksoorten te nemen gebruiken zoals omschreven in sectie 2.4.

We krijgen de volgende verdeling:

2001:db8:1234: 

G	G	G	G	I	I	I	I	I	I	I	I	I	I	B	B	B	B
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

 ::/64

Dit levert de volgende adresstructuur op:

2001:db8:1234:**GLLB**::/64

Dit is in het volgende voorbeeld terug te zien.

<b>Gebruikssoort</b>	<b>Locatie</b>	<b>Vrij te kiezen</b>	<b>Netwerk</b>
Infrastructuur (0)	Niet locatie-gebonden (0)	0	2001:db8:1234: <b>0000</b> ::/64
Infrastructuur (0)		1	2001:db8:1234: <b>0001</b> ::/64
Infrastructuur (0)		2	2001:db8:1234: <b>0002</b> ::/64
Infrastructuur (0)	Locatie 1	0	2001:db8:1234: <b>0010</b> ::/64
Infrastructuur (0)	Locatie 35	0	2001:db8:1234: <b>0230</b> ::/64
Studenten (1)	Niet locatie-gebonden (0)	0	2001:db8:1234: <b>1000</b> ::/64
Studenten (1)	Locatie 1	12	2001:db8:1234: <b>101c</b> ::/64
Studenten (1)	Locatie 35	9	2001:db8:1234: <b>1239</b> ::/64
etc.			

## 6 Beheer van hosts

### 6.1 Hosts nummeren

#### *Inleiding*

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

- StateLess Address Auto Configuration (SLAAC)
- Dynamic Host Configuration Protocol voor IPv6 (DHCPv6)
- Statische IPv6-adressen

Voor de meeste clients raden we het gebruik van automatische configuratie aan, via 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 statische configuratie toe te passen.

#### ***StateLess Address Auto Configuration (SLAAC)***

SLAAC is de meest eenvoudige manier om hosts op een IPv6-netwerk aan te sluiten. De router verstuurt zogenaamde Router Advertisements (RA's) en de hosts gebruiken de informatie in de RA in combinatie met hun MAC-adres om een IPv6-adres in te stellen.

Als er meerdere routers op één netwerk RA's versturen, zullen de hosts naar beide RA's luisteren en adressen configureren op beide netwerken. Dit kan gebruikt worden om een vorm van redundantie in te bouwen.

#### *Privacy extensions*

Sommige besturingssystemen hebben bovenop SLAAC nog privacy extensions. Het hangt af van het besturingssysteem of deze standaard aan of uit staan. Deze zorgen ervoor dat voor de buitenwereld niet zichtbaar is welk type netwerkkaart een host heeft. Bij standaard SLAAC is dit wel zichtbaar, omdat voor het aanmelden op een netwerk het MAC-adres wordt gebruikt. Bij aanmelden op verschillende netwerken (bijvoorbeeld met een smartphone), wordt steeds hetzelfde MAC-adres gebruikt. Daardoor is voor de buitenwereld zichtbaar dat het steeds om dezelfde host gaat. Privacy extensions gebruiken per host meerdere random adressen om deze herleidbaarheid te voorkomen.

Gebruik van privacy extensions in combinatie met SLAAC is echter problematisch als netwerkbeheerders willen kunnen herleiden wie op welk moment welk IPv6-adres gebruikte. Een oplossing daarvoor is het gebruik van centraal gecoördineerde adresuitgifte middels DHCPv6, zie volgende paragraaf. Niet alle besturingssystemen ondersteunen dat echter op dit moment. Het meest bekende besturingssysteem dat geen DHCPv6 ondersteuning biedt is Mac OS X. Daarnaast wordt de DHCPv6 software niet standaard door alle Linux en BSD distributies geïnstalleerd.

#### ***Dynamic Host Configuration Protocol voor IPv6 (DHCPv6)***

DHCPv6 kan op twee manieren ingezet worden:

- DHCPv6 kan samenwerken met SLAAC om de hosts van alle informatie te voorzien die SLAAC niet levert, zoals DNS-domeinen en -servers en NTP-servers.
- DHCPv6 kan gebruikt worden als vervanging van SLAAC. Hierbij worden de IPv6-adressen expliciet uitgedeeld door de DHCPv6-server.

DHCPv6 kan voor meer controle zorgen, maar niet alle hosts ondersteunen DHCPv6. Als adressen door DHCPv6 worden uitgedeeld, is het aan te raden om de switches er voor te laten zorgen dat hosts 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. Traceerbaarheid op basis van MAC-adres blijft in deze situatie dus nog steeds aangeraden.

### ***Statische adressen***

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 voor problemen. Als bijvoorbeeld van een server de netwerkadapter wordt vervangen zal het SLAAC-adres van de server ook veranderen, en de kans is groot dat degene die de netwerkadapter vervangt vergeet om de DNS-entries 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 paragraaf 3.2.

## Bijlage verhouding groepen – bits

Aantal groepen	Aantal bits
2	1
4	2
8	3
<b>16</b>	<b>4</b>
32	5
64	6
128	7
<b>256</b>	<b>8</b>
512	9
1024	10
2048	11
<b>4096</b>	<b>12</b>
8192	13
16384	14
32768	15
<b>65536</b>	<b>16</b>

## Colofon

Deze handleiding is tot stand gekomen met bijdragen van of met dank aan:

- Sander Steffann, auteur
- Roel Hoek (Universiteit Twente)
- Jeroen van Ingen Schenau (Universiteit Twente)
- Magda Pattiapon (RUG)
- Mente Heemstra (RUG)
- Rogier Spoor (SURFnet)
- Wim Biemolt (SURFnet)
- Niels den Otter (SURFnet)
- Maurice van den Akker (SURFnet)
- Jan Michielsen (SURFnet)