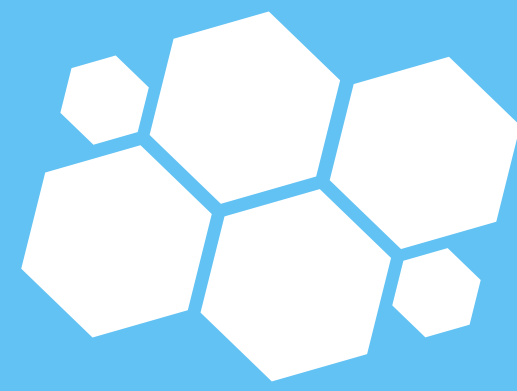




inet⁶ consult

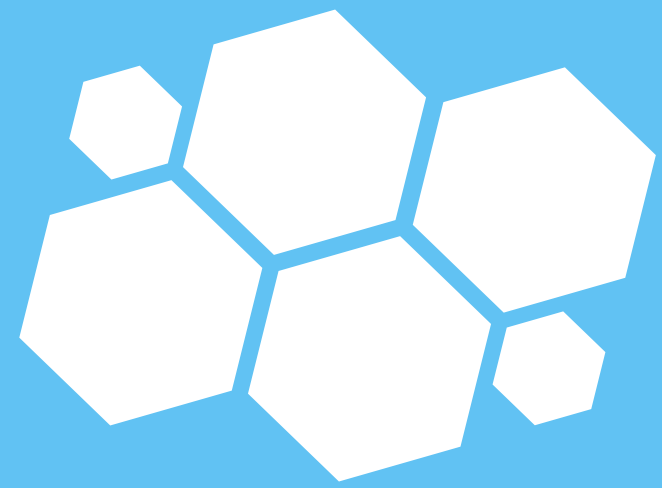
Internetbeschikbaarheid

Hoe verhoog je die?

PvIB, Utrecht, 12 april 2022

Iljitsch van Beijnum

Beveiliging: BIV



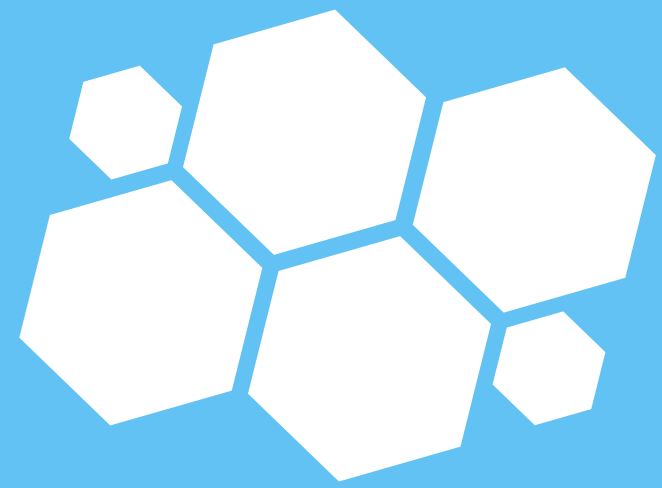
- BIV:

- beschikbaarheid

- integriteit

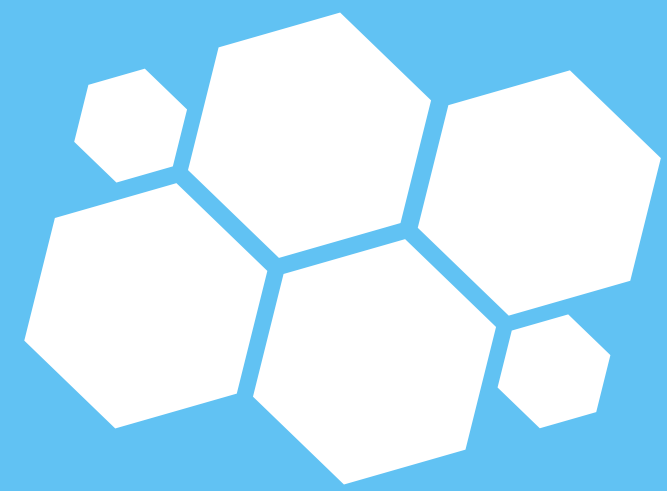
- vertrouwelijkheid

Onderwerpen



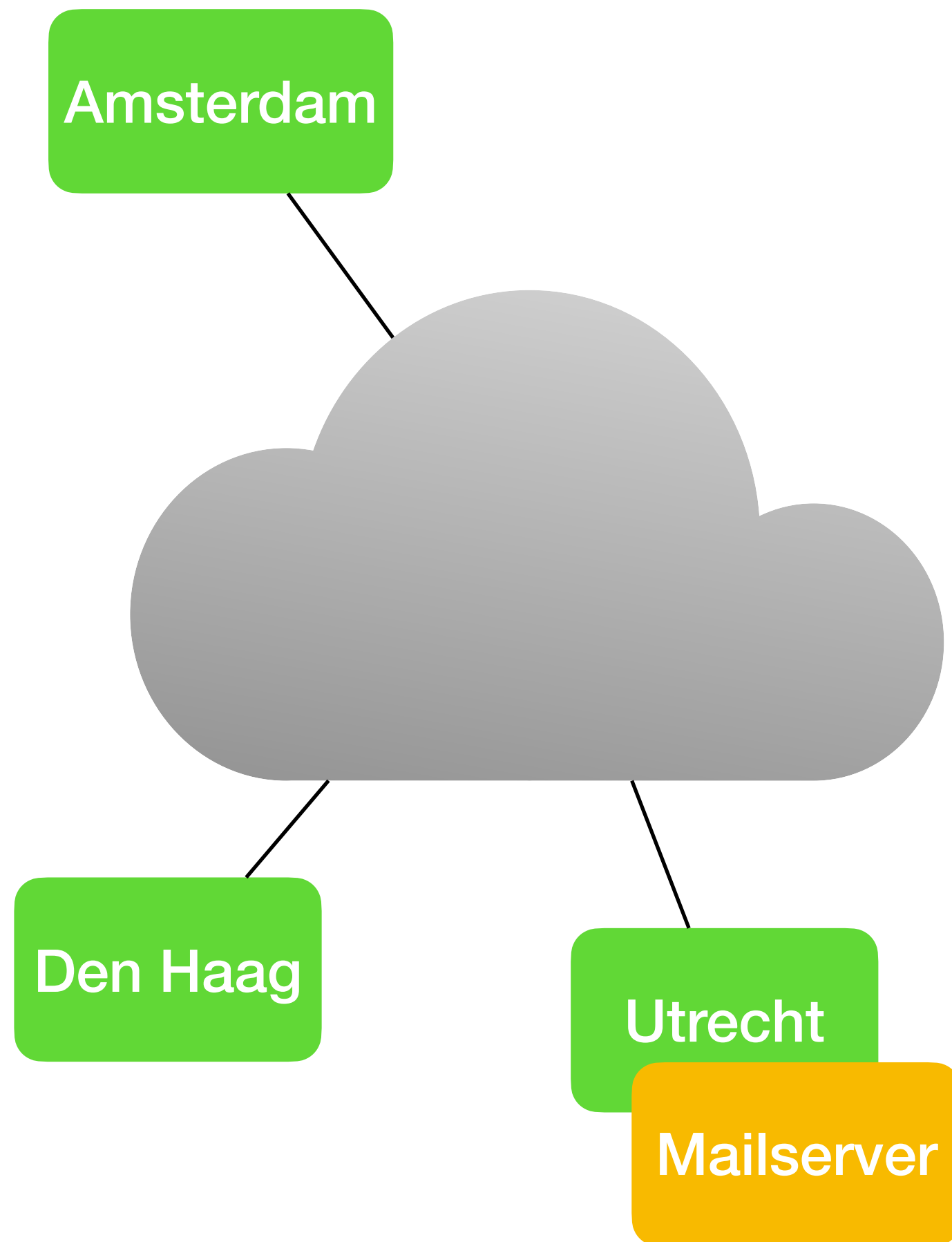
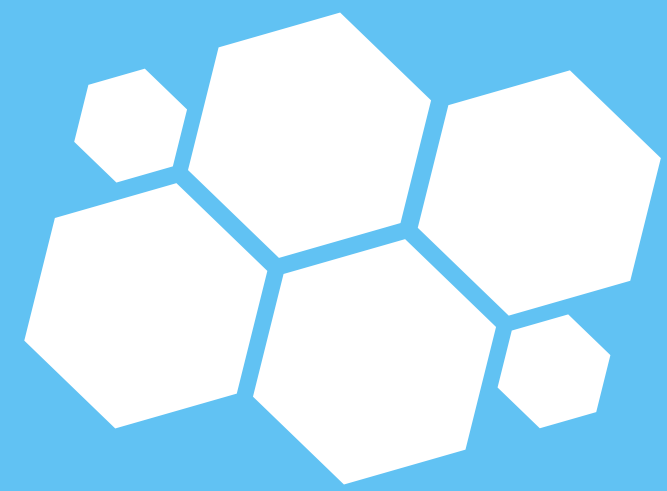
1. Hoe ziet de „cloud” eruit, gezien van uit het netwerk?
2. Afhankelijkheden
 - Inrichting eigen (kantoor-) locatie
 - ISP/internet-risico's
 - overige afhankelijkheden/risico's
3. Om het internet heen?
4. Conclusies

Hoezo "cloud"?



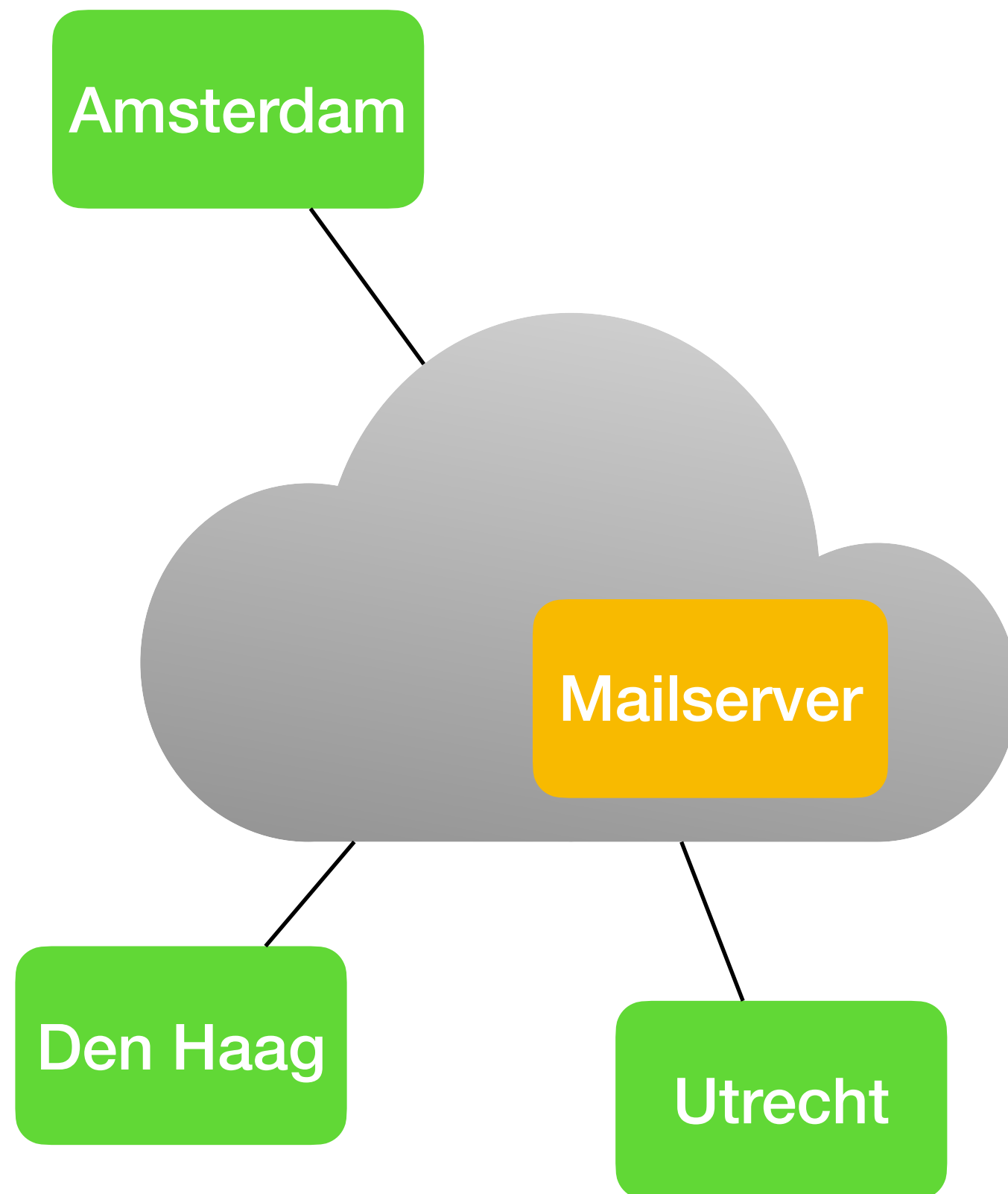
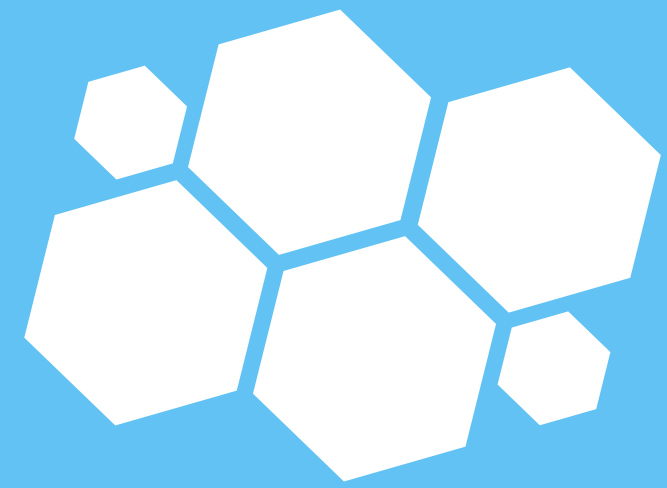
- Engels voor wolk!
- Voordat we het internet hadden...
- ...wisten we niet wat er met onze data gebeurde in het netwerk van de telecombedrijven
- Die netwerken tekenden we dus als een wolk:
 - er gaat wat in...
 - ...het wordt op één of andere manier getransporteerd...
 - ...en het komt er elders weer uit

Hoezo "cloud"? (2)



- Conceptueel:
 - in de wolk = *in* het netwerk
 - je communiceert met een DNS-naam
 - maakt niet uit waar
- Praktisch:
 - *aangesloten* op het netwerk
 - je communiceert met een IP-adres
 - dat leidt tot een specifieke server in een specifiek datacenter
- Kleinschalige uiterste:
 - DNS-naam → 1 IP-adres → 1 fysieke server

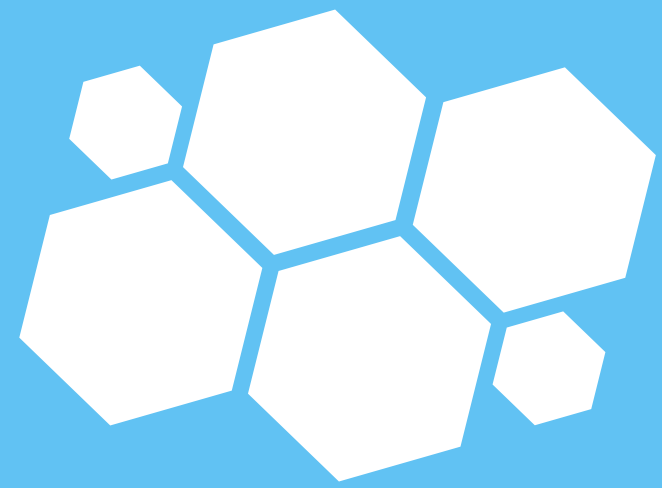
Hoezo "cloud"? (3)



- Grootschalige SaaS/PaaS/IaaS-diensten:

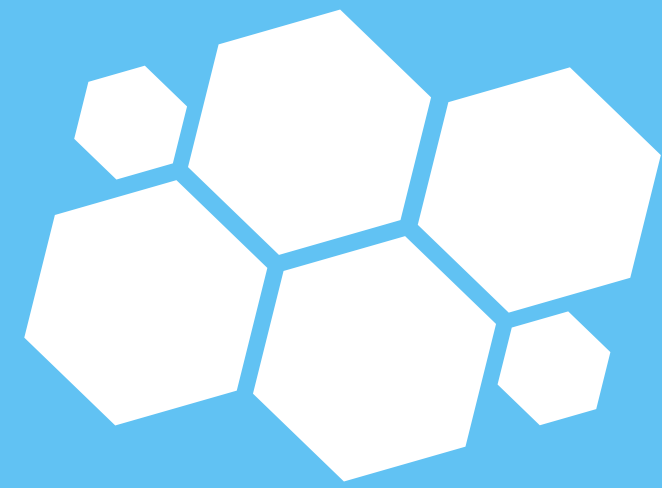
- DNS-naam ☁
- tussenliggende DNS-namen ☁
- 1 of meer publieke IP-adressen 🤔 / 😊💧 / 💶
- op 1 of meer locaties 🤔 / 😊💧 / 💶
- meerdere private IP-adressen ☁
- virtuele server ☁
- gedeelde fysieke servers ☁

Afhankelijkheden



1. Apparatuur op je eigen (kantoor-) locatie
2. Verbinding naar ISP (de daadwerkelijke kabel)
3. Infrastructuur van je internet service provider
4. DNS
5. Routing tussen ISPs
6. Lokatie-infrastructuur clouddienstaanbieder
7. Dienstaanbieder in z'n geheel
 - (weet je nog waar je was 4-10-2021?)

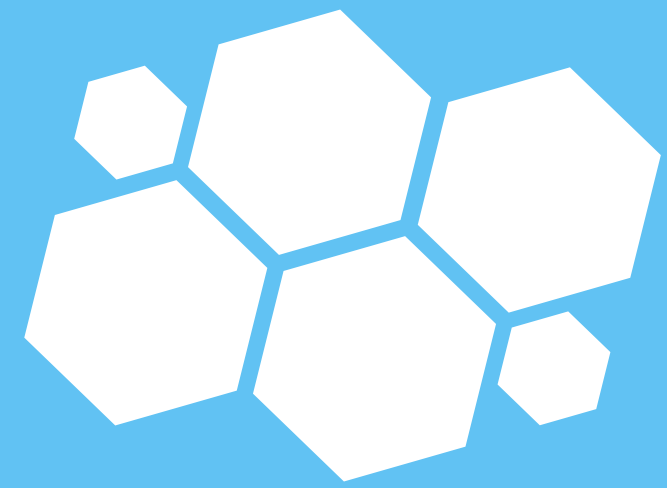
Hoe ben je on-afhankelijk?



- Simpel gezegd: van alles twee:
 - Apparatuur op je eigen (kantoor-) locatie 🤔 / 😄💧 / 💶
 - Verbinding naar ISP (de daadwerkelijke kabel) 🤔 / 💶
 - Infrastructuur van je internet service provider 💶 / 🤔
 - DNS 🤔
 - Routing tussen ISPs 🤔
 - Lokatie-infrastructuur clouddienstaanbieder ☁️ (🤔 / 💶)
 - Dienstaanbieder in z'n geheel ☁️ / 😲

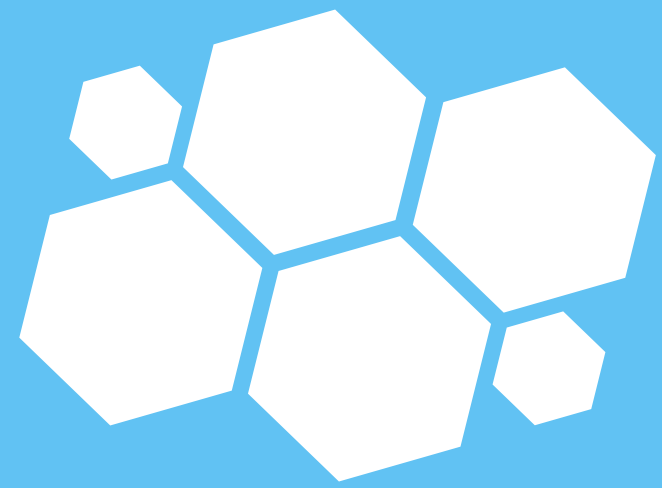
☁️ = aan dienstaanbieder 🤔 = over nadenken 😄💧 = zelf doen 💶 = betalen voor kwaliteit 😲 = lastig!

Je eigen (kantoor-) locatie



- Heel klein:
 - gewone vaste internetverbinding
 - 4G/5G als backup
- Middelgroot:
 - twee aparte ISPs
 - handmatig wisselen (b.v. tussen 2 Wi-Fi SSIDs)
- Groot:
 - eigen glasvezels naar meerdere ISPs
 - eigen BGP-routing om automatisch te herrouteren

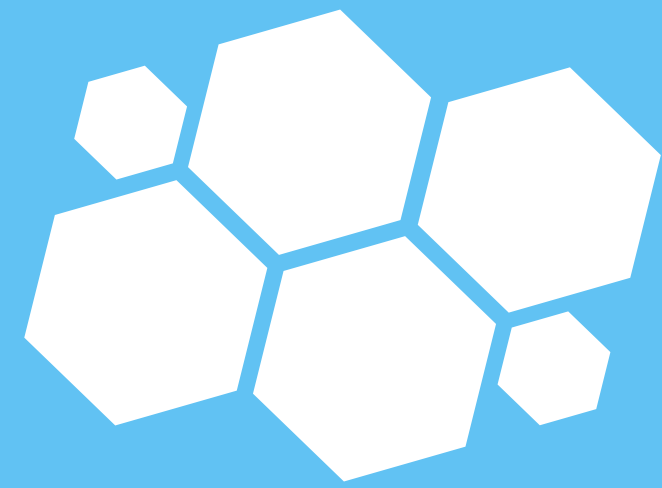
BGP?



- Border Gateway Protocol is de lijm die het internet bij elkaar houdt
- BGP berekent de routes naar alle IP-adressen op het internet
- Betekent wel:
 - eigen blok IP-adressen
 - "AS"-nummer
 - twee stevige routers
 - complexe instellingen
- Optimale robuustheid connectiviteit!

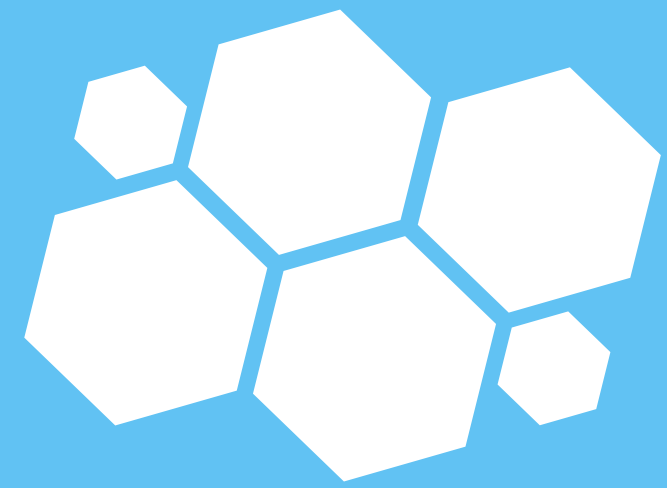


Tussenopties



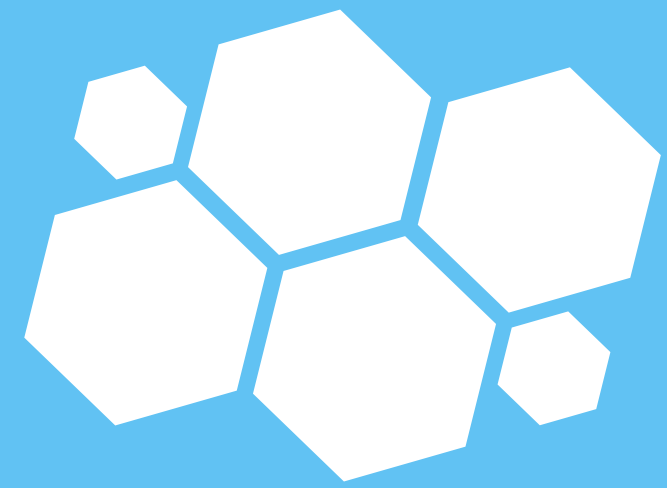
- Twee apart gerouteerde glasvezels naar *dezelfde* ISP
 - geen BGP: simpelere routers / routerinstellingen
 - maar nog wel maatwerk van ISP nodig
- Eén ISP voor IPv4, een andere ISP voor IPv6
 - kan al met consumenten-internetverbindingen
 - wel een iets geavanceerdere router nodig, maar hoeft niet duur, bijvoorbeeld Mikrotik
 - webbrowsers en veel applicaties zien vaak supersnel of IPv4 wel werkt en IPv6 niet of omgekeerd
 - maar niet alles beschikbaar via IPv6

Infrastructuur van je ISP



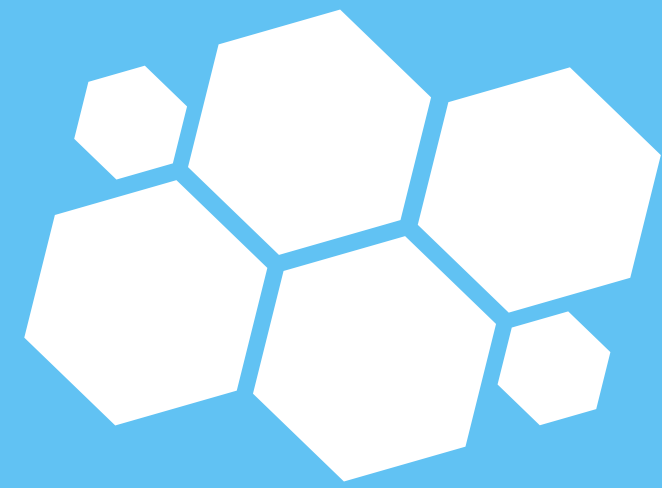
- Kan goed zijn of minder goed, zelden echt slecht
- Maar *a/s* het mis gaat... daar zit je dan
- Goed onderzoek vantevoren kan helpen:
 - grote storingen in het verleden? oplossnelheid?
 - andere incidenten? ("de-peering")
 - eigenstandig in Nederland, of bijkantoor buitenlandse partij?
- SLAs beschermen niet tegen storingen, maar in elk geval duidelijk aanspreekpunt en je krijgt geld terug

Routing tussen ISPs

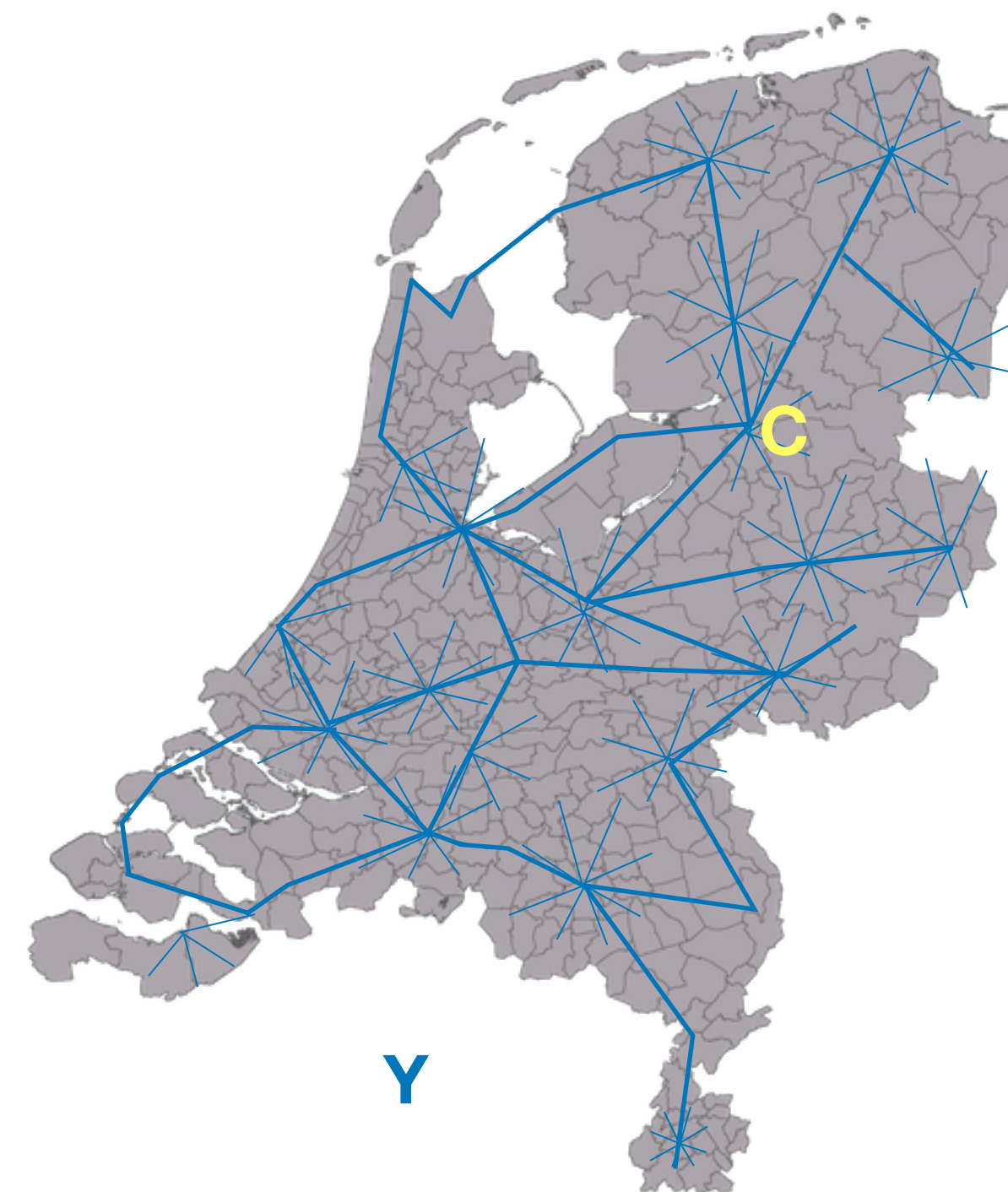
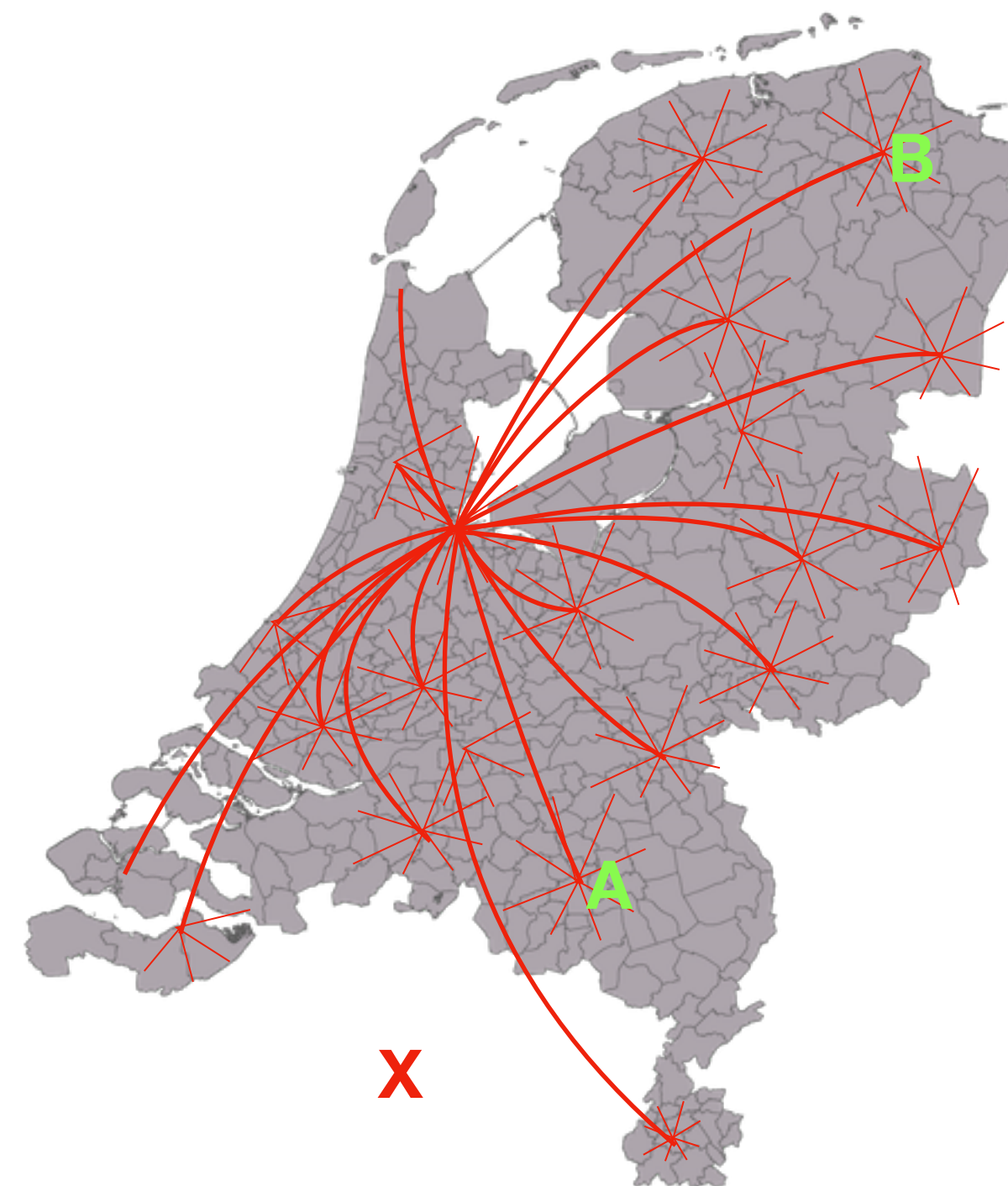


- Het internet is een "netwerk van netwerken"
- Veel van de netwerken overlappen. In Nederland:
 - KPN, Vodafone/Ziggo, T-Mobile, Telfort, Tele2, Eurofiber, Surfnets, Caiway, Delta, Dataweb, ...
- En toch kunnen klanten van elke ISP communiceren met klanten van elke andere ISP!
- Er zijn dus altijd koppelingen, rechtstreeks of via één of meer tussenliggende ISPs

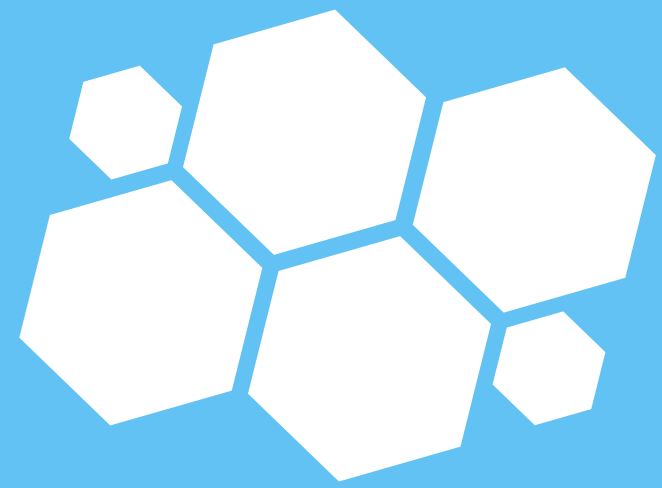
Interconnectie tussen ISPs



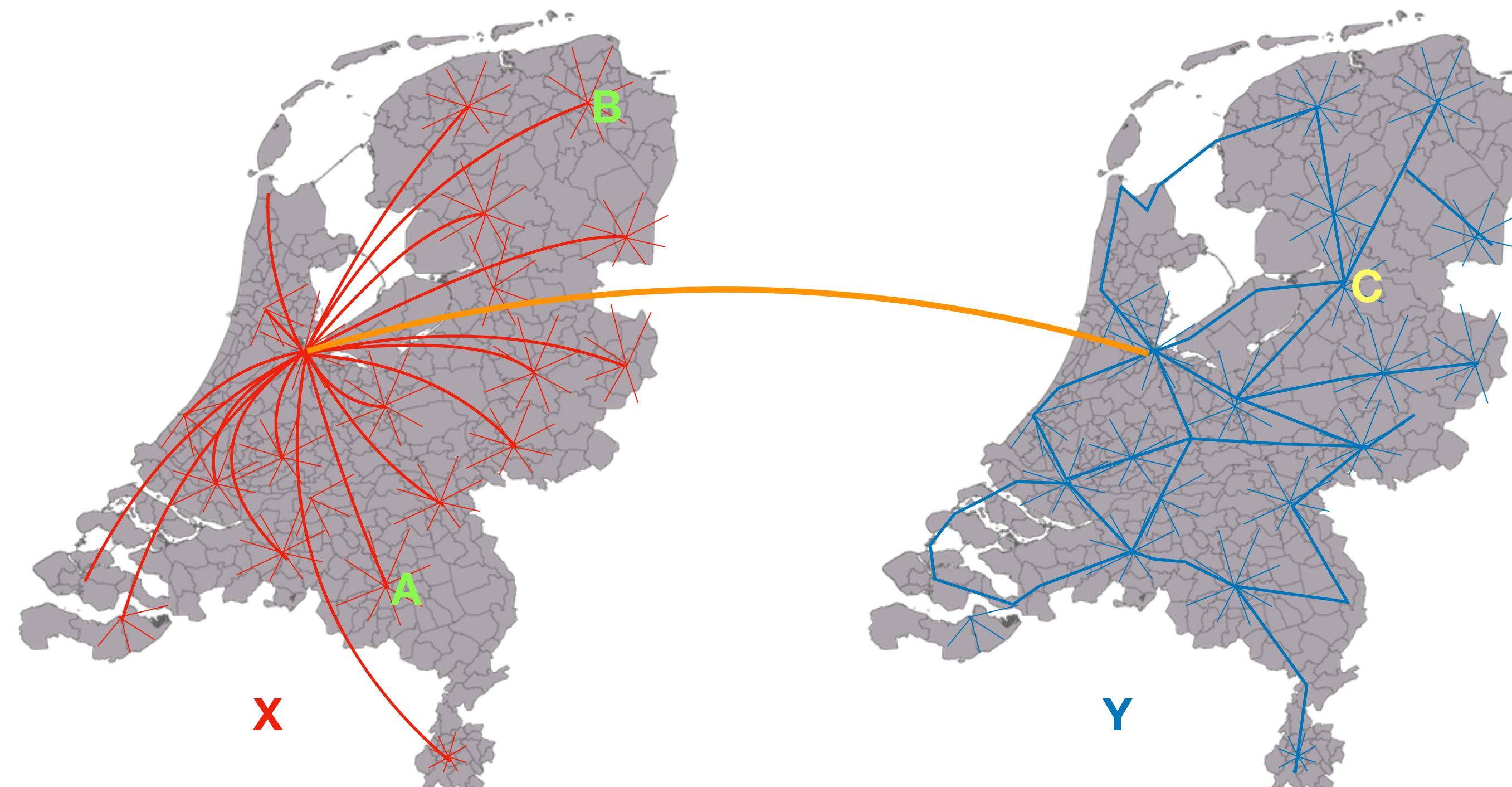
- Iedere ISP heeft z'n eigen netwerk: **A** naar **B**: makkelijk
- Maar wat als **A**, klant van ISP **X**, wil communiceren met **C**, klant van ISP **Y**?



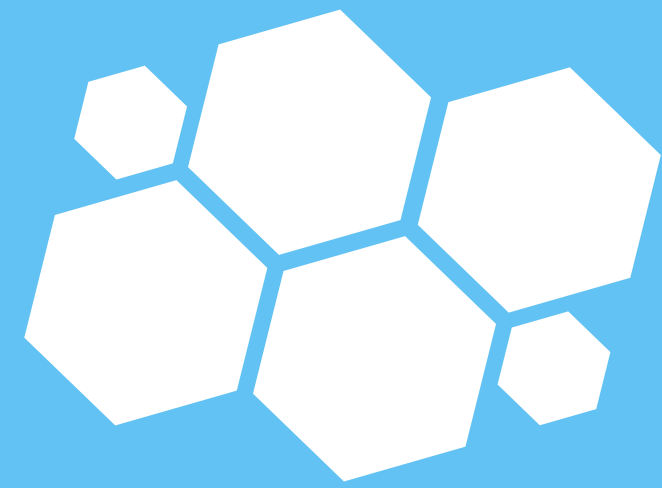
Interconnectie tussen ISPs (2)



- "Peering" tussen ISPs
- Via internet exchanges zoals AMS-IX
- of directe kabel

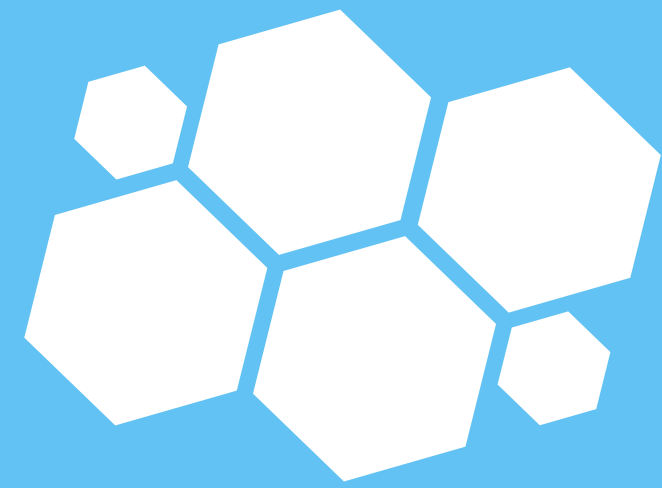


Routing tussen ISPs (2)



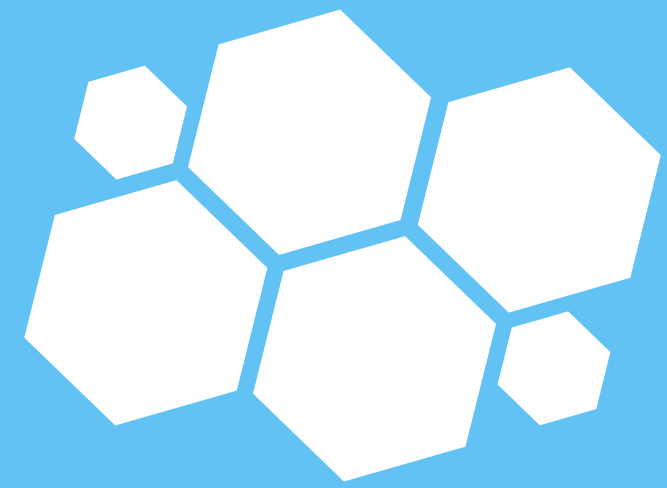
- BGP dus
- Er zijn een stuk of 12 "tier-1" netwerken
 - de rest van het internet is direct of indirect klant van één (of meer) van die grote netwerken
 - deze grote netwerken zijn allemaal onderling gekoppeld (op meerdere locaties): "peering"
- Kleinere netwerken doen ook aan peering
 - maar de groten willen meestal niet met de kleintjes

De-peering



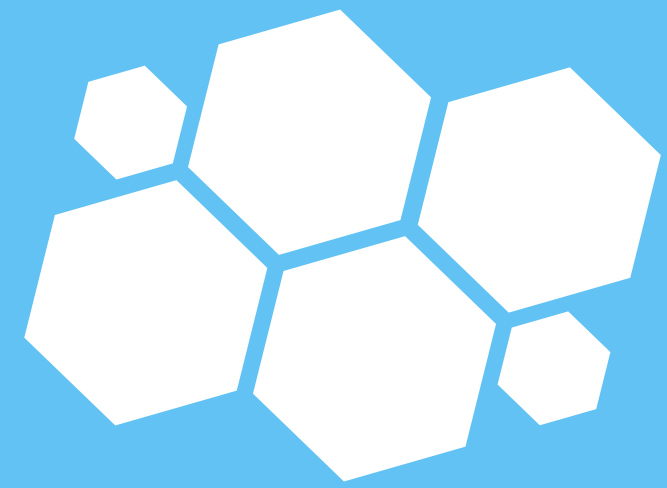
- Soms krijgen de grote(re) netwerken ruzie over de peering-voorwaarden
- Dan kan één van beide partijen besluiten te "de-peeren"
- Dan is er geen rechtstreeks verkeer meer tussen netwerk A en netwerk B meer mogelijk
 - en dus ook niet tussen de klanten van A en de klanten van B
- Pas dus op met netwerken met een de-peering-geschiedenis, en/of
- Neem zelf meerdere ISPs, of
- Neem een ISP die klant is van meerdere van de tier-1s

BGP-problemen



- BGP werkt tussen zo'n 100.000 netwerken
 - als één iets doet zien alle anderen dat binnen 30 tot 120 seconden
 - * fouten hebben onmiddellijk effect!
 - * maar de oplossingen meestal ook 😅
- Belangrijk type fout: "route leak"
 - klein(er) netwerk zegt bijvoorbeeld "Twitter is nu bereikbaar via ons!"
 - maar dat gaat natuurlijk niet goed
 - verkeer loopt dood

BGP-problemen (2)



- 28 maart nog:

BGP —

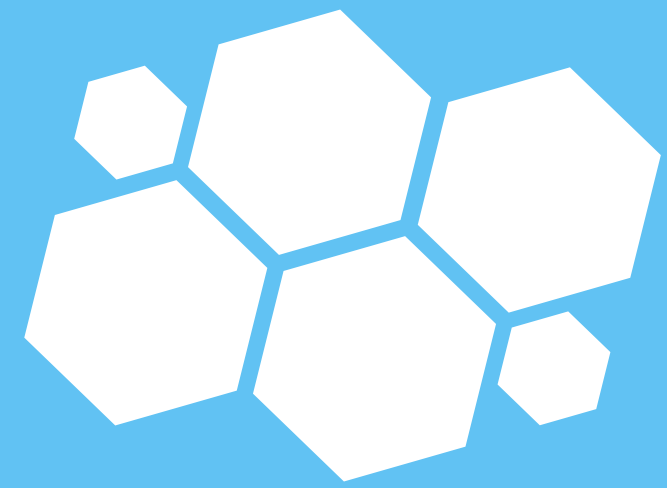
Some Twitter traffic briefly funneled through Russian ISP, thanks to BGP mishap

Despite the timing, the 45-minute hijacking was most likely an error, not an attack.

- Maar bekendste: Youtube/Pakistan
 - gerelateerd aan:
- BGP-beveiligingssysteem RPKI helpt vaak, maar niet altijd

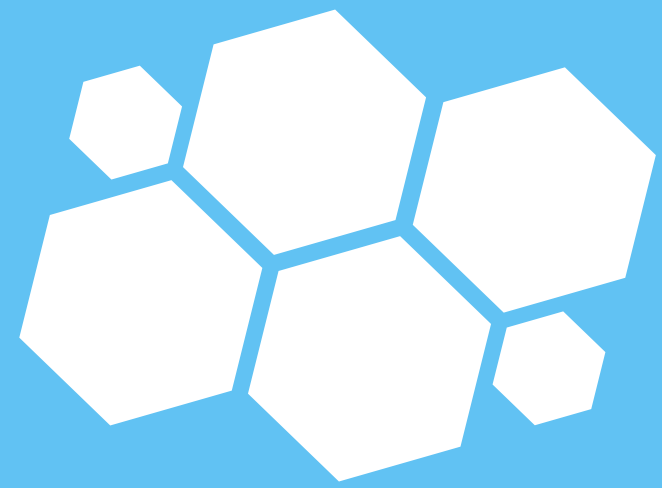


Infrastructuur dienstaanbieder

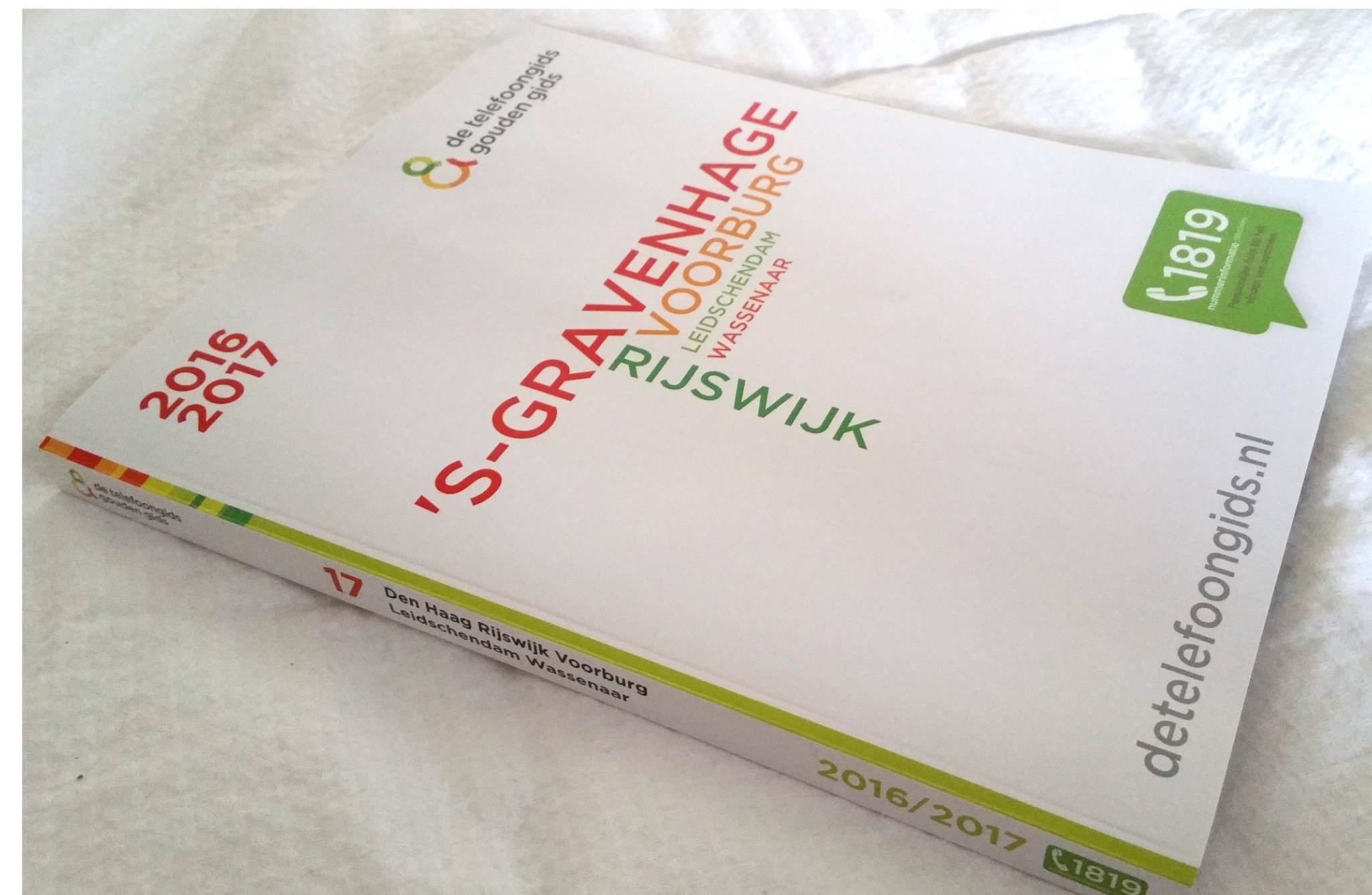


- Grote SaaS/PaaS/IaaS-dienstaanbieders hebben alles zeer meervoudig uitgevoerd:
 - zo goed als geen risico's door simpel uitvallen van apparatuur, verbindingen of stroom
 - desnoods word je naar een ander continent geherrouteerd!
- Overblijvende risico's:
 - falen complexe monitoring/herrouteringsystemen
 - "laag 8"-problemen

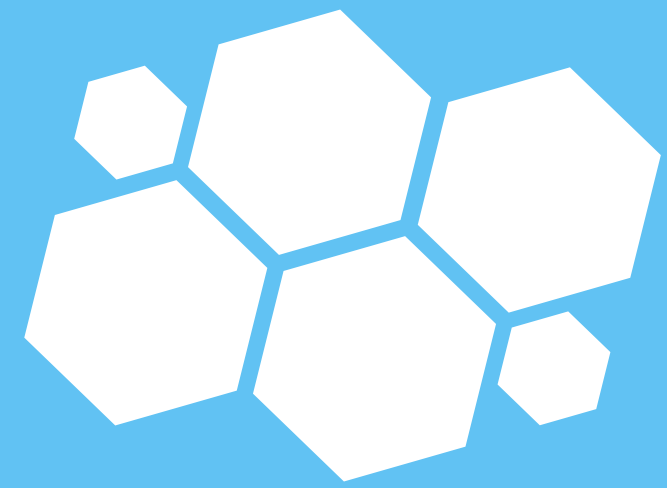
DNS



- "Telefoonboek" van het internet
- Kan veel mee mis gaan
- Maar gebeurt gelukkig zelden
- Wel handig om echt verschillende DNS-servers te gebruiken, niet twee van dezelfde ISP
- Bonuspunten: DNSSEC
- En let goed op de hosting van je eigen domeinen, als een aanvaller dat wachtwoord te pakken krijgt...

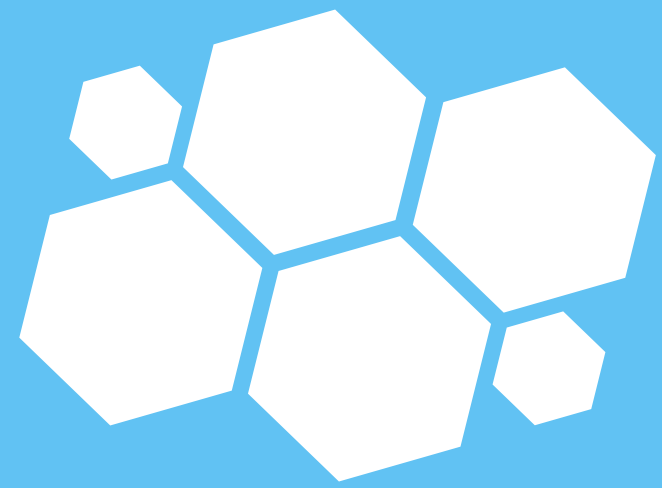


Om het internet heen?



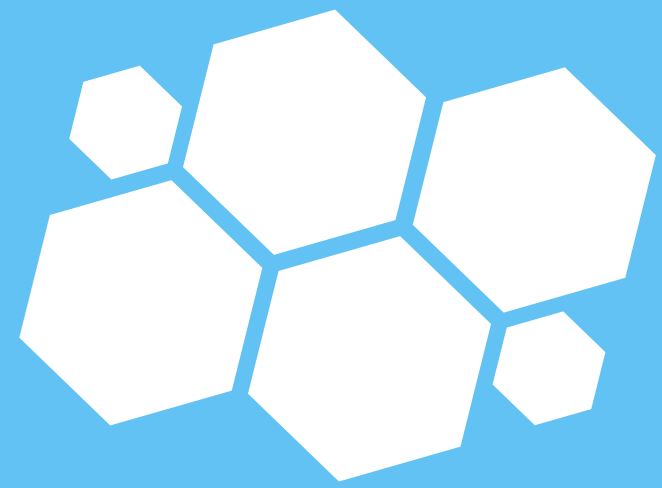
- Als je eigen apparatuur in een aantal datacenters hebt staan kan je glasvezels daar naartoe huren, geen internetrisico's!
 - met name nuttig als je ook nog kritische apparatuur op eigen (kantoor-) locaties hebt staan
- Rechtstreeks naar clouddiensten: "cloudconnect"
 - wel flinke beperkingen:
 - geen rechtstreekse glasvezel, er zit nog een telecombedrijf tussen
 - je kom vlak voor de "voordeur" uit:
 - * dus samen met internetverkeer door firewalls en anti-DDoS
 - * blijft afhankelijk van publieke DNS
 - * blijft afhankelijk van publieke IP-adressen van de clouddienst
 - * niet volledig immuun voor internet-routeringsproblemen

Conclusies



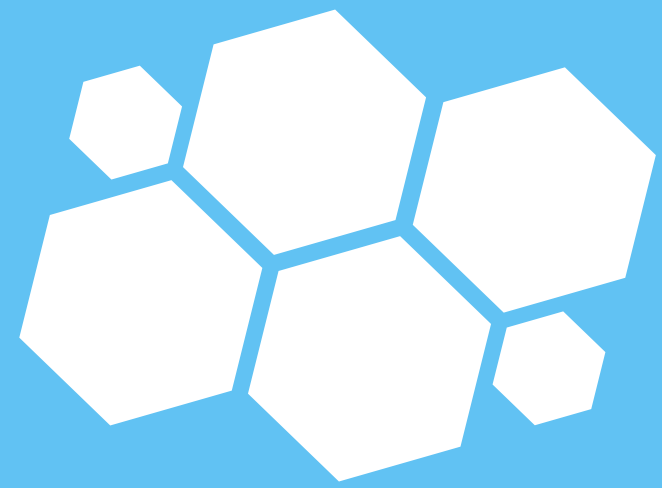
- Alles gaat ooit een keer kapot!
- Dus voorkom "single point of failure"
 - neem twee ISPs
 - * al is het maar 4G/5G via je telefoon als backup
 - gebruik twee IP versies: IPv4 *en* IPv6
 - indien van toepassing: DNSSEC en RPKI
 - * "publiceer" in elk geval, dat is relatief simpel
 - * waar mogelijk: ook controles toepassen

Te afhankelijk ☁ ?



- De vraag van de avond...
- *Het hangt er vanaf:*
 - hoeveel miljoen kost elk uur dat bol.com onbereikbaar is?
 - hoeveel scheelt het als een medewerker een halve dag niet kan mailen en Googlen, maar wel verder kan met Word en Powerpoint op haar eigen PC?
 - voordelen van *zero footprint*-systemen voor medewerkers, maar dan wel het nadeel dat zonder netwerk medewerkers helemaal niks meer kunnen?
- Ofwel: als je er maar over nagedacht hebt

Vragen?



Bedankt voor het luisteren!

inet6consult.com