



# SINT-MAARTENINSTITUUT

CAHIER-REEKS OVER INFORMATICATOEPASSINGEN

NETWERKEN & IT

6 NIT


## Cahier 2 B: Module netwerken - deel 2 Beheer van Computersystemen en Netwerken



## Samenvatting

Deze cursus werd ontwikkeld met  $\text{\LaTeX}$  en is bestemd voor de leerlingen van het laatste jaar **Netwerken & IT** van het **Sint-Maarteninstituut** te Aalst.

Deze cursus is samengesteld op basis van tientallen jaren lespraktijk op school, aangevuld met diverse bronnen (internet, boeken, tijdschriften). In de mate van het mogelijk zijn telkens de correcte bronvermeldingen, in toepassing van het auteursrecht, opgenomen. Eventuele vergetelheden mogen de auteur via de school gemeld worden.

De cursus is auteursrechtelijk beschermd door de Creative Commons licentie - versie "Naamsvermelding -NietCommercieel -GelijkDelen 4.0 Internationaal (CC BY-NC-SA 4.0)", zoals beschreven in <https://creativecommons.org/licenses/by-nc-sa/4.0/deed.nl> en voorgesteld door .

In de tabel hieronder vind je de verschillende aanpassingen sinds de eerste versie.

Datum	Aanpassing
2023-01-09	Eerste versie klaar voor verspreiding.

# Inhoudsopgave

<b>I</b>	<b>IP adressering</b>	<b>I-1</b>
<b>1</b>	<b>IPv4: herhaling van basisbegrippen</b>	<b>I-3</b>
1.1	Inleiding . . . . .	I-3
1.2	Het IP-adres . . . . .	I-3
1.2.1	De <b>bouw</b> van het IP-adres . . . . .	I-3
1.2.2	De indeling in klassen . . . . .	I-4
1.2.3	De speciale IP adressen . . . . .	I-4
1.3	Het subnetmasker . . . . .	I-5
1.3.1	De <b>bouw</b> van het subnetmasker . . . . .	I-5
1.3.2	De <b>betekenis</b> van het subnetmasker . . . . .	I-5
1.3.3	Wat je moet je weten of kunnen? . . . . .	I-6
<b>2</b>	<b>Subnetting in klasse c</b>	<b>I-7</b>
2.1	Waarom subnetting . . . . .	I-7
2.2	Hoe doe je subnetting . . . . .	I-8
2.2.1	Als voorbeeld /25: werken met twee subnetten . . . . .	I-9
2.2.2	De verbinding tussen twee routers . . . . .	I-11
2.2.3	Een subnet voor 14tal pc's . . . . .	I-12
2.2.4	En verder... . . . .	I-14
2.2.5	Wat moet je weten of kunnen? . . . . .	I-14
<b>3</b>	<b>Werken met IPv6</b>	<b>I-15</b>
3.1	Het overzicht van de basisbegrippen . . . . .	I-15
3.2	MultiMedia verkenning . . . . .	I-18
3.3	Inleiding . . . . .	I-19
3.4	De kenmerken van een IPv6 adres . . . . .	I-19
3.4.1	De bouw van een IPv6 adres . . . . .	I-19
3.4.2	Het MAC adres als basis van een uniek hostgedeelte . . . . .	I-20
3.4.3	Grafische voorstelling van het IP adres . . . . .	I-21
3.4.4	DHCP v6 . . . . .	I-23
3.4.5	Het weglaten van de voorloophnullen. . . . .	I-23
3.4.6	SLAAC . . . . .	I-25
3.5	De verschillende types van een IPv6 adres . . . . .	I-26
3.6	De reikwijdte van een IPv6 adres . . . . .	I-26
3.7	Het zone nummer van een IPv6 adres . . . . .	I-28
3.8	Scripting . . . . .	I-28
3.9	Speciale IPv6 adressen . . . . .	I-29
3.10	Hoe kan je een bruikbaar IP adres aan je computer geven . . . . .	I-33
3.11	Synthesetabel . . . . .	I-34
3.12	Wat moet je weten of kunnen . . . . .	I-35

<b>II</b>	<b>Bijlagen en documentatie</b>	<b>II-1</b>
<b>1</b>	<b>Opvolging van Leren-Leren</b>	<b>II-3</b>
1.1	Overzicht van taken en toetsen in 6 NIT (Beheer) . . . . .	II-3

**Deel I**

# **IP adressering**



# 1 IPv4: herhaling van basisbegrippen

## 1.1 Inleiding

**Doelstelling:** 3.1.12 *De mogelijke technieken van adressering in een actuele netwerkachitectuur toelichten.*

**Doelstelling:** 3.1.13 *De begrippen subnet en subnetmasker en de functie ervan toelichten.*

Om een computertoestel éénduidig te kunnen aanwijzen heb je een unieke referentie nodig, dat al dan niet afhankelijk van de gebruikte computerhardware. Het MAC (Media Access Control) is een referentie op basis van de netwerkkaart en situeert zich op de 2de laag van het OSI model. Het IP adres is een identificatie op de 3de laag van het OSI model.

De leerstof in dit deel bespreekt IPv4. Sinds enkele jaren is ook IPv6 in gebruik met de bedoeling dat 'binnenkort' IPv6 volledig IPv4 vervangt. Sinds februari 2011 zijn de laatste beschikbare IPv4 adressen toegewezen maar dit had niet tot gevolg dat iedereen en overal de overstap maakte.

Voor **WAN netwerken** zal de overstap veel vlugger en transparant gebeuren. Het is een zaak van **Internet Service Providers (ISP)** en elke organisatie die het Internet in stand houdt. Voor **LAN netwerken** zal de komende jaren nog altijd IPv4 gebruikt worden.

## 1.2 Het IP-adres

### 1.2.1 De bouw van het IP-adres

Het IP-adres is als volgt opgebouwd:

- het is opgebouwd uit 32 bits
- per acht bits gegroepeerd
- door een 'punt' gescheiden
- als decimaal getal voorgesteld

### 1.2.2 De indeling in klassen

De beschikbare IP adressen worden in klassen ingedeeld. In de tabel hieronder vind je de verschillende netwerken

Klasse	Linker bits 1ste byte	Netwerkdeel	Individueel PC deel	Def. Subnetmasker
A	0	0 -> 127	0.0.1 -> 255.255.254	255.0.0.0
B	10	128.0 -> 191.255	0.1 -> 255.254	255.255.0.0
C	110	192.0.0 -> 223.255.255	1 -> 254	255.255.255.0
D	1110	—	—	—
E	1111	—	—	—

Tabel 1.1: Indeling in klasse voor IPv4

In de praktijk worden enkel klasse A, B en C gebruikt. Klasse D is toegewezen aan multicasting. Klasse E is voorbehouden voor experimenten.

### 1.2.3 De speciale IP adressen

#### 1.2.3.1 Het IPadres van het netwerk

Het IP adres van het netwerk is opgebouwd uit het netwerkdeel (zie hoger), aangevuld met binair '0' aan de rechterkant. Deze laagste waarde is het IP adres van het netwerk en kan nooit aan een individueel toestel gegeven worden. Je gebruikt het IPadres van een netwerk om het netwerk in zijn geheel aan te duiden. Het wordt best gevolgd door het subnetmasker, in verkorte vorm, ook als het subnetmasker het defaultsubnetmasker voor die klasse van IP adressen is.

Bijvoorbeeld: Het Netwerkdeel van **194.58.9.7/24** is gelijk aan 194.58.9. je vult dit aan met binaire '0' tot je terug 32 bits bekomt. In dit geval heb je 8 keer '0' nodig, omgerekend '0'. Het IP adres van dit netwerk is dus **194.58.9.0/24**

#### 1.2.3.2 Het broadcastadres van het netwerk

Het broadcast adres van het netwerk is opgebouwd uit het netwerkdeel (zie hoger), aangevuld met binair '1' aan de rechterkant. Deze hoogste waarde is het broadcast adres van het netwerk en kan nooit aan een individueel toestel gegeven worden. Het broadcastadres gebruik je als je een broadcast naar je netwerk verstuurt opdat elk toestel zou reageren op jouw bericht.

#### 1.2.3.3 De private adressen

Elke klasse heeft één of meerdere netwerken die je kan gebruiken voor lokale netwerken uit te werken. Deze IP adressen zullen nooit door een router doorgegeven worden. De adressen zijn dus beperkt tot lokale netwerken (de scope zijn dus lokale netwerken).

In de tabel hieronder vind je het overzicht van die privé netwerken



Klasse	Privé netwerken	Aantal privé netwerken voor gegeven klasse
A	10.0.0.0	1
B	172.16.0.0 tot 172.31.0.0	16
C	192.168.0.0 tot 192.168.255.0	256

Tabel 1.2: Overzicht van de private adressen

## 1.3 Het subnetmasker

### 1.3.1 De bouw van het subnetmasker

Voor de bouw van het subnetmasker gelden volgende regels:

- de voorwaarden van het IP adres, met name: het subnetmasker bestaat uit 32 bits, per acht gegroepeerd, door een 'punt' gescheiden en decimaal voorgesteld  
het begint met een binaire '1'
- het subnetmasker eindigt op een binaire '0'
- na een binaire '0' kan nooit een binaire '1' volgen

Door deze laatste drie regels, is **255.0.255.0** geen geldig subnetmasker. De waarde 255.255.240.0 is wel een geldig subnetmasker want 240 onder binaire vorm is **11110000** en voldoet aan de bovenstaande regels.

Het subnetmasker kan je ook verkort voorstellen. Je telt het aantal keer binaire waarde '1' voorkomt in het subnetmasker. Hieronder vind je een aantal voorbeelden

- /8 is gelijk aan 11111111.00000000.00000000.00000000 en omgerekend 255.0.0.0, het subnetmasker van een klasse **A** netwerk
- /16 is gelijk aan 11111111.11111111.00000000.00000000 en omgerekend 255.255.0.0. Dit is het subnetmasker van een klasse **B** netwerk
- /20 is gelijk aan 11111111.11111111.11110000.00000000 en omgerekend 255.255.240.0. Dit is het subnetmasker van een **subnet** van klasse B
- /24 is gelijk aan 11111111.11111111.11111111.00000000 en omgerekend 255.255.255.0. Dit is het subnetmasker van een klasse **C** netwerk

Je kan nog analoge voorbeelden bedenken.

### 1.3.2 De betekenis van het subnetmasker

Het subnetmasker splitst het IP adres in twee delen

- een **netwerkdeel** : waar het bijhorend Subnetmasker gelijk is aan binair '1'

- een **hostdeel**, ook **individueel pc deel** geheten, waar het bijhorend subnetmasker gelijk is aan binair '0'

Je moet altijd de combinatie gebruiken van IP adres en het bijhorend subnetmasker. Krijg je geen subnetmasker expliciet gegeven, dan mag je het defaultsubnetmasker die bij het IP adres behoort , gebruiken. Zie hiervoor tabel 1.1 op pagina I-4 gebruiken.

Enkele voorbeelden: 172.16.3.2 /16.

1. /16 staat voor het subnetmasker 255.255.0.0
2. de linker 16 bits, dus de linker 2 bytes behoren tot het netwerkdeel. het netwerkdeel is dus **172.16**
3. de rechter 16 bits, dus de rechter 2 bytes behoren tot het individueel pc deel. Het individueel pcdeel is dus gelijk aan **3.2**
4. Het IP adres van het netwerk is de combinatie van het netwerkdeel, aan de rechterkant aangevuld met de nodige aantal 'nul' om tot in totaal 32 bits te geraken. Dus het netwerkdeel **172.16** wordt zo aangepast tot **172.16.0.0**

### 1.3.3 Wat je moet je weten of kunnen?

Dit lesdeel is herhaling van vorig jaar. De typevragen verwijzen naar permanente kennis over dit onderdeel

- ? Reproduceer de overzichtstabel met de verschillende IP adressen per klasse
- ? Reproduceer de overzichtstabel van de private adressen in IPv4
- ? Bespreek de bouw van het IP adres
- ? Bespreek de bouw van het subnetmasker
- ? Bespreek de betekenis van het subnetmasker
- ? Bespreek de speciale IP adressen, met name het IP adres van het netwerk en het broadcastadres

## 2 Subnetting in klasse c

### 2.1 Waarom subnetting

**Doelstelling:** 3.1.13 *De begrippen subnet en subnetmasker en de functie ervan toelichten.*

Bij **subnetting** kan je een bestaand netwerk in kleinere, afzonderlijke netwerken splitsen. Dit kan de prestaties en de veiligheid verhogen.

**Veiligheid** door subnetting splits je je bestaand netwerk in kleinere netwerken die enkel nog via een **router** onderling kunnen verbonden worden. Op de router kan je regels (**ACL = Access control list**) instellen om ongewenst netwerkverkeer zoveel mogelijk te verhinderen.

**Performantie - broadcastdomein** door subnetting reduceer je de broadcastdomeinen. Het netwerkverkeer dat door een broadcast, bijvoorbeeld door een DHCP client naar een DHCP server, wordt daardoor beperkt tot het subnet in plaats van het volledige netwerk.

**Performantie - congestie** in een client-server netwerk kan je door een gepaste topologie de server met zijn direct verbonden clients in één afzonderlijk subnet plaatsen zodat dit client-server netwerkverkeer de rest van het netwerk niet stoort. Occasionele toegang tot de server door een client buiten het specifiek subnet is mogelijk via de router.

**Uitputting** Het aantal beschikbare IPv4 netwerken is uitgeput. Voor de meeste bedrijven is een klasse C netwerk met 254 toestellen te klein. Een klasse b netwerk kan wel  $2^{16} - 2 = 65534$  toestellen adresseren, wat voor de meeste bedrijven veel te veel is. Voor die bedrijven past de provider subnetting op een klasse B netwerk toe.

Het toepassen van subnetting vereist wel dat je op voorhand de nodige netwerkanalyse maakt en bijvoorbeeld het aantal personeelsleden en toestellen in rekening brengt. Niet alleen het huidige aantal maar ook de groeiprognose kan verwerken. *het heeft geen zin om voor een bepaalde afdeling een subnet te maken van pakweg 14 toestellen als je weet dat er een personeelsgroei verwacht wordt tot minstens 30 toestellen..... Je neemt beter dadelijk voldoende maar ook weer niet te veel toestellen in dat netwerk op.*

Je vindt op internet zeer veel documentatie over subnetting, vaak ook over de alternatieve

benaming 'Classless Inter Domain Routing' (CIDR).

### Opdracht 1

Noteer hieronder de url van 3 YouTube video's die subnetting en/of CIDR op een voldoende vlotte en begrijpbare manier uitleggen.

1.

2.

3.

*Opdracht 1: Kennismaking met subnetting, CIDR*

## 2.2 Hoe doe je subnetting

**Doelstelling:** 3.1.12 De mogelijke technieken van adressering in een actuele netwerkar-chitectuur toelichten.

In het hoofdstuk over de betekenis van het subnetmasker op pagina I-5 leer je dat het subnetmasker het IP adres in twee delen splitst :

- een **netwerkdeel** : waar het bijhorend Subnetmasker gelijk is aan binair '1'
- een **hostdeel**, ook **individueel pc deel** geheten, waar het bijhorend subnetmasker gelijk is aan binair '0'

De verkorte notitie van het subnetmasker is gelijk aan het aantal bits op '1'. Zonder subnetting is dat gelijk aan '/8' voor klasse A, '/16' voor klasse B en '/24' voor klasse C.

Bij subnetting gaan we het netwerkdeel uitbreiden en het hostgedeelte verminderen bit per bit. Telkens wordt de meest linker bit die '0' was, op '1' gezet. Alle regels voor de bouw van het subnetmasker (zie pagina I-5) blijven behouden.

Bij het lezen van de probleemstelling moet je je afvragen :

- gaat de vraag over het aantal subnetten?

Bepaal aan de hand van de opgave het aantal subnetten. Bepaal de eerst volgende macht van twee die gelijk of net groter is dan het aantal subnetten dat je nodig hebt. Voorbeeld: je hebt 7 subnetten nodig. De eerste macht van twee die groter is dan 7, is  $2^3 = 8$ . Je zal dus werken met 8 subnetten.

Het is een klassieke fout als je blijft werken met het aantal subnetten zoals in de opgave staat. De stapgrootte,  $\frac{256}{7} = 36,57$  is geen geheel getal. Dat zou je er op moeten wijzen

dat je een redeneerfout gemaakt hebt.

- gaat de vraag over het aantal pc's per subnet? In dit geval moet je rekening houden met het IP adres van het volledig netwerk en met het broadcastadres. Je moet dus eerst het maximaal aantal IP adressen dat bestemd is voor de toestellen met twee verhogen. Nu bekom je het totaal aantal IP adressen dat nodig is. Ook hier neem je de eerst volgende macht van twee die gelijk of groter is dan het totaal aantal IP adressen. *Bijvoorbeeld: je hebt in een netwerk maximaal 7 pc's nodig. Je verhoogt 7 met 2 = 9. In plaats van 8 moet je nu 16 nemen (want  $16 = 2^4$ ).* De stapgrootte is dus 16 en het aantal subnetten =  $\frac{256}{16} = 16$

De oplossingsmethode is verschillend.

Als geheugensteun vind je hiernaast de tabel met de machten van twee

n	$2^n$
0	1
1	2
2	4
3	8
4	16
5	32
6	64
7	128
8	256

Tabel 2.1: Overzicht van de machten van 2

### 2.2.1 Als voorbeeld /25: werken met twee subnetten

Als we **een bit** in het subnetmasker voor een klasse c IP adres van '0' naar '1' veranderen, wordt voor dat klasse C subnet, het subnetmasker in verkorte vorm gelijk aan '/25' (= /24 + 1). In binaire vorm uitgeschreven is het subnetmasker dan **11111111.11111111.11111111.10000000** of decimaal uitgerekend **255.255.255.128**

In dit /25 netwerk zijn er nu door het veranderen van die ene bit  $2^1 = 2$  subnetten, waarvan het individueel pc gedeelte telkens uit **7 bits** bestaat. *tip:*  $8 - 1 = 7$ . Met die 7 bits zijn er totaal  $2^7 = 128$  IP adressen beschikbaar, 126 voor het aanwijzen van individuele toestellen, 1 voor het IP adres van het netwerk en 1 voor het broadcastadres.

We kunnen voor een gegeven netwerk, bijvoorbeeld het willekeurig bepaald privénetwerk **192.168.3.0 /24** de volgende tabel samenstellen. **SVM** staat voor **subnetmasker**.

Nr sub-net	IP adres van het netwerk	Range van bruikbare IP adressen	Broadcastadres	SNM <sup>1</sup>
1	192.168.3.0	192.168.3.1 tot 192.168.3.126	192.168.3.127	/25
2	192.168.3.128	192.168.3.129 tot 192.168.3.254	192.168.3.255	/25

Tabel 2.2: Overzicht van de IP verdeling bij subnetting van één bit in klasse c netwerk

Je bouwt op de volgende manier deze tabel met het vast netwerkgedeelte: **192.168.3**. Je kan dit in elk vakje invullen. Het komt er nu op aan om de meest rechter byte te bepalen.

1. Je vult de kolom van 'nr subnet' aan. De eerste rij is '1' en zo verder tot je aan  $2^k$  komt met  $k$  gelijk aan het aantal bits in het subnet, hier gelijk aan **1** bit. Dus  $2^1 = 2$
2. Het IP adres van het eerste subnet is gelijk aan het IP adres van het volledige netwerk zonder subnetting, dus gelijk aan **192.168.3.0**
3. Het broadcastadres van het **laatste subnet** is ook altijd gelijk aan het broadcastadres van het volledige netwerk zonder subnetting, dus gelijk aan **192.168.3.255**.
4. je bepaalt de **stapgrootte** in de IP adressen per subnet. De *stapgrootte* =  $\frac{256}{\text{aantal subnetten}} = (\text{hier}) \frac{256}{2} = 128$ . Het tweede IP adres van het tweede subnet = het IPadres van het vorige subnet, verhoogd met de stapgrootte. In de praktijk is dat  $0 + 128 = 128$ . Je vult nu de waarde van **192.168.3.128** in als IPadres van het tweede subnet. Bij meer dan twee subnetten herhaal je deze stap.
5. Je bepaalt het broadcastadres. Dit is de waarde die net voor het IP adres van het volgend subnet komt. Bijvoorbeeld het broadcastadres van het eerste subnet is  $192.168.3.128 - 1 = \mathbf{192.168.3.127}$
6. Je vult overal de range van bruikbare IP adressen in: dit zijn alle IP adressen die liggen tussen het IPadres van het subnet en het broadcastadres.

De algemene formule voor het bepalen van het IPadres van het  $n^{\text{de}}$  subnet is afhankelijk van de vierde byte die je als volgt bereken:  $(n - 1) * \text{stapgrootte}$ . De stapgrootte is beperkt tot een waarde uit de lijst **4, 8, 16, 32, 64 en 128**. Het aantal subnetten dat je kan hebben, is beperkt tot een waarde uit de lijst **2, 4, 8, 16, 64**. Bovendien moet het product van stapgrootte en aantal netwerken altijd 256 opleveren. Alle andere rekenkundige mogelijkheden zijn in de praktijk niet mogelijk.

? Je vertrekt van het netwerk klasse C (niet privé) **201.66.54.0/24**. Je splitst dit netwerk in twee delen. Noteer de gegevens van het IP adres per subnet, de range per subnet, het broadcastadres en het subnetmasker in verkorte vorm.

Je past het bovenstaand stappenplan op de gelijkaardige situaties, bijvoorbeeld voor 4 of 8 subnetten toe. Hieronder vind je nog een voorbeeld.

### 2.2.2 De verbinding tussen twee routers

Het toekennen van IP adressen aan het netwerk tussen twee routers, is een klassiek voorbeeld van het voordeel van subnetting. Immers in dat netwerk heb je één (UTP-)kabel die beide routers met elkaar verbindt en daardoor één IP adres per verbonden poort van de router. Dat IPadres is telkens het IP adres van de gateway in dat netwerkdeel.

In totaal heb je dus vier IP adressen nodig, naast slechts twee IP adressen om beide routers te verbinden, moet je nog beschikken over IP adres van het volledig netwerk en over het broadcastadres.

De stapgrootte bij subnetting is dan 4. Je gebruikte hiervoor **twee bits** van rechts te tellen. Omdat dit gaat over het aantal IP adressen, zijn de twee overeenkomende bits van het subnetmasker hiervoor gelijk aan *nul*. De overige  $8 - 2 = 6$  bits die oorspronkelijk *nul* waren, maken nu deel uit van het aantal subnetten en worden dus op *een* gezet. In totaal heb je nu  $24 + 6 = 30$  bits die '1' zijn.

Het subnetmasker verkort is dan **/30**. Het subnetmasker volledig binair uitgeschreven is **11111111. 11111111. 11111111. 11111100** wat decimaal gelijk is aan **255.255.255.252**.

Het aantal subnetten dat je kunt maken is gelijk aan  $\frac{256}{4} = 64$ . Hieronder vind je de tabel met een aantal voorbeelden genomen uit het begin, eind en tussenin.

? Bepaal van het 32<sup>ste</sup> subnet het IPadres van het subnet dat twee routers met elkaar verbindt, het broadcastadres en de range van toekenbare IPv4 adressen. Je vertrekt van het privénetwerk 192.168.55.0/24

De onderstaande tabel is analoog aan het hoger beschreven stappenplan opgebouwd. Je moet dit voor gelijkaardige probleembeschrijvingen kunnen opstellen.

Nr sub-net	IP adres van het netwerk	Range van bruikbare IP adressen	Broadcastadres	SNM <sup>2</sup>
1	192.168.55.0	192.168.55.1 tot 192.168.55.2	192.168.55.3	/30
2	192.168.55.4	192.168.55.5 tot 192.168.55.6	192.168.55.7	/30
3	192.168.55.8	192.168.55.9 tot 192.168.55.10	192.168.55.11	/30
4	192.168.55.12	192.168.55.13 tot 192.168.55.14	192.168.55.15	/30

*vervolg op volgende pagina*

Nr sub-net	IP adres van het netwerk	Range van bruikbare IP adressen	Broadcastadres	SNM <sup>2</sup>
30	192.168.55.116	192.168.55.117 tot 192.168.55.118	192.168.55.119	/30
31	192.168.55.120	192.168.55.121 tot 192.168.55.122	192.168.55.123	/30
32	192.168.55.124	192.168.55.125 tot 192.168.55.126	192.168.55.127	/30
33	192.168.55.128	192.168.55.129 tot 192.168.55.130	192.168.55.131	/30
62	192.168.55.244	192.168.55.245 tot 192.168.55.246	192.168.55.247	/30
63	192.168.55.248	192.168.55.249 tot 192.168.55.250	192.168.55.251	/30
64	192.168.55.252	192.168.55.253 tot 192.168.55.254	192.168.55.255	/30

Tabel 2.4: Overzicht van de IP verdeling bij subnetting tussen twee routers in een klasse c netwerk

### 2.2.3 Een subnet voor 14tal pc's

De vraagstelling bespreekt het aantal toestellen per subnet. Je hebt 14 IP adressen nodig voor de toestellen. Je telt er twee bij (IP netwerk en broadcastadres). In totaal heb je dus 16 IP adressen nodig. 16 is een macht van 2 ( $16 = 2^4$ ), dus je mag die waarde behouden. De **stapgrootte** is **16**. Het aantal subnetten is gelijk aan  $\frac{256}{16} = 16$ . Voor 16 subnetten te beschrijven heb je 4 bits nodig. Deze 4 bits maken deel uit van het netwerkdeel en zijn bij het subnetmasker dus gelijk aan '1'. De overblijvende bits, 4 want  $8 - 4 = 4$  zijn dan gelijk aan binair 0. Het subnetmasker (verkorte vorm) is dan  $/(24 + 4) = /28$ .

Analoog aan hierboven kan je nu voor elk subnet bepalen wat de grenswaarden en wat de mogelijke IP adressen voor een gegeven toestel kunnen zijn.



Nr sub-net	IP adres van het netwerk	Range van bruikbare IP adressen	Broadcastadres	SNM <sup>3</sup>
1	192.168.55.0	192.168.55.1 tot 192.168.55.14	192.168.55.15	/28
2	192.168.55.16	192.168.55.17 tot 192.168.55.30	192.168.55.31	/28
3	192.168.55.32	192.168.55.33 tot 192.168.55.46	192.168.55.47	/28
4	192.168.55.48	192.168.55.49 tot 192.168.55.62	192.168.55.63	/28
9	192.168.55.128	192.168.55.129 tot 192.168.55.142	192.168.55.143	/28
10	192.168.55.144	192.168.55.145 tot 192.168.55.158	192.168.55.159	/28
11	192.168.55.160	192.168.55.161 tot 192.168.55.176	192.168.55.175	/28
14	192.168.55.208	192.168.55.209 tot 192.168.55.221	192.168.55.223	/28
15	192.168.55.224	192.168.55.225 tot 192.168.55.238	192.168.55.239	/28
16	192.168.55.240	192.168.55.241 tot 192.168.55.254	192.168.55.255	/28

Tabel 2.6: Overzicht van de IP verdeling bij subnetting met 14 toestellen per subnet

### 2.2.4 En verder...

Je bent nu in staat om analoge oefeningen te maken. Onthoud de basisregels:

**netwerken of toestellen** Gaat de vraagstelling over aantal subnetten (bits van links te tellen) of over het aantal toestellen (bits van rechts te tellen). Het aantal toestellen vermeerder je met twee voor IPadres van het netwerk en voor het broadcastadres.

**Macht van 2** Bepaal het aantal bits  $n$  zodat  $2^n$  de eerst volgende macht van 2 te nemen die gelijk is of groter dan het aantal subnetten of totaal aantal IP adressen. De geldige waarden voor  $n$  zijn:  $0 \leq n \leq 8$ .

### 2.2.5 Wat moet je weten of kunnen?

Je krijgt op de overhoring analoge vragen als de typevragen hierboven.

- ? Deel een gegeven netwerk 192.168.0.0/24 in 8 gelijke subnetten in. Vermeld IP adres van netwerk, broadcastadres, de range van bruikbare IPadressen en het subnetmasker onder verkorte notatie
- ? Deel een gegeven netwerk 192.168.55.0/24 in subnetten zodat elk subnet tussen 50 en 60 toestellen kan bevatten. Vermeld IP adres van netwerk, broadcastadres, de range van bruikbare IPadressen en het subnetmasker onder verkorte notatie

#### Opdracht 2

Werk de bovenstaande typevragen volledig schriftelijk uit.  
*Deze oefening werd in de klas gemaakt.*

*Opdracht 2: Oefeningen op subnetten*

### 3 Werken met IPv6

**Doelstelling:** 3.1.12 De mogelijke technieken van adressering in een actuele netwerkar-chitectuur toelichten.

**Doelstelling:** 3.1.13 De begrippen subnet en subnetmasker en de functie ervan toelichten.

Dit cursusdeel wil enkele basisprincipes toelichten zonder volledig te willen zijn. Het volstaat voor een eerste kennismaking. Als achtergrondinformatie kan je de bron op <https://4sysops.com/archives/ipv6-part-1-get-started-now/>, geconsulteerd op 14 januari 2020, gebruiken.



<http://www.steves-internet-guide.com/ipv6-guide/>



<https://pcmweb.nl/artikelen/internet/alles-over-het-verschil-tussen-ipv4-en-ipv6/>



[https://www.youtube.com/watch?v=bkLs5\\_geTM4](https://www.youtube.com/watch?v=bkLs5_geTM4)



<https://www.youtube.com/watch?v=irhS0ASkvy8> dit filmpje geeft je basisinformatie



<https://www.youtube.com/watch?v=eMe88FqiPso> voor een algemene inleiding, inclusief EUI-64 en de opbouw van globale adressen.



[https://www.ripe.net/participate/member-support/lir-basics/ipv6\\_reference\\_card.pdf](https://www.ripe.net/participate/member-support/lir-basics/ipv6_reference_card.pdf)

#### 3.1 Het overzicht van de basisbegrippen

Begrip	Omschrijving
ISP	Een <b>ISP</b> , voluit <b>Internet Service provider</b> , is de <b>organisatie</b> die je een IP adres toekent. Voorbeelden in België zijn <b>Telenet</b> en <b>Proximus</b> .
DUID	<b>DUID</b> , voluit <b>DHCP Unique Identifier</b> , identificeert de client computer, en dus niet enkel de netwerkinterface en wordt gebruikt bij DHCP v6
IAID	<b>IAID</b> , voluit <b>Identity Association Identifier</b> , identificeert <b>wel</b> de netwerkinterface

*vervolg op volgende pagina*

Begrip	Omschrijving
EUI-64	<b>EUI-64</b> , voluit <b>Extended Unique Identifier</b> , is de techniek waarmee je een 48 bits <b>MAC adres</b> omvormt tot een unieke <b>64 bits</b> identificatie van een computertoestel ( <i>host gedeelte</i> ).
Statefull	<b>statefull</b> is een <b>techniek</b> waarbij de <b>handeling verband</b> houdt met <b>eerdere handelingen</b> of <b>bekomen en/of opgeslagen informatie</b> . Afhankelijk van de context kunnen dat <b>cookies</b> of <b>sessie variabelen</b> zijn bij <b>webverkeer</b> ,
Stateless	<b>Stateless</b> is een <b>techniek</b> waarbij de handeling onafhankelijk is en geen verband houdt met bijkomende informatie of opgeslagen informatie.
SLAAC	<b>SLAAC</b> , voluit <b>Stateless Address Autoconfiguration</b> , is een techniek om een <b>IPv6 adres</b> aan een <b>netwerkkkaart</b> toe te kennen <b>zonder</b> enige <b>informatie</b> van het <b>netwerk</b> en er is ook <b>geen DHCP server</b> nodig. Het <b>besturingssysteem</b> van de computer berekent een <b>link local adres</b> dat start met <b>FE80::</b> en berekent een hostgedeelte op basis van MAC adres.
Neighbor Discovery Protocol	<b>Neighbor Discovery Protocol</b> is een IPv6 protocol om informatie op het netwerk, waar onder de configuratie van lokale verbindingen, de <b>DNS servers</b> en de routergateways, te verzamelen. Het bestaat onder andere uit <b>router solicitation</b> en <b>router advertisement</b> .
router solicitation	Een <b>router solicitation</b> is onderdeel van <b>Neighbor Discovery Protocol</b> waarbij de clientcomputer bij het opstarten probeert om de verschillende routers via een multicast op te sporen. Bij <b>IPv6</b> wordt het adres <b>FF02::2</b> gebruikt. Bij <b>IPv4</b> wordt het multicastadres <b>224.0.0.2</b> gebruikt. <sup>1</sup>
router advertisement	Een <b>router advertisement</b> is onderdeel van <b>Neighbor Discovery Protocol</b> waarbij de routers de gevraagde netwerkinformatie aan de clientcomputer via een <b>unicast bericht</b> doorgeven. Op geregelde tijdstippen zal de router een <b>multicast</b> bericht naar <b>alle</b> lokale <b>host</b> doorsturen met updates van de netwerkconfiguratie. Bij <b>IPv6</b> wordt het adres <b>FF02::1</b> gebruikt. Bij <b>IPv4</b> wordt het multicastadres <b>224.0.0.1</b> gebruikt

vervolg op volgende pagina

<sup>1</sup><https://www.oreilly.com/library/view/internet-core-protocols/1565925726/ch05s01s04s04.html> , geconsulteerd op 2021-01-17

Begrip	Omschrijving
neighbor solicitation	Een <b>neighbor solicitation</b> is protocol waarbij onder andere een computer kan controleren of er nog <b>andere nodes</b> zijn die ook zijn eigen unicast adres gebruiken. Deze stap is nodig om dat het niet uit te sluiten is dat door toeval toch twee computers hetzelfde IP adres zouden hebben.
unicast	Een <b>unicast</b> is een vorm van <b>communicatie</b> waarbij <b>één</b> toestel met <b>één</b> andere toestel in verbinding staat. Dit is de meest voorkomende situatie. Samengevat is het een <b>één op één</b> communicatievorm.
anycast	Een <b>anycast</b> is een <b>communicatievorm</b> waarbij <b>één toestel</b> in <b>verbinding</b> staat met <b>één toestel uit een groep</b> van <b>gelijkaardige</b> . Samengevat is het een <b>één op één uit veel</b> communicatievorm. Vaak zal de communicatie gevoerd worden door het toestel dat het eerst bereikt wordt en/of het toestel dat het eerst zal reageren. Dit principe wordt bijvoorbeeld toegepast bij <b>DNS servers</b> en maakt vooral gebruik van <b>UDP</b> als communicatieprotocol op laag <b>vier</b> van het <b>OSI model</b> .
multicast	Een [ <b>multicast</b> ] is een communicatievorm waarbij <b>één toestel communiceert</b> met <b>veel</b> (maar niet noodzakelijk met alle) toestellen van een netwerk(deel). Samengevat is het een <b>één op veel</b> communicatievorm. Een klassiek voorbeeld is een <b>livestream</b> van bv een concert dat door één bron naar een aantal toestellen wordt gestuurd. Deze communicatievorm bestaat ook in IPv4 en hiervoor werden IP-adressen uit klasse D gebruikt.
broadcast	Een <b>broadcast</b> is een communicatievorm was waarbij de communicatie van <b>één toestel</b> naar <b>alle andere toestellen</b> op eenzelfde <b>netwerk(-deel)</b> wordt gestuurd. Samengevat is het een <b>één op allen</b> communicatievorm. Deze communicatievorm is <b>enkel</b> in <b>IPv4</b> bruikbaar en in IPv6 vervangen door <b>multicast</b> . Een broadcast gaf veel netwerkbelasting. Het werd door een hub en een switch doorgegeven maar niet door een router.
prefix	Een <b>prefix</b> , soms vertaald als <b>voorvoegsel</b> , is het <b>netwerkgedeelte</b> van een IPv6 adres. Dit zijn de <b>64 bits</b> van <b>links</b> te tellen. Bij <b>publieke adressen</b> wordt het prefix door de <b>ISP</b> toegekend.

*vervolg op volgende pagina*

Begrip	Omschrijving
suffix	Een <b>suffix</b> , soms vertaald als <b>achtervoegsel</b> , is het <b>hostgedeelte</b> van een IPv6 adres. Dit zijn de <b>64 bits</b> van <b>rechts</b> te tellen. Dit kan <b>willekeurig</b> zijn of door <b>EUI-64</b> afgeleid uit het MAC adres.

Tabel 3.2: Overzicht van de basisbegrippen

## 3.2 MultiMedia verkenning

Via een gerichte zoektocht op Internet naar geschikt multimedia materiaal, lukt de verwerking van leerstof, zowel als inleiding als nadien bij het begrijpen en instuderen, beter. <sup>2</sup>

Een korte **inleiding** van ongeveer **2 minuten** vind je op <https://www.youtube.com/watch?v=-Uwj32NvVA>.

Een goede, iets langere **inleiding** op IPv6 krijg je op <https://www.youtube.com/watch?v=aor29pGh1FE>. In het filmpje herhalen ze kort het aantal beschikbare IPv4 en IPv6 adressen, vind je de **vergelijking** tussen **NAT** en het nummer in een appartementsblok en wordt de **kostprijs** van de **omschakeling** van IPv4 naar IPv6 zonder dadelijk zichtbaar een meerwaarde voor de eindgebruiker, als reden aangehaald waarom op dit ogenblik niet alle Internet Service Providers, zoals Telenet en Proximus in België, volledig naar IPv6 omgeschakeld zijn.

Een visuele inleiding krijg je op <https://www.youtube.com/watch?v=uJbM-GsbB4w>. Het een gesproken PowerPoint en duurt 20 minuten.

Het filmpje <https://www.youtube.com/watch?v=irhS0ASkvy8> is een inleiding die door een zes-tal leerlingen aanbevolen werd.

Het filmpje <https://www.youtube.com/watch?v=M1v1-AEHC1E> herhaalt de leerstof en gebruikt de spreker de **command line interface** om een aantal pingcommando's te demonstreren.

Voor minstens één leerling van de klas was [https://www.youtube.com/watch?v=dUmhZ0nz\\_qc](https://www.youtube.com/watch?v=dUmhZ0nz_qc) goed om het **verschil** tussen de IPv4 en IPv6 beter uit te leggen. Het is ook een alternatieve manier om **binaire getallen** naar **hexadecimaal** kan converteren en legt het de **zero compression** en **zero suppression** duidelijk uit. Het filmpje start met een **grafiek** van het **gebruik van IPv6** in functie van de **tijd**.

Een leuke afwisseling vormt [https://www.youtube.com/watch?v=pUrdDelghwA&ab\\_channel=IDGTECHtalk](https://www.youtube.com/watch?v=pUrdDelghwA&ab_channel=IDGTECHtalk) met een *hoog South Park gehalte*. Het is een goede inleiding tot de lessenreeks van IPv6 maar geeft geen diepgaandere extra inzichten mee.

<sup>2</sup>Deze tekst is de verwerking van de enquêtes die de leerlingen van 6NIT op 13 januari 2021 ingediend hebben.

### 3.3 Inleiding

Het aantal beschikbare adressen IPv4 is uitgeput <sup>3</sup> <sup>4</sup>. Via technieken zoals **subnetting** en **NAT (Network address translation)** kan men zich nog wat redden, maar het is maar een tijdelijke oplossing met andere nadelen.

Ook de opkomst van **IoT (Internet Of Things)**, zorgt voor een enorme toename van het aantal IP adressen. Met **NAT** en een correcte configuratie van je **router** heb je bijvoorbeeld nog altijd je IP-camera thuis, maar de voorkeur geef je beter aan een rechtstreeks IP adres aan het randapparaat.

De oplossing ligt in het verhogen van het aantal **bits** voor het adres van het individueel toestel. Van **32 bits** is de stap gemaakt naar **128 bits**, vier keer **meer** bits.

Die overgang van IPv4 (32 bits adressering) naar IPv6 (128 bits adressering) laat toe om elk toestel rechtstreekse netwerktoegang aan te bieden.

Door de verhoging van het aantal bits, zijn er nu <sup>2</sup><sup>98</sup> meer adressen dan bij IPv4. <sup>5</sup>. Een protocol zoals ARP heb je niet meer nodig, en ook valt de noodzaak weg om met NAT te werken.

Een IP adres vraag je op met het Windows commando **ipconfig /all** . Onder Linux met het commando **ifconfig** <sup>6</sup> of **ip addr show** .

Een voorbeeld van een IPv6 adres zie je op onderstaande figuur 3.1:

In de computer zit één fysieke netwerkkaart. De installatie van software zoals **Virtual box**, **VMware**, bepaalde anti-virusprogramma's of **VPN verbindingen** zorgen voor bijkomende fictieve netwerkkaarten, elk met hun eigen instellingen zoals IP adres en MAC adres (ook wel **fysical address** of **fysisch adres** geheten).

Bij IPv6 merk je dat je ook voor eenzelfde interface verschillende IPv6 adressen hebt (onderkant van de figuur 3.1 op pagina I-20). Een *gewoon* adres dat met **2001** begint en een *link local* adres dat met **fe80** begint. Hieronder vind je de verklaring.

### 3.4 De kenmerken van een IPv6 adres

#### 3.4.1 De bouw van een IPv6 adres

Een IPv6 adres heeft volgende **kenmerken**: <sup>7</sup>

- Het bestaat uit **128 bits**. Dit zijn omgerekend 16 bytes , 32 hexadecimale tekens
- Het wordt voorgesteld onder **hexadecimale** vorm

<sup>3</sup><https://arstechnica.com/information-technology/2014/06/with-the-americas-running-out-of-ipv4-its-official-the-> , geconsulteerd op 2021-01-07

<sup>4</sup><https://itdaily.be/nieuws/infrastructuur/europese-ipv4-adressen-zijn-opgebruikt/> , geconsulteerd op 2021-01-07

<sup>5</sup>98 = 128 – 32

<sup>6</sup>dit commando is nog wel het meest bekende maar geraakt verouderd.

<sup>7</sup>Vergelijk dit met de kenmerken van IPv4

```

Connection-specific DNS Suffix . : Huisnet.local
Description . . . . . : Realtek PCIe GBE Family Controller
Physical Address. . . . . : 8C-89-A5-54-52-DC
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . : fe80::e4ef:11f:cb55:cb47%24(Preferred)
IPv4 Address. . . . . : 192.168.123.110(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : zaterdag 10 februari 2018 9:52:07
Lease Expires . . . . . : zaterdag 17 februari 2018 9:52:07
Default Gateway . . . . . : 192.168.123.254
DHCP Server . . . . . : 192.168.123.254
DHCPv6 IAID . . . . . : 42764709
DHCPv6 Client DUID. . . . . : 00-01-00-01-1E-5D-07-D5-8C-89-A5-54-52-DC
DNS Servers . . . . . : 192.168.123.254
                        8.8.8.8
NetBIOS over Tcpip. . . . . : Enabled

.

Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Teredo Tunneling Adapter
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2001:0:9d38:6abd:2c7b:16d5:3f57:8491(Preferred)
Link-local IPv6 Address . . . . : fe80::2c7b:16d5:3f57:8491%17(Preferred)
Default Gateway . . . . . : ::
DHCPv6 IAID . . . . . : 285212672
DHCPv6 Client DUID. . . . . : 00-01-00-01-1E-5D-07-D5-8C-89-A5-54-52-DC
NetBIOS over Tcpip. . . . . : Disabled

```

Figuur 3.1: Voorbeeld van IP instellingen

- Het wordt gegroepeerd in **8 blokjes** van **4** hexadecimale tekens
- Het wordt gescheiden door een **dubbele punt**

Vergelijk deze kenmerken met die voor een IPv4 adres. Er zijn geen 'kenmerken' voor een subnetmasker. Dit bestaat nog altijd bij IPv6 maar enkel in verkorte vorm zoals **/64**.

Het standaard **subnetmasker** is **/64**. **/64** noemt men ook wel **subnet prefix**. **/48** noemt men ook wel **route prefix**.

### 3.4.2 Het MAC adres als basis van een uniek hostgedeelte

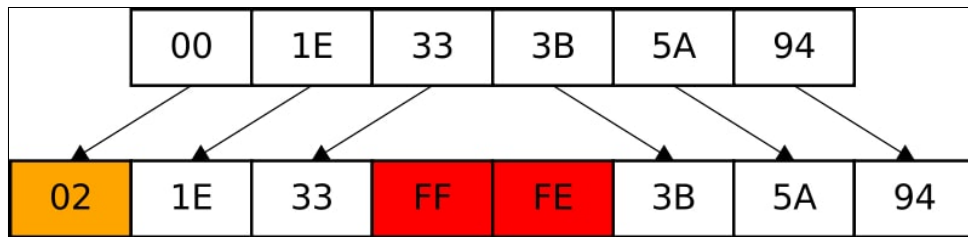
Je kan op basis van het **MAC adres** een uniek hostgedeelte opbouwen.

**EUI-64**, voluit **Extended Unique Identifier**, is de techniek waarmee je een 48 bits **MAC adres** omvormt tot een unieke **64 bits** identificatie van een computertoestel (*host gedeelte*).

De interface ID, op de figuur hieronder vertaalt als 'hostgedeelte' bevat standaard 64 bits, dus 8 bytes. Een van de mogelijke identificietechnieken is gesteund op het **MAC-adres** dat naar een **EUI-64** adres wordt omgevormd. Een MAC adres bevat 12 hexadecimale tekens of 6 bytes. De onderstaande figuur toont duidelijk hoe de omvorming van een MAC adres (6 bytes) naar een EUI-64 standaard. Zoals je op de figuur ziet, ondergaat het MAC adres volgende aanpassingen

- Na de derde byte, dus in het midden, wordt de code **FF FE** toegevoegd
- De 7de bit wordt geïnverteerd. In het voorbeeld wordt 00x omgevormd tot O2x





Het inventeren van de 7de bit (of de tweede bit van rechts te tellen) zorgt -in decimale omrekening- een verschil van twee eenheden. We splitsen de byte in twee gelijke delen, elk om te zetten in een hexadecimaal getal. In het rechterhexadecimaal getal doen we nu de conversie. We schrijven die 4 bits binair uit, berekenen de decimale en vervolgens hexadecimale waarden. Het inverteren van die bit zorgt voor een verandering met twee eenheden (decimaal gerekend).

- als die bit '0' is en dus nu "1" wordt, verhoogt het overeenkomend getal met 2 eenheden.
- als die bit van '1' naar '0' veranderd wordt, verlaagt het overeenkomend getal met 2 eenheden.

Deze techniek op basis van het MAC adres levert ongetwijfeld een volledig unieke identificatie. Alleen is dit niet altijd wenselijk, bijvoorbeeld voor **privacy** redenen.

Daarom wordt vaak een willekeurige **reeks van 64 bits**, gebruikt waarbij er geen band meer is met het MAC adres, als identificatie van het individueel toestel. Via de techniek van **neighbor solicitation** kan het toestel nagaan of hetzelfde IPv6 adres in het netwerk al aanwezig is.

Voor multimediamateriaal en verdere verduidelijking vind je hieronder enkele links, geldig op 17 januari 2021:

- <https://www.youtube.com/watch?v=gT3A4v6dk2g>
- <https://www.youtube.com/watch?v=u6IdXMju-9c>

### 3.4.3 Grafische voorstelling van het IP adres

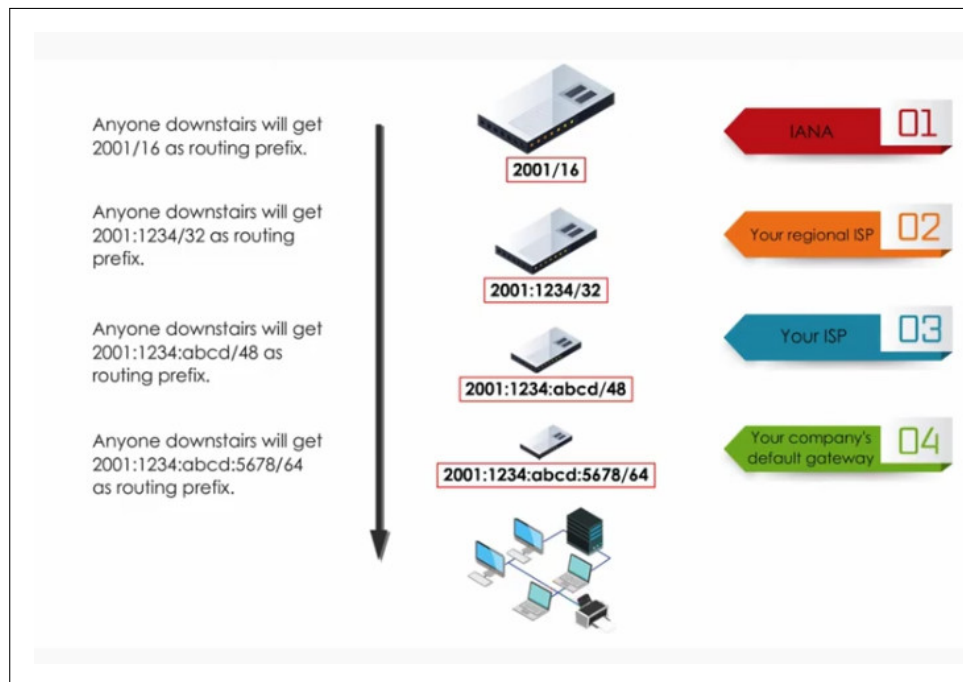
Op de onderstaande figuur 3.2 zie je de **grafische voorstelling** van het IP adres, dat uit twee delen bestaat:

- de **prefix**: het netwerkgedeelte dat 64 bits bevat en zo nodig verder kan opgesplitst worden in :
  - het **global unicast** adres dat door je **ISP** wordt toegekend en **48 bits** groot is
  - het **subnet** van **16 bits** dat kan gebruikt worden voor **opsplitsing** van het netwerk in verschillende **subnetten**.
- de **suffix**: het **hostgedeelte** dat **64 bits** groot is en de **identificatie** van het individueel toestel in het netwerk is.

netwerkgedeelte standaard 64 bits		hostgedeelte standaard 64 bits
global unicast adres 48 bits	subnet 16 bits	

Figuur 3.2: De grafische voorstelling van het IPv6 adres

De onderstaande figuur 3.3 leert ons de bijdrage van de verschillende organisaties die een rol spelen bij de toekenning van globale IP adressen. Onze providers, zoals **Proximus** en **Telenet** bepalen de eerste **48 bits** van het globaal IP adres.



Figuur 3.3: De opbouw van een global unicast adres

a

<sup>a</sup><https://www.youtube.com/watch?v=eMe88FqiPso>

### 3.4.4 DHCP v6

Bij gebruik van `ipconfig /all` zie je de vermelding van **DHCPv6 IAID** en **DHCPv6 client DUID**. (zie bijvoorbeeld figuur 3.1 op pagina I-20) Je herinnert je wellicht nog dat bij **DHCPv4** het **MAC adres** en optioneel een **client ID**, maar dit is amper toegepast en ook niet in de cursus vermeld.

Bij **DHCPv6 verplicht** het gebruik van de **client ID**. Het is uit twee delen opgebouwd:

- **DHCP Unique Identifier**, afgekort **DUID**. Deze parameter identificeert de client computer, en dus niet enkel de netwerkinterface
- **Identity Association Identifier**, afgekort **IAID**. Deze parameter identificeert **wel** de netwerkinterface

### 3.4.5 Het weglaten van de voorloophnullen.

In een hexadecimaal adres kan verschillende keren de waarde '0' voorkomen. Je mag in bepaalde gevallen dit hexadecimaal teken weglaten. Vergelijk met het decimaal rekenen:

- het decimale getal **5** is gelijk aan **000005**. Het doet er niet toe hoeveel keer het cijfer nul aan de linkerkant wordt toegevoegd. De getalwaarde verandert niet: vijf (eenheden) blijft vijf (eenheden). deze 'nullen' noemen we de **voorloophnullen**.
- het decimale getal **5** is **niet gelijk** aan **50** noch aan **500**. Dan zou immers vijf van 'eenheid' naar 'tiental' of naar 'honderdtal' veranderen.
- het decimale getal **5002** is **niet gelijk** aan het decimale getal **52** want een 'nul' mag je ook niet zo maar tussen twee andere cijfers weglaten.
- Bij een **kommagetal** zoals **0,5** mag je dan weer wel een 'nul' toevoegen aan de rechterkant want **0,5 is gelijk aan 0,50000**.

Deze principes uit de lagere school passen we toe op een hexadecimaal IP adres. Ook daar laten we de voorloophnullen weg. Bijkomend mogen we per IPv6 adres **eenmalig** opeenvolgende reeksen van '0000' vier hexadecimale waarden 0 bij elkaar, ook weglaten en vervangen door ::

We werken beide principes uit op volgende voorbeelden: **2001:0DB8:0021:0111:0000:0000:0000:0000/64**. We gaan als volgt te werk:

1. Alle voorloophnullen mogen weg. We bekomen dan **2001:DB8:21:111::/64**
2. De opeenvolgende reeks van 4 voorloophnullen mogen ook vervangen éénmalig per IP adres worden door ::. Dus het IPv6 adres wordt dan **2001:DB8:21:111::/64**

## Opdracht 3

Hieronder vind je een aantal IPv6 adressen. Vereenvoudig ze zoveel mogelijk

- 2001:cdba:0000:0000:0000:0000:3257:9652 <sup>a</sup>
- 2001:cdba:0000:0000:0000:3257:0000:9652 <sup>b</sup>
- 2001:cdba:0000:0000:3257:0000:0000:9652 <sup>c</sup>

Hieronder vind je een aantal vereenvoudigde IPv6 adressen. Schrijf ze volledig uit.

- 2001:db8::7 <sup>d</sup>
- 2001:db8:0:45::20 <sup>e</sup>

Op internet vind je nog talloze andere voorbeelden.

---

<sup>a</sup>2001:cdba::3257:9652

<sup>b</sup>2001:cdba::3257:0:9652

<sup>c</sup>2001:cdba:0:0:3257::9652 of 2001:cdba::3257:0:0:9652 want beide oplossingen zijn correct.

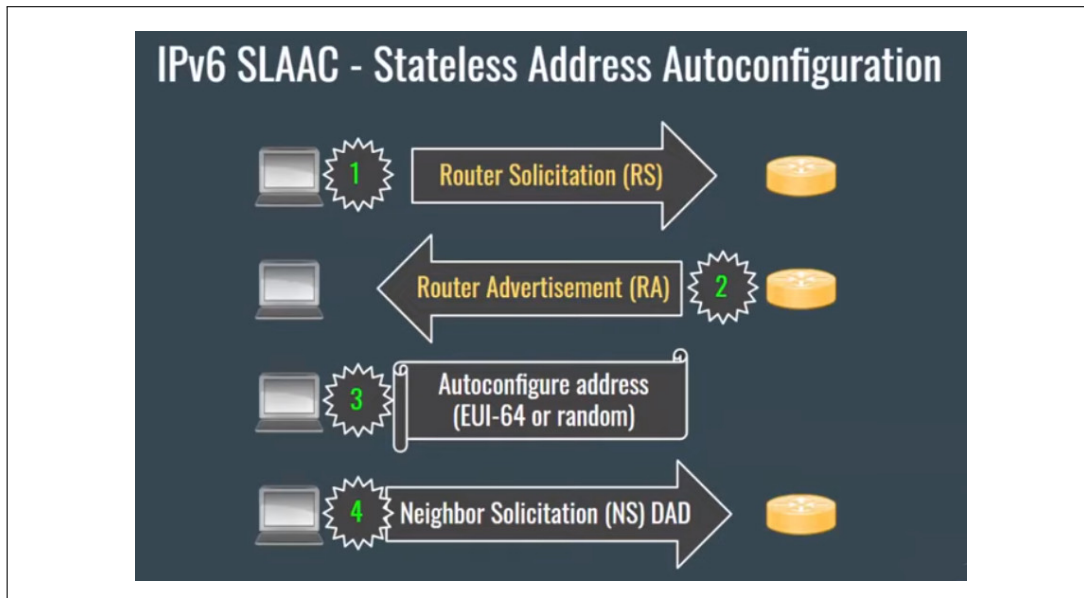
<sup>d</sup>2001:0db8:0000:0000:0000:0000:0000:0007

<sup>e</sup>2001:0db8:0000:0045:0000:0000:0000:0020

*Opdracht 3: Vereenvoudig volgende IPv6 adressen*

### 3.4.6 SLAAC

**SLAAC** staat voor **Stateless Address Autoconfiguration** en is een techniek om een IPv6 adres aan een netwerkkaart toe te kennen. **Stateless** betekent dat deze techniek start zonder enige informatie van het netwerk en er is ook geen DHCP server nodig. Het besturingssysteem van de computer berekent een **link local adres** dat start met **FE80::** en berekent een hostgedeelte op basis van MAC adres.



Figuur 3.4: De verschillende stappen van SLAAC

a

<sup>a</sup><https://www.youtube.com/watch?v=z7A13P8ShM8>

IPv6 SLAAC			
RFC 4861 Neighbor Discovery - SLAAC - ICMPv6			
Message	Source address	Destination address	Type
Router Solicitation (RS) 1	unspecified address :: /128	all-routers multicast FF02::2	133
Router Advertisement (RA) 2 <ul style="list-style-type: none"> <li>sent periodically,</li> <li>sent in response to a router solicitation (RS)</li> </ul>	router link-local FE80::x	all-nodes multicast FF02::1	134
	IPv6 prefixes (one or more)	2000:1234:ABCD:EF22:: /64	
	Router lifetime information	0 (not default), 1 - 9000 seconds	
	flag information	M = managed, 0 = other (DHCPv6)	
	gateway / source address	FE80::x	

Figuur 3.5: De verschillende stappen van SLAAC

a

<sup>a</sup><https://www.youtube.com/watch?v=z7A13P8ShM8>

### 3.5 De verschillende types van een IPv6 adres

We onderscheiden drie types:

**unicast** : één op één. Dit is een vorm van communicatie waarbij één toestel met één andere toestel in verbinding staat. Dit is de meest voorkomende situatie.

**anycast** : één op één uit veel. Dit is een communicatievorm waarbij één toestel in verbinding staat met één toestel uit een groep van gelijkaardige. Het toestel dat het eerst bereikt kan worden, wordt gekozen. Dit principe wordt bijvoorbeeld toegepast bij **DNS servers** en maakt vooral gebruik van **UDP** als communicatieprotocol op laag vier van het **OSI model**.

**multicast** : één op veel. Dit is een communicatievorm waarbij één toestel communiceert met veel (maar niet noodzakelijk met alle) toestellen van een netwerk(deel). Een klassiek voorbeeld is een **livestream** van bv een concert dat door één bron naar een aantal toestellen wordt gestuurd. Deze communicatievorm bestaat ook in IPv4 en hiervoor werden IP-adressen uit klasse D gebruikt.

Dit verschilt met **broadcast**, dat een communicatievorm was waarbij de communicatie van één toestel naar alle andere toestellen op een netwerk(-deel) wordt gestuurd. Deze communicatievorm is enkel in IPv4 bruikbaar en in IPv6 vervangen door **multicast**. Een broadcast gaf veel netwerkbelasting. Het werd door een hub en een switch doorgegeven maar niet door een router.

### 3.6 De reikwijdte van een IPv6 adres

De **reikwijdte**, synoniem voor **werkgebied** en **bereik** en vertaling voor **scope** is gelijkaardig aan dat van een IPv4.

Bij het toewijzen van een IPv4 adres aan een toestel of knooppunt, stel je de vraag of het adres een privé adres of een publiek adres is. Als je privé-adressen gebruikt, zoals 10.5.6.8, dan blijft het bereik beperkt tot het lokaal netwerk en zal je pakketten nooit een router passeren.

Bij het toewijzen van een IPv6 adres aan een toestel of een knooppunt zullen we altijd een **link local** adres voorzien. Ook de router zal zo'n adres hebben. Bij IPv4 kreeg de (gateway van de) router geen link local adres. Het netwerk **169.254.0.0/16** is voorbehouden voor eindtoestellen.

We onderscheiden volgende **reikwijdtes**:

**global unicast GUA** heeft de volgende kenmerken

- publiek adres
- begint altijd met "2001"
- toegekend door SLAAC, statefull(DHCPv6) of manueel
- routerbaar op het internet

**Unique local ULA** heeft de volgende kenmerken

- lokaal adres (privé adres)
- begint altijd met "FC00::/7"
- dit adres is niet routerbaar op het internet
- dit adres is routerbaar in een lokaal netwerk (zoals een IPv4 privé adres)
- toegekend door SLAAC, statefull(DHCPv6) of manueel

**link local** heeft de volgende kenmerken

- lokaal adres
- begint altijd met "FE80::/10"
- dit adres is niet routerbaar
- vergelijkbaar met een IPv4 APIPA adres (169.254.0.0/16)

**multicast** heeft de volgende kenmerken

- multicast adres: één op veel adres
- begint altijd met "FF00::/8"
- dit adres is routerbaar, zowel intern als op het Internet

### 3.7 Het zone nummer van een IPv6 adres

In de figuur 3.1 op pagina I-20 vind je achter het **link local** adres de waarde **%17** en **%21**. Deze getallen (17 en 21) verwijzen naar het ID-nummer van de zone.<sup>8</sup>

Stel dat je een computer PC01 hebt met twee netwerkkaarten A en B, elke netwerkkaart is verbonden met een eigen netwerkdeel (of subnet). Elke netwerkkaart heeft ook een link local adres. Het is best mogelijk dat de netwerkkaart A van PC01 verbonden is met de netwerkkaart C van PC02. Eveneens is het theoretisch mogelijk dat zowel netwerkkaart A als netwerkkaart C hetzelfde link local adres zou hebben. Om verwarring te vermijden, zal PC01 de **interface index** van netwerkkaart A als **site ID** gebruiken.

Voor site-local adressen, zal het besturingssysteem de **site ID**, ook **scope ID** gebruiken. Als de computer slechts met één site verbonden is, is de ID altijd gelijk aan **1**.

De zone-ID is alleen door de locale host gekend. In de praktijk heb je hier zelden mee te maken en moet je dit niet manueel instellen.

### 3.8 Scripting

Je kan de IP v6 adressen zien via het commando `ipconfig /all`. Je krijgt de output als **address%zone\_ID**

In PowerShell kan je ook `netsh interface ipv6 show address level=verbose` gebruiken.

---

<sup>8</sup><https://4sysops.com/archives/ipv6-tutorial-part-7-zone-id-and-unique-local-ipv6-unicast-addresses/>



### 3.9 Speciale IPv6 adressen

In de onderstaande tabel vind je de speciale IPv6 adressen met uitleg en de verwijzing naar de eventueel overeenkomende waarde bij IPv4.

Begrip	bit	Voorstelling	Ipv4	Verklaring
Onbepaald	00...00	::/128	0.0.0.0	Bronadres enkel te gebruiken voordat er een IP adres is toegekend aan host tijdens het opstartproces
Loopback	00...01	::1/128	127.0.0.1	Door het versturen van een pakketje naar een loopback-adres test je de configuratie van IPv6 op je pc. Bij correcte installatie krijg je altijd een antwoord. Een datapakketje dat naar dat adres gestuurd wordt verlaat de pc niet en zal nooit op het netwerk met bv <b>Wireshark</b> aantoonbaar zijn.
IPv4 mapped	-	::ffff:189.24.65.6	189.24.65.6	Elk IPv4 adres, hier toevallig gekozen voor 189.24.65.6, kan tot een IPv6 adres omgevormd worden
Voorbeeld IP	-	2001:db8::/32	-	Alle voorbeelden van IPv6 zijn afgeleid van dit IPv6 adres. Deze adressen kunnen niet binnen een bestaand netwerk gebruikt worden maar zijn uitsluitend als documentatie bedoeld.
Site local	1111 1110 11	fec0::/10	-	Dit IPv6 adres is alleen binnen een bepaalde <b>organisatie</b> geldig. De overblijvende 54 bits van het netwerkdeel zijn bestemd voor het <b>subnet ID</b> . Dit bepaal je binnen de organisatie zelf. Deze manier van werken wordt bij voorkeur niet meer toegepast en is vervangen door <b>link local</b> adressen.
vervolg op volgende pagina				

Begrip	bit	Voorstelling	Ipv4	Verklaring
Unique local	1111 110	fc00::/7	<ul style="list-style-type: none"> <li>• klasse A: 10.0.0.0/8</li> <li>• klasse B: 172.16.0.0 tot 172.31.0.0/16</li> <li>• Klasse c: 192.168.0.0 tot 192.168.255.0/24</li> </ul>	Deze adressen wordt gerouterd binnen een netwerk van verbonden sites (bv schoolcampus) maar niet op het Internet. Ze vervangen de <b>site local</b> adressen die voorbijgestreefd zijn.
link-local	1111 1110 10	fe80::/10	APIPA 169.254.0.0/16	<p>Een link-local adres is enkel geldig in een <b>netwerksegment</b> (ook <b>link</b> geheten). Het wordt niet door een router doorgegeven.</p> <p>De <b>9<sup>de</sup> bit</b> is op dit moment altijd '1' want dit adres wordt lokaal toegewezen. De waarde '0' wordt niet gebruikt.</p> <p>De volgende 54 bits van het netwerkdeel allemaal '0'. In twee verschillende netwerksegmenten kunnen identieke IPadressen van dit type voorkomen. Bij IPv6 is het verplicht dat een netwerkkaart (ook) over een link-local adres beschikt voor de goede werking van diverse protocollen.</p> <p>Het link local adres blijft behouden als DHCPv6 toch beschikbaar zou zijn. Bij IPv4 is dit niet het geval: het APIPA adres is niet meer bruikbaar, van zodra de DHCP terug IP adressen toekent.<sup>9</sup></p>
vervolg op volgende pagina				

<sup>9</sup>[https://en.wikipedia.org/wiki/Link-local\\_address](https://en.wikipedia.org/wiki/Link-local_address)

Begrip	bit	Voorstelling	Ipv4	Verklaring
<b>Multicastadres</b>	1111 1111	ff00::/8	Elk adres van klasse D (224.0.0.0/4)	<p>Elk IP adres met deze suffix wordt als een multicastadres beschouwd. Dit vervangt bij IPv6 het broadcastadres.<sup>10</sup></p> <p>Speciale gevallen zijn :</p> <ul style="list-style-type: none"> <li>• <b>ff02::1</b> voor alle toestellen op een lokaal netwerksegment. Dit is het <b>link local, alle nodes multicast adres</b></li> <li>• <b>ff02::2</b> voor alle <b>routers</b> op een lokaal netwerksegment.</li> <li>• <b>ff0x::114</b> is het adres dat voor experimenten wordt gebruikt.</li> </ul>
<b>global unicast</b>	001	2001::/3	alle publieke adressen	<p>De eerst drie bits zijn verplicht '001'; De volgende 45 bits vormen de 'global routing prefix'. Samen vormen ze 48 bits en wordt aan een individuele site van een organisatie toegewezen. Eenmaal die koppeling gebeurd is, wordt al het Internet-netwerkverkeer naar de routers van die organisatie gerouterd. De volgende 16 bits worden gebruikt om subnetten binnen die organisatie aan te duiden.</p>
vervolg op volgende pagina				

<sup>10</sup>[https://en.wikipedia.org/wiki/Multicast\\_address#IPv6](https://en.wikipedia.org/wiki/Multicast_address#IPv6)

Begrip	bit	Voorstelling	Ipv4	Verklaring
<b>Terendo</b>	-	2001:0000::/32	-	Dit is een mapped adres dat het gebruik van een IPv6 - tunnel doorheen een IPv4 NAT router mogelijk maakt. Het adres bestaat uit de Terendo-prefix, het IPv4 adres van de server, het IPv4 adres en de verborgen poort van de client en het type van de NAT. Zie ook <a href="http://www.potaroo.net/cgi-bin/ipv6addr">http://www.potaroo.net/cgi-bin/ipv6addr</a> , waar je het IPv6 adres kan ontleden.
<b>Benchmarking</b>	-	2001:0002::/48	-	Ook deze adressen kunnen niet binnen een bestaand netwerk gebruikt worden maar zijn uitsluitend als documentatie bedoeld.
<b>Orchid</b>	-	2001:0010::/28	-	Deze adres kan je enkel binnen lokale netwerken voor experimentele opstellingen gedurende een beperkte tijd (bv labopdrachten voor leerlingen) gebruiken. De routers negeren dergelijke adressen.
<b>6 naar 4</b>	-	2002:::/16	192.88.99.0/24	Een '6 naar 4' gateway voegt het IPv4 adres van de gateway toe aan 2002::/16 en maakt zo een uniek /48 prefix-adres. Het IPv4 adres kan nadien hieruit nog afgeleid worden. Bij IPv4 is er geen equivalent maar het 192.88.99.0/24 is als 6 naar 4 relay anycast adres gereserveerd.

Tabel 3.3: Overzicht van IPv6 adresruimte

## 3.10 Hoe kan je een bruikbaar IP adres aan je computer geven

Bij de verschillende labo's, bijvoorbeeld voor **Windows server 2019**, werden **IPv6** adressen altijd **uitgeschakeld**. In dit cursusdeel willen we **IPv4 uitschakelen** en **experimenteren** met **IPv6**. We starten met het toekennen van een geldig IP adres aan je computer, vertrekkend van de verschillende mogelijkheden (zie gedeelte over de reikwijdte van een IPv6 adres).

Er zijn verschillende types van IPv6 adres.

Een **link local** adres wordt automatisch door je besturingssysteem toegekend.

Een **global unicast** adres komt van je provider. Hoe kan je dit op je pc gebruiken? Je hebt volgende mogelijkheden: <sup>11</sup>

- **zelf ingeven**: In theorie kan je dit zelf invullen maar in de praktijk komt het niet veel voor. De kans op typfouten is te groot
- via de techniek van **Stateless Address Autoconfiguration (SLAAC)** waarbij de router je via een **router advertisement** de nodige gegevens doorstuurt. Zie hiervoor cursusdeel 3.4.6 **SLAAC** op pagina I-25.
- **statefull configuration** door een router IPv6

Een **unique local** adres toekennen doe je als volgt:

- **prefix**: het **netwerkdeel** is als volgt opgebouwd:
  - start met binaire code **1111 110**, omgerekend **FE00 /7**
  - bij **conventie** is het gevolgd door allemaal nullen, zodat je FE80::/64 bekomt. Je kan ook voor de overblijvende bits ( $64 - 7 = 57$ ) bits willekeurig binair **1** of **0** invullen en het bekomen resultaat hexadeximaal uitschrijven.
- **suffix** dit bepaal je via **EUI-64** en je MAC adres of bepaal je volledig willekeurig.

Bij de **netwerkconfiguratie** is het **gatewayadres** voor een host gelijk aan het **link local adres** van de **gateway** van je **router**. Voor toegang tot internet heb je beide adressen nodig <sup>12</sup>

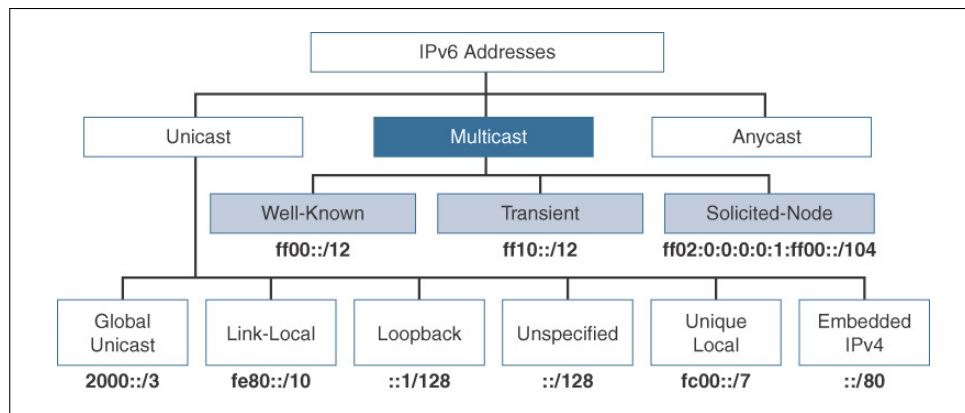
- globaal adres
- link local adres om met de gateway te communiceren

<sup>11</sup><https://meneer.depuydt.eu/tag/eui-64/> , geconsulteerd op 2021-01-17

<sup>12</sup><https://www.youtube.com/watch?v=M1v1-AEHClE> , geconsulteerd op 2021-01-17

### 3.11 Synthesetabel

De onderstaande figuur is een goede samenvatting van de verschillende mogelijkheden. Ontbreekt er één of meerdere gegevens? Laat gerust weten!



Figuur 3.6

*a*

<sup>a</sup>[https://ptgmedia.pearsoncmg.com/images/chap4\\_9781587144776/elementLinks/04fig11\\_alt.jpg](https://ptgmedia.pearsoncmg.com/images/chap4_9781587144776/elementLinks/04fig11_alt.jpg)

### 3.12 Wat moet je weten of kunnen

- ? Bespreek de basisbegrippen zoals je die vindt in de tabel vooraan dit cursusdeel
- ? Bespreek de volgende begrippen: SLAAC, unicast, anycast, multicast, broadcast
- ? Bespreek de volgende adressen met hun reikwijdte en een voorbeeld: global unicast adres, unique local address en link local address
- ? Noteer de kenmerken van een IPv6 adres
- ? Vergelijk de kenmerken van een IPv6 adres met die van een IPv4 adres
- ? Noteer het IPv6 adres van een gegeven computer. *Hiervoor mag je het commando **ipconfig** gebruiken.*
- ? Vereenvoudig een voluit geschreven IPv6 adres waar mogelijk
- ? Noteer het volledig IPv6 adres als je het IPv6 adres in verkorte vorm krijgt
- ? Converteer een MAC adres in een EUI-64 interface ID
- ? Leid het MAC adres af uit een EUI-64 interface ID
- ? Bespreek de 3 mogelijkheden bij de reikwijdte van een IPv6 adres
- ? Bespreek de speciale IPv6 adressen, waaronder onbepaald, loopback, IPv4 mapped, voorbeeld IP, site local, unique local, link local, multicast, global unicast,
- ? Bespreek op welke wijze je een IPv6 adres aan een toestel kan toekennen

*Pagina voor eigen notities.*



## **Deel II**

# **Bijlagen en documentatie**



# 1 Opvolging van Leren-Leren

## 1.1 Overzicht van taken en toetsen in 6 NIT (Beheer)

In de onderstaande tabel vind je het overzicht van de taken en toetsen. Dit blad, aangevuld met je klasnummer, naam en behaalde quotering, dien je samen met de taken en toetsen in. De behaalde quotering vul je zelf aan. Minimaal zet je een kruisje in de correcte kolom.

- **OV** : onvoldoende - niet geslaagd voor deze evaluatie.
- **OK** : voldoende

Nr.	Naam:
-----	-------

Nr	Indienen op	Onderwerp	Toelichting	Taak	Toets	Max.	OV	OK
1	2021-01-13	IPv6	Enquête op Smartschool	x		5		
2	2021-01-20	IPv4 subnetting	Overhoring leerstof		X	20		
3	2021-01-20	IPv6 basis	Overhoring leerstof		X	30		
4	2021-02-02	Inhaaloverhoring	Subnetting en IPv6		X	30		
5	2021-02-04	Module Linux	Console - deel 1		X	10		
6	2021-02-10	Module Linux	Inleiding en installatie		X	10		
7	2021-03-03	Module Linux	Tar commando	X		3		
8	2021-03-03	Module Linux	Console 2b(bookwidgets)		X	7		
9	2021-03-18	Module Linux	GIP 1.4-Stand van zaken 1	X		10		
10	2021-05-19	Module Linux	GIP 1.4- Stand van zaken 2	X		10		

*Pagina voor eigen notities.*



## Internet Protocol Version 6 (IPv6) Basics Cheat Sheet

by Jens Roesen

### IPv6 quick facts

successor of IPv4 • 128-bit long addresses • that's  $2^{96}$  times the IPv4 address space • that's  $2^{128}$  or  $3.4 \times 10^{38}$  or over 340 undecillion IPs overall • customer usually gets a /64 subnet, which yields 4 billion times the IPv4 address space • no need for network address translation (NAT) any more • no broadcasts any more • no ARP • stateless address configuration without DHCP • improved multicast • easy IP renumbering • minimum MTU size 1280 • mobile IPv6 • mandatory IPsec support • fixed IPv6 header size of 40 bytes • extension headers • jumbograms up to 4 GiB

### IPv6 & ICMPv6 Headers

#### IPv6 header

0	8	16	24	32
version	traffic class	flow label		
payload length		next header	hop limit	
source IPv6 address				
destination IPv6 address				

**Version** (4 bits): IP version. Always 6.

**Traffic class** (8 bits): Used for QoS. Like the TOS field in IPv4. [RFC 2474](#).

**Flow label** (20 bits): Used for packet labelling, End-to-end QoS. [RFC 6437](#).

**Payload length** (16 bits): Length of the payload following the header in bytes. Limits packet size to 64 KB.

**Next header** (8 bits): Code for the following extension header or UL protocol. Like protocol type field in IPv4.

**Hop limit** (8 bits): Number of hops until the packet gets discarded. TTL in IPv4.

**Source address** (128 bit): IPv6 source address.

**Destination address** (128 bits): IPv6 destination address.

#### ICMPv6 header

0	8	16	24	32
ICMPv6 type	ICMPv6 code	ICMPv6 checksum		
ICMPv6 data				

**ICMP type** (8 bits): Error messages have a 0 high-order-bit (types 0 to 127), info messages have a 1 high-order-bit (types 128 to 255).

**ICMP code** (8 bits): Further specifies the kind of message along with the type. F.i. type 1 code 4 is "destination port unreachable".

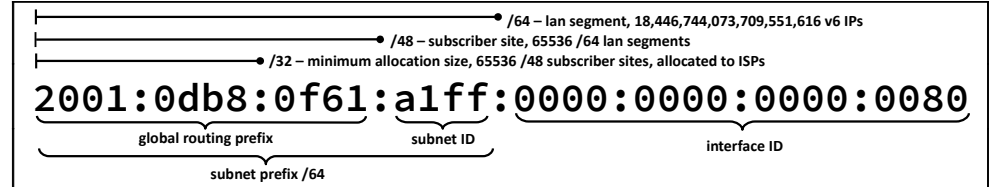
**ICMP checksum** (16 bits): Checksum to prevent data corruption.

### IPv6 Extension Headers (RFC 2460 and it's updates)

Because of the IPv6 header simplification and fixed size of 40 bytes (compared to the IPv4 header with more fields and options and 20 to 60 bytes in size) additional IP options were moved from the main IPv6 header into additional headers. These extension headers (EH) will be appended to the main header as needed. The first 8 bit of each EH identify the next header (another EH or upper layer protocol) following. Only the hop-by-hop header must be examined by every node on the path and, if present, it must be the first header following the main IPv6 header. Every EH must only occur once, only the destination options EH may occur twice - before a routing EH and before the upper layer header.

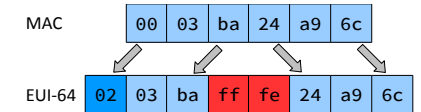
order as suggested in RFC 2460	IPv6 Header	NH 0
	Hop-by-Hop Options (0)	NH 60
	Destination Options (60)	NH 43
	Routing Header(43)	NH 44
	Fragment Header(44)	NH 51
	Authentication Header (51)	NH 50
	ESP Header (50)	NH 60
	Destination Options (60)	NH 6
	TCP Header (6)	

### IPv6 Addresses



IPv6 addresses are written in hexadecimal and divided into eight pairs of two byte blocks, each containing four hex digits. Addresses can be shortened by skipping leading zeros in each block. This would shorten our example address to 2001:db8:f61:a1ff:0:0:0:80. Additionally, once per IPv6 IP, we can replace consecutive blocks of zeros with a double colon: 2001:db8:f61:a1ff::80.

The 64-bit interface ID can/should be in **modified EUI-64** format. A 48-bit MAC can be transformed to an 64-bit interface ID by inverting the 7<sup>th</sup> (universal) bit and inserting a ff and fe byte after the 3<sup>rd</sup> byte. So the MAC 00:03:ba:24:a9:c6 becomes 0203:baff:fe24:a9c6. See [RFC 4291](#) Appendix A and [RFC 4941](#).



### IPv6 Address Scopes

::/128	unspecified address
::1/128	localhost
fe80::/10	link local scope
fec0::/10	site local scope, intended as <a href="#">RFC 1918</a> successor, deprecated in <a href="#">RFC 3879</a>
fc00::/7	unique local unicast scope, <a href="#">RFC 4193</a> , divided into:
fc00::/8	centrally assigned by <i>unknown</i> (see <a href="http://bit.ly/IETFFc00">http://bit.ly/IETFFc00</a> ), routed within a site
fd00::/8	free for all, global ID must be generated randomly, routed within a site
ff00::/8	multicast scope, after the prefix ff there are 4 bits for flags (ORPT) and 4 bits for the scope
::/96	IPv4-compatible IPv6 address, example: ::192.168.1.2, deprecated with <a href="#">RFC 4291</a>
::ffff:0:0/96	IPv4-mapped IPv6 address, example: ::ffff:192.168.2.1, see <a href="#">RFC 4038</a>
2000::/3	global unicast scope, divided into:
2001::/16	/32 subnets assigned to providers, they assign /48, /56 or /64 to the customer
2001::/32	Global Teredo IPv6 Service Prefix.
2001:db8::/32	Reserved for use in documentation. See <a href="#">RFC 3849</a> .
2001:678::/29	Provider Independent (PI) space and anycasting TLD nameservers (f.i. 2001:678:2::/48 for DENIC)
2002::/16	6to4 scope, 2002:c058:6301:: is the 6to4 public router anycast (deprecated with <a href="#">RFC 7526</a> )
3ffe::/16	6Bone scope, returned to IANA with <a href="#">RFC 3701</a> , you should not see these
64:ff9b::/96	prefix used for representing IPv4 addresses in the IPv6 address space, see <a href="#">RFC 6052</a>

### Well Known Multicast Addresses (T-Flag = 0)

ff0X::1	all nodes address (scopes 1 and 2)
ff0X::2	all routers address (scopes 1, 2 and 5)
ff05::1:3	all site-local DHCP servers
ff02::9	all link-local RIP routers
ff02::1:ff/104	solicited-node address, the 24 low-order bits are equal to the interfaces IP 24 low-order bits
ff02::1:2	all link-local DHCP relay agents and servers
ff0X::fb	Multicast Domain Name Service v6 (all scopes)
ff0X::101	Network Time Protocol (all scopes)

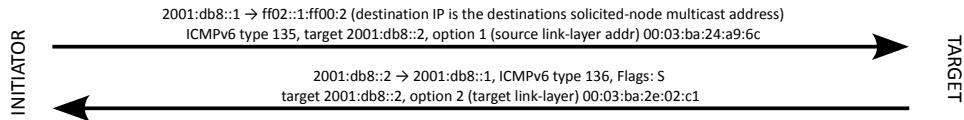
### Multicast Scopes

1	Interface-local	5	Site-local
2	Link-local	8	Organization-Local
3	Admin-local	e	Global

← A "X" in the prefix is a place holder for the scope ↑

### Neighbor Discovery (ND): Neighbor Solicitation (NS) and Neighbor Advertisement (NA)

Neighbor Solicitation (ICMPv6 type 135) messages are sent to determine the link-layer address of a neighbor (multicasts) or to verify that a neighbor is still reachable (unicasts).

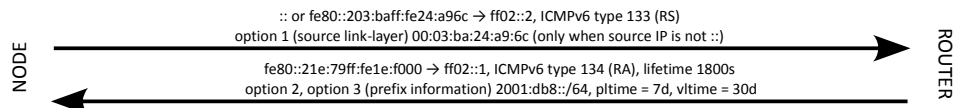


In the example above node 2001:db8::1 wants to reach 2001:db8::2 but does not know the link-layer address of 2001:db8::2. So it sends a NS packet to the solicited-node multicast address of 2001:db8::2 (ff02::1:ff00:0/104 followed by the last 24 bits of the interface ID) along with its own link-layer address and receives a NA (ICMPv6 type 136) packet with the targets link-layer address.

**Duplicate Address Detection (DAD):** To perform DAD the NS message is sent with the unspecified source IP :: and to the solicited-node multicast address of the IP which should be configured. If there is already a node using this desired IP it will answer with a NA packet sent to the all-node multicast address ff02::1.

### Neighbor Discovery (ND): Router Solicitation (RS) and Router Advertisement (RA)

Router Solicitation (RS) packets are sent in order to receive a Router Advertisement (RA) message independently from the periodically sent RAs. This is typical during stateless address autoconfiguration after successful DAD. The source IP used for the RS message can be :: or the link-local IP for this interface.



After receiving the RS message a router sends a RA message to the all-nodes multicast address. The RA message contains, amongst others, information about the router lifetime (time in seconds the router expects to be a default router), all available prefixes and their preferred (pltime) and valid (vlttime) lifetimes. When pltime reaches zero the address becomes deprecated and should not be used for new connections. When the vlttime reaches zero the address becomes invalid.

## Stateless Address Autoconfiguration (RFC 4862) and Stateful Autoconfiguration DHCPv6 (RFC 3315)

**Stateless Address Autoconfiguration (SLAAC)** comes in handy when it's not important which exact address a node uses as long as it's properly routable. SLAAC uses mechanisms of Neighbor Discovery.

Steps taken during SLAAC presuming there were no DAD errors along the way: forming a link-local address → DAD for the link-local address → activating the link-local address and sending RS message(s) to ff02::2 → forming a global address for each received prefix within an RA message with set "autonomous address-configuration flag" → DAD for each tentative global address → addresses become valid and preferred (for pltime > 0). See [RFC 6106](#) for DNS configuration options advertising via RAs.

**DHCPv6** can assign IPs and additional information like DNS/NTP Servers. A client sends a SOLICIT message (type 1) to the All\_DHCP\_Relay\_Agents\_and\_Servers multicast IP ff02::1:2. Servers answer with a ADVERTISE message (2). The client chooses a server, sends a REQUEST message (3) and receives a REPLY message (7) with configuration options. DAD has to be performed for every address received! Alternatively, and in coexistence with SLAAC, DHCPv6 can only provide clients with additional information like DNS and NTP servers. The client sends a INFORMATION-REQUEST message (11) and receives the options in a REPLY message (7). See [RFC 3315](#) for detailed description of DHCPv6 messages and options.

## Connect to IPv6 IPs on the Command Line or in a Browser

CLI	# ssh '2001:db8:dead:f00d:203:baff:fe24:a9c6' # lynx http://[2001:db8:dead:f00d:203:baff:fe24:a9c6] # wget ftp://[2001:db8:dead:f00d:203:baff:fe24:a9c6]
Browser	http://[2001:db8:dead:f00d:203:baff:fe24:a9c6]

## IPv6 and DNS (RFC 3596)

The IPv6 equivalent to the IPv4 A Resource Record is the AAAA RR. No big difference there. The A6 RR with additional fields for prefix length and prefix name defined in [RFC 2874](#) was declared experimental in favour of AAAA RRs. See [RFC 3363](#) and [3364](#) for more information and discussion.

[illegible]

The host command will look for both A and AAAA records, using dig you have to explicitly ask for AAAA records (`dig host.example.com aaaa`). Reverse lookups as usual can be done using host without further switches (`host 2001:db8::1`) or with dig using the `-x` switch (`dig -x 2001:db8::1`).

## Linux IPv6 Interface Configuration examples (Steps might slightly differ between distributions)

**Manual configuration:** You can temporarily configure an IPv6 address with the `ifconfig` or `ip` command:

```
# ifconfig eth0 inet6 add 2001:db8::2/64
# ip addr add 2001:db8::2/64 dev eth0
```

### Add a default route

```
# route -A inet6 add default 2001:db8::1 or
# ip -6 route add default via 2001:db8::1
```

To check the configuration use `ifconfig eth0` or `ip -6 addr show eth0` respectively `route -A inet6` or `ip -6 route show`. For making the changes permanent you'll have to edit the config files specific for your distribution.

**Automatic configuration using SLAAC:** Just having IPv6 enabled and IPv4 configured on the interface should normally do the trick.

**SLAAC with privacy extensions (RFC 4941):** To deal with security and privacy concerns regarding EUI-64 interface IDs enable and prefer temporary addresses over other public addresses with: \_\_\_\_\_

```
# sudo sysctl net.ipv6.conf.all.use_tempaddr = 2
# sudo sysctl net.ipv6.conf.all.use_tempaddr = 2
```

To make these settings boot proof put them into `/etc/sysctl.conf`.

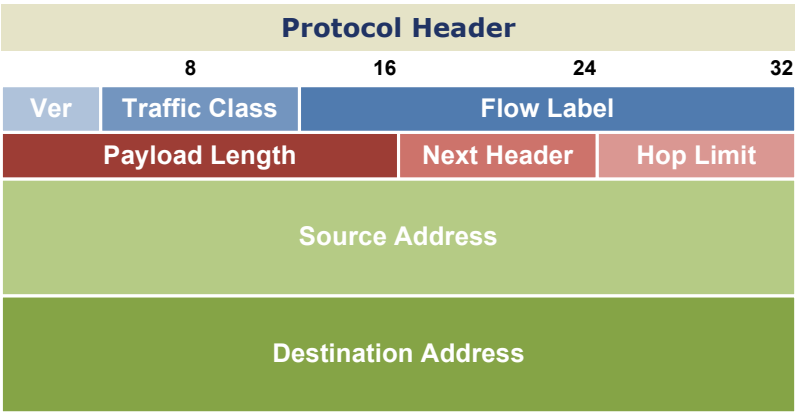
Change valid and preferred lifetime of temporary addresses by editing `net.ipv6.conf.all.temp_valid_lft` and `net.ipv6.conf.all.temp_preferred_lft`. Defaults are 604800 (7d) and 86400 (1d) seconds.

## \*NIX IPv6 Console Tools

ping6	IPv6 version of ping. Solaris ping supports IPv6 out of the box.
tracert6 tracert6	IPv6 versions of traceroute and tracepath. Also try mtr -6.
ip -6	Configure or view interfaces, routes, ND, list neighbors, multicasts.... on linux
ipv6calc	Powerful tool for all sorts of conversions and information gathering. See <a href="http://www.deepspace6.net/projects/ipv6calc.html">http://www.deepspace6.net/projects/ipv6calc.html</a>
tcpdump ip6 snoop inet6	Packet sniffing tools with IPv6 options. Also works with options like icmp6.

IPv6 RFCs (available at <http://tools.ietf.org/html/rfc<RFC number>>)

<a href="#">RFC 8200</a>	IPv6 Specifications	<a href="#">RFC 4193</a>	Unique Local IPv6 Unicast Addresses
<a href="#">RFC 4291</a>	IPv6 Addressing Architectures	<a href="#">RFC 2375</a>	IPv6 Multicast Address Assignments
<a href="#">RFC 4861</a>	IPv6 Neighbor Discovery	<a href="#">RFC 3849</a>	IPv6 Address Prefix For Documentation
<a href="#">RFC 4862</a>	IPv6 Stateless Address Configuration	<a href="#">RFC 4941</a>	Privacy Extensions for SLAAC in IPv6
<a href="#">RFC 8201</a>	Path MTU Discovery for IPv6	<a href="#">RFC 6147</a>	DNS64 – DNS Extensions for NAT64
<a href="#">RFC 3596</a>	DNS Extensions to Support IP Version 6	<a href="#">RFC 6146</a>	Stateful NAT64
<a href="#">RFC 4443</a>	ICMPv6 for IPv6	<a href="#">RFC 6434</a>	IPv6 Node Requirements
<a href="#">RFC 3587</a>	IPv6 Global Unicast Address Format	<a href="#">RFC 6540</a>	IPv6 Support Required for All IP-Capable Nodes



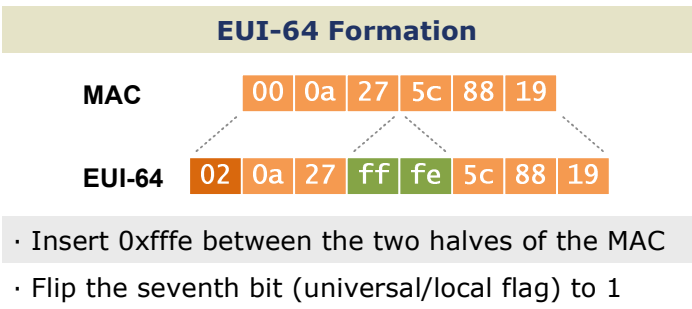
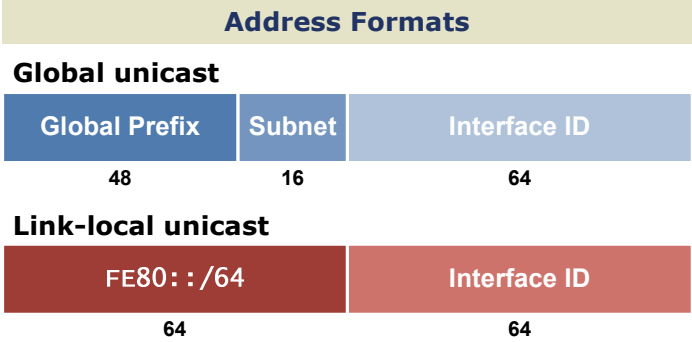
- Version (4 bits) · Always set to 6
- Traffic Class (8 bits) · A DSCP value for QoS
- Flow Label (20 bits) · Identifies unique flows (optional)
- Payload Length (16 bits) · Length of the payload in bytes
- Next Header (8 bits) · Header or protocol which follows
- Hop Limit (8 bits) · Similar to IPv4's time to live field
- Source Address (128 bits) · Source IP address
- Destination Address (128 bits) · Destination IP address

- Address Types
- Unicast · One-to-one communication
- Multicast · One-to-many communication
- Anycast · An address configured in multiple locations

Multicast Scopes	
1 Interface-local	5 Site-local
2 Link-local	8 Org-local
4 Admin-local	E Global

Special-Use Ranges	
::/0	Default route
::/128	Unspecified
::1/128	Loopback
::/96	IPv4-compatible*
::FFFF:0:0/96	IPv4-mapped
2001::/32	Teredo
2001:DB8::/32	Documentation
2002::/16	6to4
FC00::/7	Unique local
FE80::/10	Link-local unicast
FEC0::/10	Site-local unicast*
FF00::/8	Multicast
	* Deprecated

- Address Notation
- Eliminate leading zeros from all two-byte sets
- Replace up to one string of consecutive zeros with a double-colon (::)



- Extension Headers
- Hop-by-hop Options (0)  
Carries additional information which must be examined by every router in the path
- Routing (43)  
Provides source routing functionality
- Fragment (44)  
Included when a packet has been fragmented by its source
- Encapsulating Security Payload (50)  
Provides payload encryption (IPsec)
- Authentication Header (51)  
Provides packet authentication (IPsec)
- Destination Options (60)  
Carries additional information which pertains only to the recipient

- Transition Mechanisms
- Dual Stack  
Transporting IPv4 and IPv6 across an infrastructure simultaneously
- Tunneling  
IPv6 traffic is encapsulated into IPv4 using IPv6-in-IP, UDP (Teredo), or Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
- Translation  
Stateless IP/ICMP Translation (SIIT) translates IP header fields, NAT Protocol Translation (NAT-PT) maps between IPv6 and IPv4 addresses





# Index

/64, I-20  
6 naar 4, I-32  
  
Access control list, I-7  
achtervoegsel, I-18  
ACL, I-7  
anycast, I-17, I-26  
  
Benchmarking, I-32  
bereik, I-26  
broadcast, I-17, I-26  
  
CIDR, I-8  
Classless Inter Domain Routing, I-8  
  
DHCP Unique Identifier, I-15, I-23  
DHCPv4, I-23  
DHCPv6, I-23  
DHCPv6 client DUID, I-23  
DHCPv6 IAID, I-23  
DUID, I-15, I-23  
  
EUI-64, I-16, I-20  
Extended Unique Identifier, I-16, I-20  
  
ff02::1, I-31  
ff02::2, I-31  
ff0x::114, I-31  
  
global unicast, I-27, I-31  
  
IAID, I-15, I-23  
Identity Association Identifier, I-15, I-23  
ifconfig, I-19  
Internet Service provider, I-15  
IoT, I-19  
ip addr show, I-19  
ipconfig /all, I-19  
IPv4 mapped, I-29  
ISP, I-15  
  
link, I-30  
link local, I-27  
link-local, I-30  
livestream, I-17, I-26  
  
MAC adres, I-20  
multicast, I-17, I-26, I-27  
Multicastadres, I-31  
  
Neighbor Discovery Protocol, I-16  
neighbor solicitation, I-17, I-21  
netwerksegment, I-30  
  
Orchid, I-32  
OSI model, I-17, I-26  
  
prefix, I-17  
  
reikwijdte, I-26  
route prefix, I-20  
router advertisement, I-16  
router solicitation, I-16  
  
scope, I-26  
scope ID, I-28  
site ID, I-28  
Site local, I-29  
SLAAC, I-16, I-25  
statefull, I-16  
Stateless, I-16  
subnet prefix, I-20  
subnetmasker, I-20  
subnetting, I-7  
suffix, I-18  
  
Terendo, I-32  
  
UDP, I-17, I-26  
unicast, I-17  
Unique local, I-27, I-30

Voorbeeld IP, I-29  
voorloopnul, I-23  
voorvoegsel, I-17

werkgebied, I-26  
Wireshark, I-29

## Leerplandoelstellingen

- [1] 3.1.12. *De mogelijke technieken van adressering in een actuele netwerkarchitectuur toelichten.* (Zie pag. I-3, I-8, I-15).
- [2] 3.1.13. *De begrippen subnet en subnetmasker en de functie ervan toelichten.* (Zie pag. I-3, I-7, I-15).

*Pagina voor eigen notities.*

## Lijst van figuren

3.1	Voorbeeld van IP instellingen . . . . .	I-20
3.2	De grafische voorstelling van het IPv6 adres . . . . .	I-22
3.3	De opbouw van een global unicast adres . . . . .	I-22
3.4	De verschillende stappen van SLAAC . . . . .	I-25
3.5	De verschillende stappen van SLAAC . . . . .	I-25
3.6	. . . . .	I-34

*Pagina voor eigen notities.*

## Lijst van tabellen

1.1	Indeling in klasse voor IPv4 . . . . .	I-4
1.2	Overzicht van de private adressen . . . . .	I-5
2.1	Overzicht van de machten van 2 . . . . .	I-9
2.2	Overzicht van de IP verdeling bij subnetting van één bit in klasse c netwerk . . . .	I-10
2.4	Overzicht van de IP verdeling bij subnetting tussen twee routers in een klasse c netwerk . . . . .	I-12
2.6	Overzicht van de IP verdeling bij subnetting met 14 toestellen per subnet . . . . .	I-13
3.2	Overzicht van de basisbegrippen . . . . .	I-18
3.3	Overzicht van IPv6 adresruimte . . . . .	I-32

*Pagina voor eigen notities.*



## Lijst met typevragen

1.1	Reproduceer de overzichtstabel met de verschillende IP adressen per klasse . . .	I-6
1.2	Reproduceer de overzichtstabel van de private adressen in IPv4 . . . . .	I-6
1.3	Bespreek de bouw van het IP adres . . . . .	I-6
1.4	Bespreek de bouw van het subnetmasker . . . . .	I-6
1.5	Bespreek de betekenis van het subnetmasker . . . . .	I-6
1.6	Bespreek de speciale IP adressen, met name het IP adres van het netwerk en het broadcastadres . . . . .	I-6
2.7	Je vertrekt van het netwerk klasse C (niet privé) <b>201.66.54.0/24</b> . Je splitst dit netwerk in twee delen. Noteer de gegevens van het IP adres per subnet, de range per subnet, het broadcastadres en het subnetmasker in verkorte vorm. . .	I-10
2.8	Bepaal van het 32 <sup>ste</sup> subnet het IPadres van het subnet dat twee routers met elkaar verbindt, het broadcastadres en de range van toekenbare IPv4 adressen. Je vertrekt van het privénetwerk 192.168.55.0/24 . . . . .	I-11
2.9	Deel een gegeven netwerk 192.168.0.0/24 in 8 gelijke subnetten in. Vermeld IP adres van netwerk, broadcastadres, de range van bruikbare IPadressen en het subnetmasker onder verkorte notatie . . . . .	I-14
2.10	Deel een gegeven netwerk 192.168.55.0/24 in subnetten zodat elk subnet tussen 50 en 60 toestellen kan bevatten. Vermeld IP adres van netwerk, broadcastadres, de range van bruikbare IPadressen en het subnetmasker onder verkorte notatie	I-14
3.11	Bespreek de basisbegrippen zoals je die vindt in de tabel vooraan dit cursusdeel	I-35
3.12	Bespreek de volgende begrippen: SLAAC, unicast, anycast, multicast, broadcast	I-35
3.13	Bespreek de volgende adressen met hun reikwijdte en een voorbeeld: global unicast adres, unique local address en link local address . . . . .	I-35
3.14	Noteer de kenmerken van een IPv6 adres . . . . .	I-35
3.15	Vergelijk de kenmerken van een IPv6 adres met die van een IPv4 adres . . . . .	I-35
3.16	Noteer het IPv6 adres van een gegeven computer. <i>Hiervoor mag je het commando <b>ipconfig</b> gebruiken.</i> . . . . .	I-35
3.17	Vereenvoudig een voluit geschreven IPv6 adres waar mogelijk . . . . .	I-35
3.18	Noteer het volledig IPv6 adres als je het IPv6 adres in verkorte vorm krijgt . . . .	I-35
3.19	Converteer een MAC adres in een EUI-64 interface ID . . . . .	I-35
3.20	Leid het MAC adres af uit een EUI-64 interface ID . . . . .	I-35
3.21	Bespreek de 3 mogelijkheden bij de reikwijdte van een IPv6 adres . . . . .	I-35
3.22	Bespreek de speciale IPv6 adressen, waaronder onbepaald, loopback, IPv4 mapped, voorbeeld IP, site local, unique local, link local, multicast, global unicast,	I-35
3.23	Bespreek op welke wijze je een IPv6 adres aan een toestel kan toekennen . . .	I-35