BGP-beveiliging en route leaks

NiVo Kennissessie
Weesp, 10 september 2019

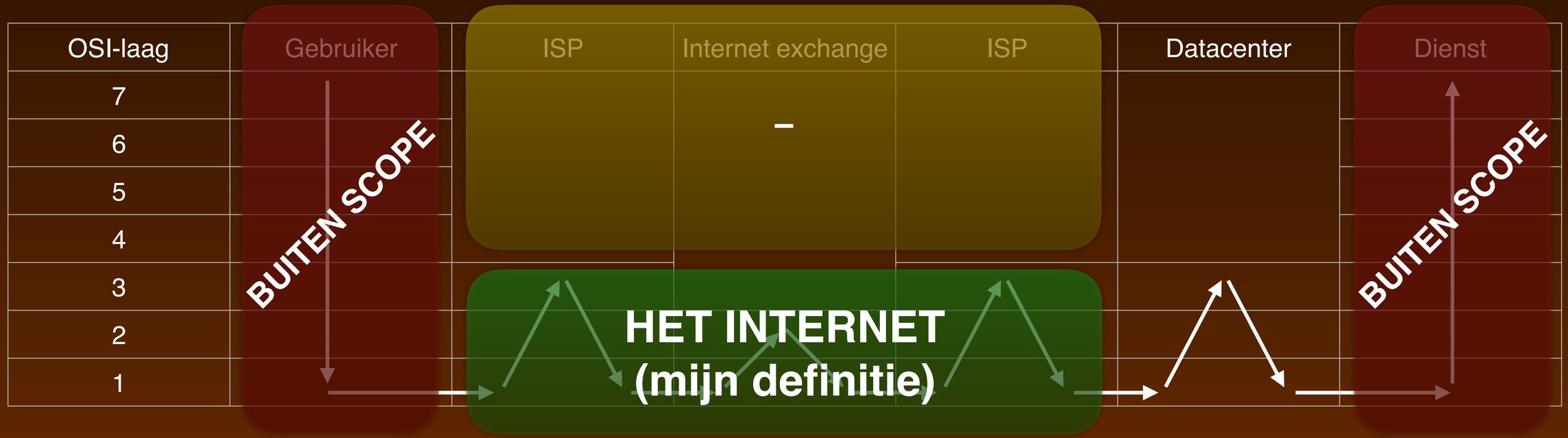
Iljitsch van Beijnum

Wat is BGP?

- BGP is de lijm die het internet bij elkaar houdt
- BGP berekent de routes naar alle IP-adressen op het internet

Wat is het internet?

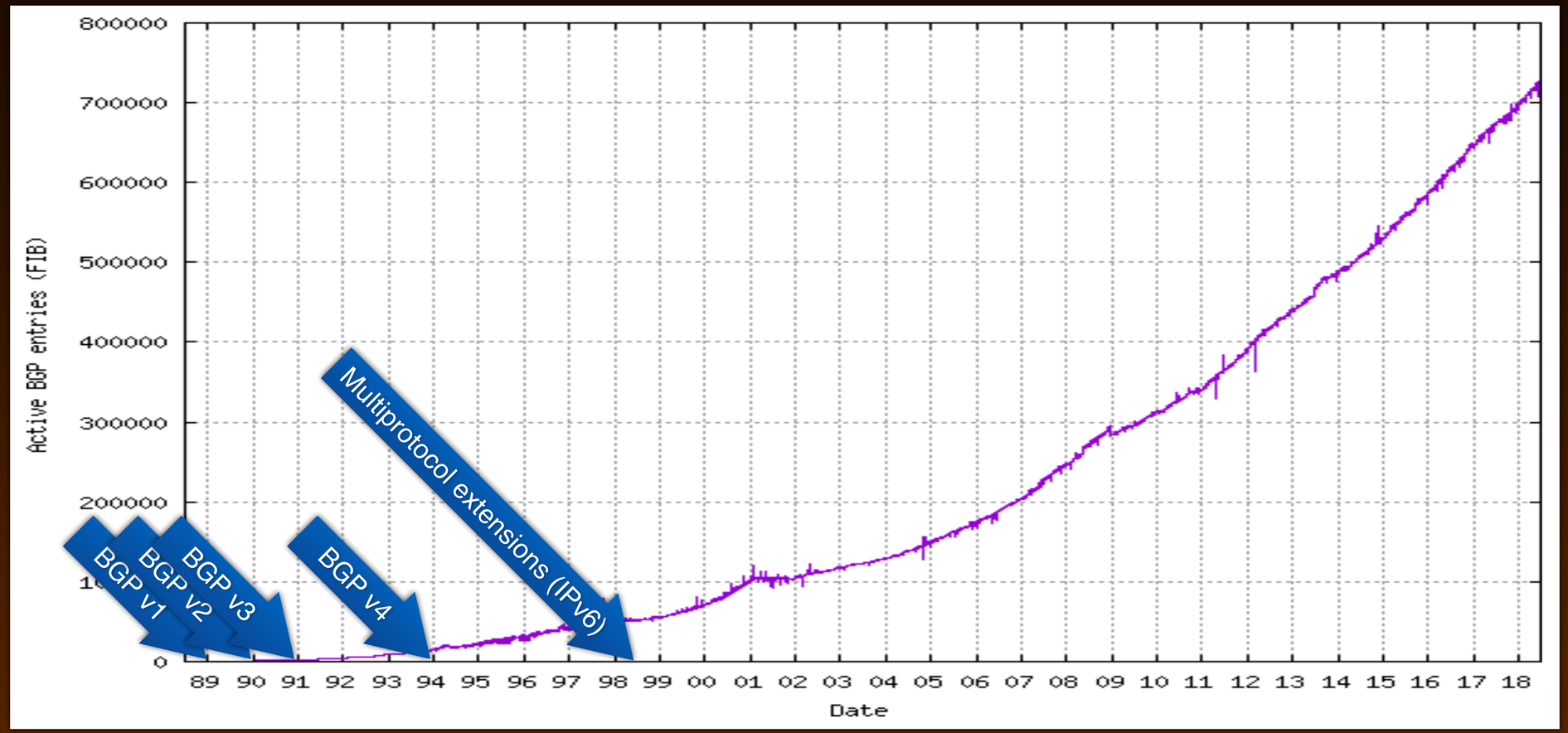
~~"The Internet is the global system of interconnected computer networks that use the Internet protocol suite (TCP/IP) to link devices worldwide. It is a network of networks that consists of private, public, academic, business, and government networks"~~



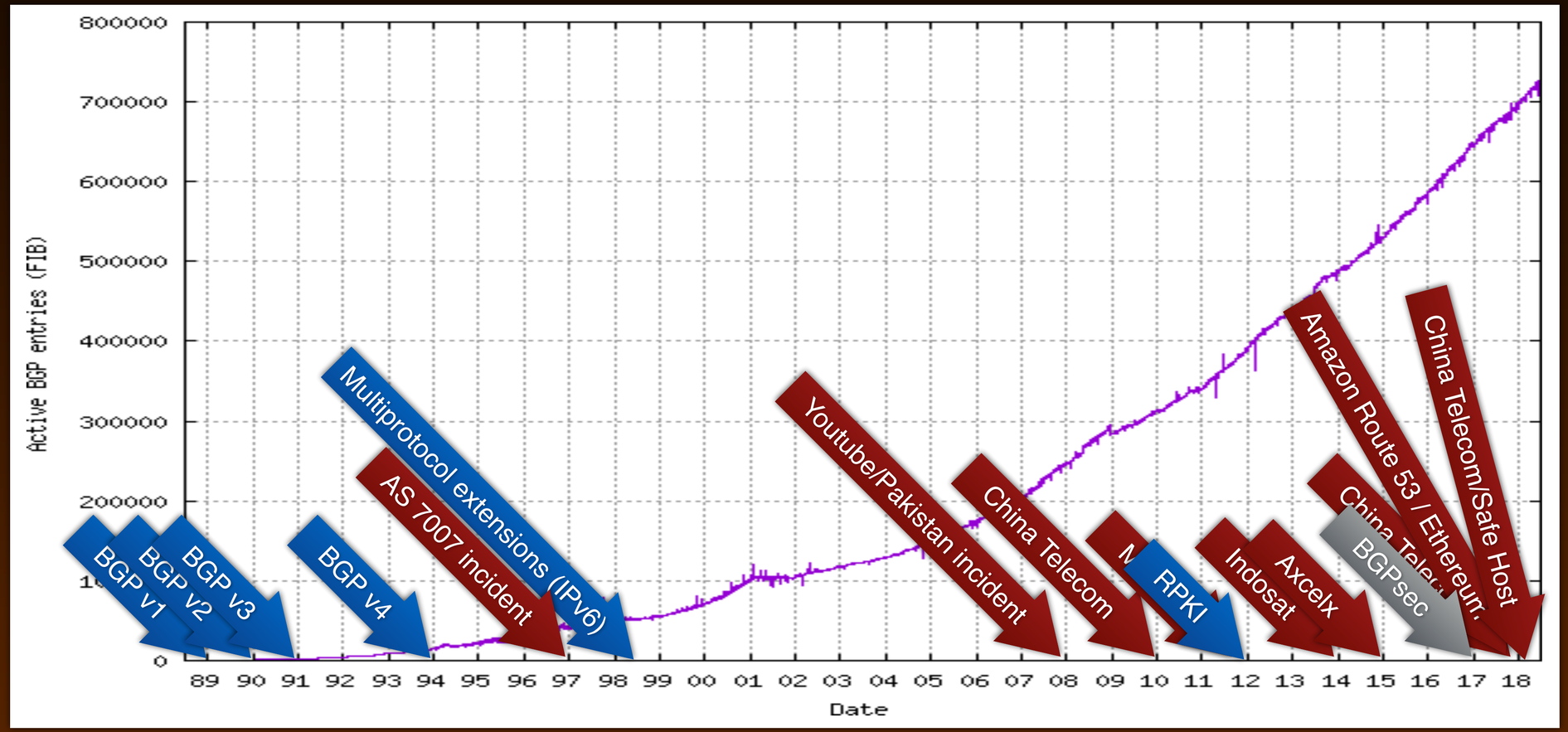
Het internet en BGP

- Het internet is de "wolk" die begint bij jouw drempel en eindigt bij de drempel van degenen waarmee je communiceert
- Die internet-wolk bestaat uit de netwerken van enkele tienduizenden ISPs die met elkaar verbonden zijn
- BGP zorgt ervoor dat pakketten daarbinnen juist gerouteerd worden
- Normaal "ontzorgt" de ISP de klant qua BGP-routering
- Maar als je op meerdere ISPs aansluit moet je zelf in BGP participeren

BGP-tijdlijn



Soms heeft BGP een slechte dag...



Maar het gaat <u>veel</u> vaker mis...

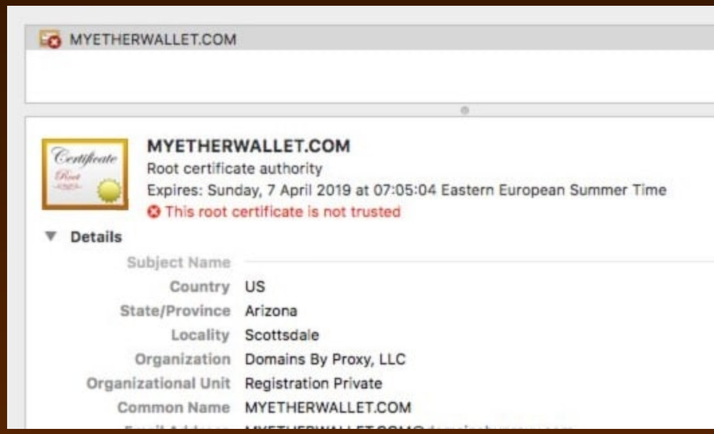
Youtube / Pakistan

- In februari 2008 gaf de Pakistaanse overheid ISPs in het land opdracht Youtube te blokkeren
  - naar verluidt vanwege de video's van Geert Wilders
- Daarop routeerde Pakistan Telecom de adressen van de Youtube videoservers naar "null0"
- Alleen... deze routeringsingreep werd via BGP gepropageerd naar Pakistan Telecom's ISP in Hong Kong
- En vanaf daar richting de rest van de wereld, waardoor veel netwerken verkeer voor Youtube naar Pakistan stuurden
- Zowel in Pakistan als Hong Kong had dit gefilterd moeten worden...

https://arstechnica.com/uncategorized/2008/02/insecure-routing-redirects-youtube-to-pakistan/

Amazon Route 53 / Ethereum wallets

- Criminelen injecteerden de IP-adressen van de Amazon Route 53 DNS-servers in BGP vanuit een server in Chicago
- De server in Chicago gaf nep-DNS-antwoorden voor "myetherwallet.com" die verwezen naar een server in Rusland
- Waar vervolgens nietsvermoedende bezoekers hun Ethereum cryptovaluta kwijtraakten
- Maar wacht even... beschermt HTTPS / TLS daar niet tegen???



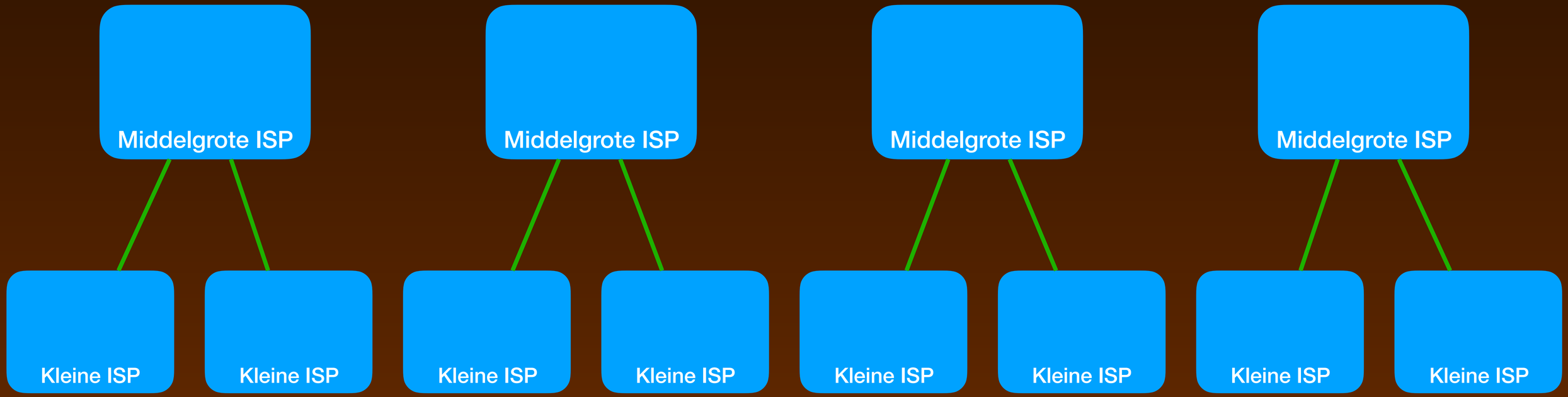
https://www.welivesecurity.com/2018/04/25/ethereum-cryptocurrency-wallets-raided/
https://www.internetsociety.org/blog/2018/04/amazons-route-53-bgp-hijack/

Problemen ver van huis

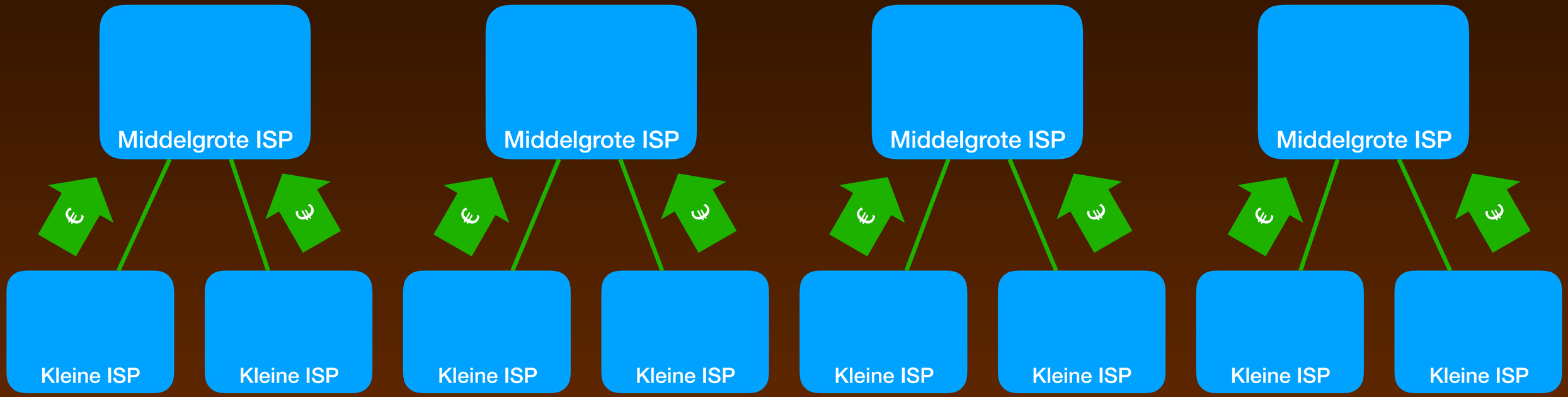
- We zijn gewend onze eigen apparatuur en ons eigen netwerk te beveiligen
  - daar hebben we zelf controle over
- Maar er kunnen ook heel vervelende dingen gebeuren in de internet-wolk
  - met name op het gebied van BGP en DNS
  - we kunnen/moeten *zelf* RPKI en DNSSEC toepassen
  - maar dat is alleen effectief als *anderen* het ook doen

Transit versus peering

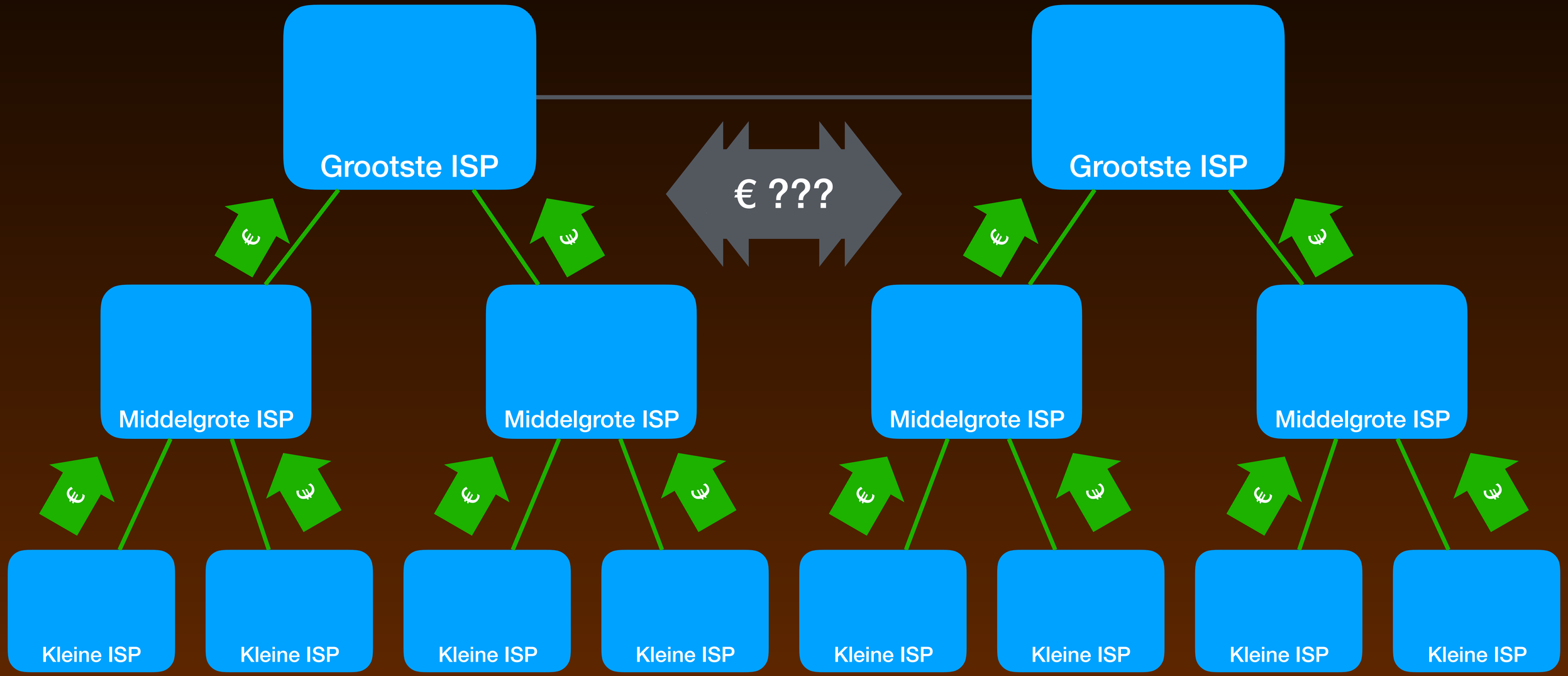
Transit: klein betaalt groot



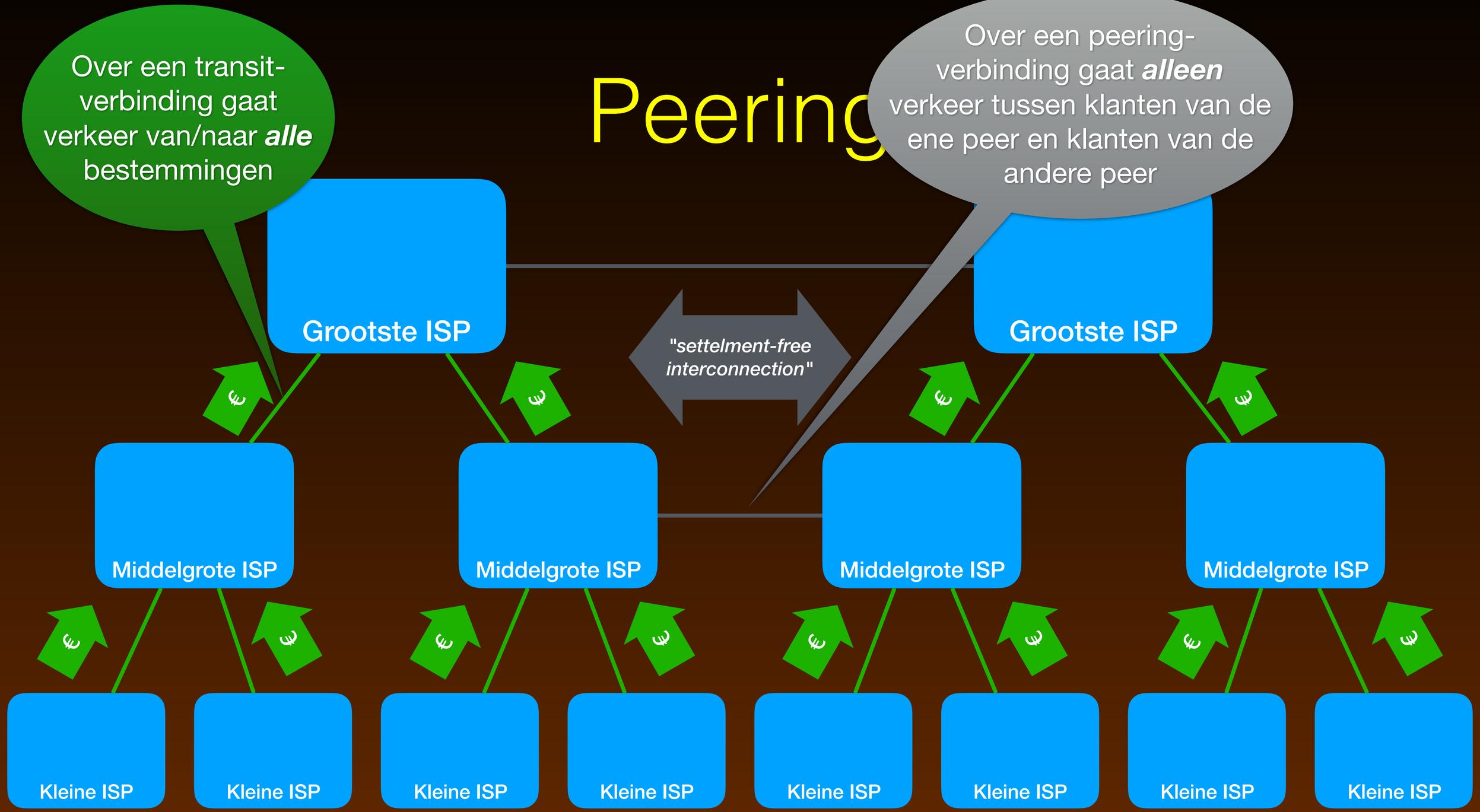
Transit: klein betaalt groot



Peering


Grootste ISP
Grootste ISP
€ ???
Middelgrote ISP
Middelgrote ISP
Middelgrote ISP
Middelgrote ISP
Kleine ISP
Kleine ISP
Kleine ISP
Kleine ISP
Kleine ISP
Kleine ISP
Kleine ISP
Kleine ISP

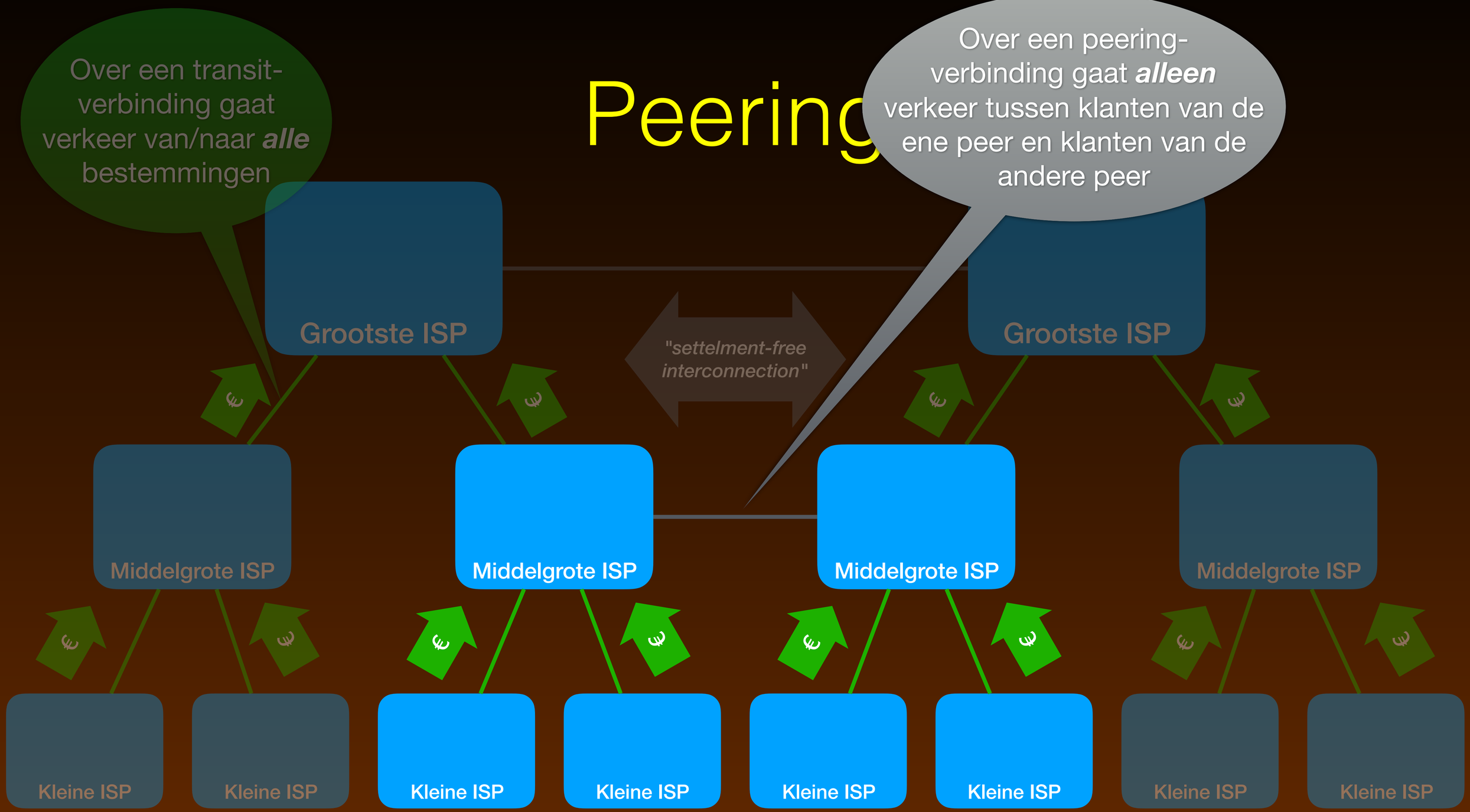
Peering


Over een transit-verbinding gaat verkeer van/naar *alle* bestemmingen
Over een peering-verbinding gaat *alleen* verkeer tussen klanten van de ene peer en klanten van de andere peer
Grootste ISP
Grootste ISP
"settelment-free interconnection"
Middelgrote ISP
Middelgrote ISP
Middelgrote ISP
Middelgrote ISP
Kleine ISP
Kleine ISP
Kleine ISP
Kleine ISP
Kleine ISP
Kleine ISP
Kleine ISP
Kleine ISP

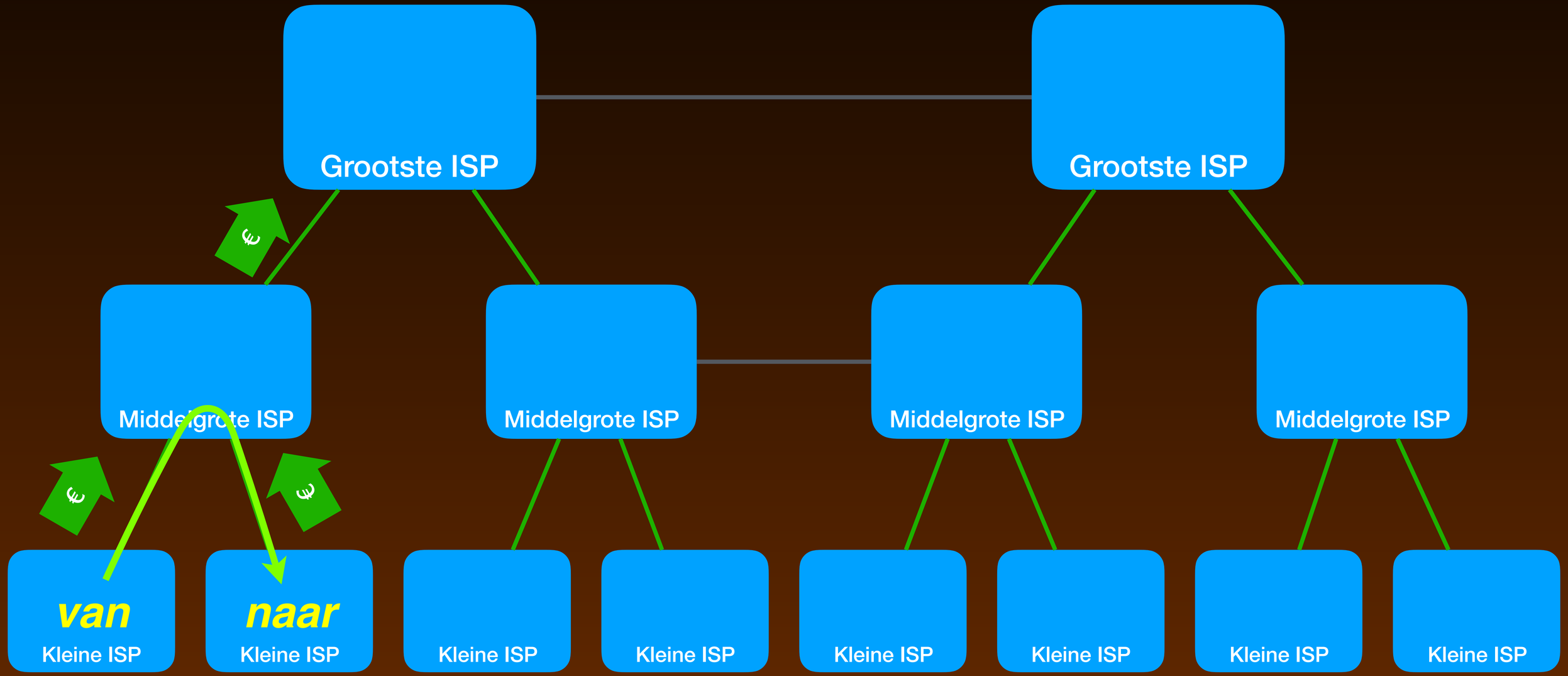
Peering

Over een transit-verbinding gaat verkeer van/naar ***alle*** bestemmingen

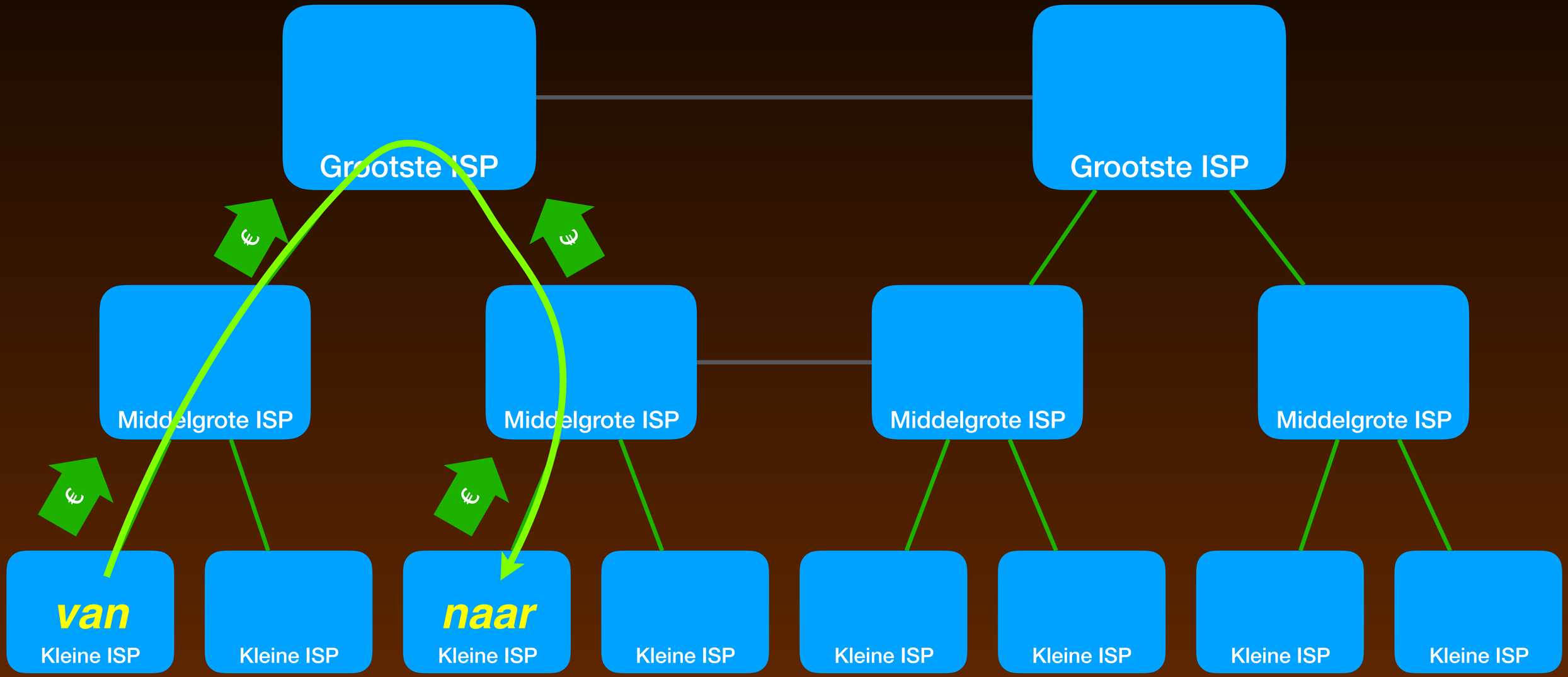
Over een peering-verbinding gaat ***alleen*** verkeer tussen klanten van de ene peer en klanten van de andere peer



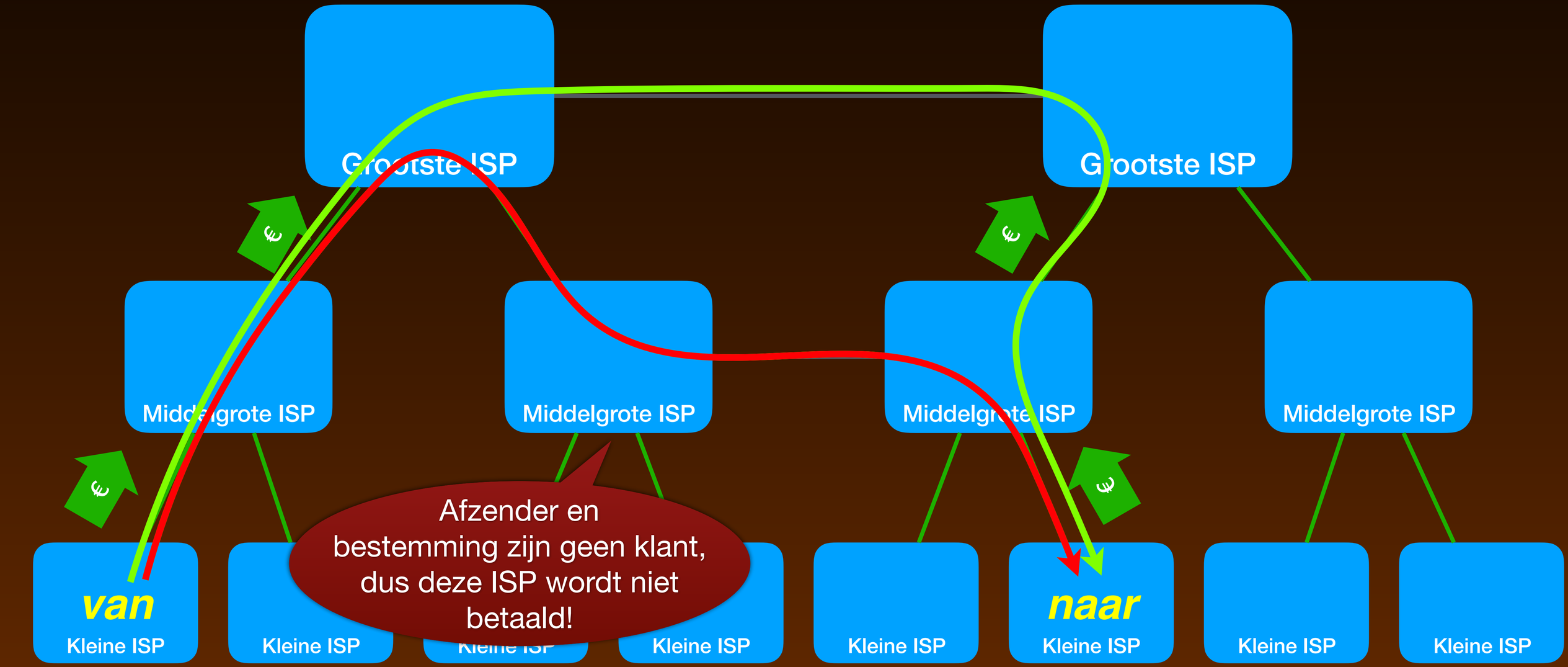
"Valley-free" (1)



"Valley-free" (2)



"Valley-free" (3+4)



Niet-valley-free is een probleem

- Als een pad van A naar B niet dal-vrij (valley-free) is dan is er een financieel probleem
- Maar: in de meeste gevallen ook een praktisch probleem
  - de pakketten kunnen gefilterd worden
  - het onbedoelde pad raakt verstopt door het extra verkeer
- En: een niet-geautoriseerde partij kan het verkeer inspecteren (en misschien zelfs wijzigen)

Problemen met BGP

1. Man-in-the-middle onderschept BGP-pakketten
   - oplossing: TCP MD5 optie
2. Een netwerk "adverteert" adresblok van iemand anders (AWS/Ethereum-incident)
   - slecht werkende oplossing: filters
   - betere oplossing: RPKI origin validation
3. Een netwerk propageert een niet-valley-free pad (meeste incidenten)
   - slecht werkende oplossing: filters
   - wordt aan betere oplossingen gewerkt in de IETF
4. Een netwerk manipuleert BGP om filters en beveiligingsmaatregelen te omzeilen
   - BGPsec

RPKI

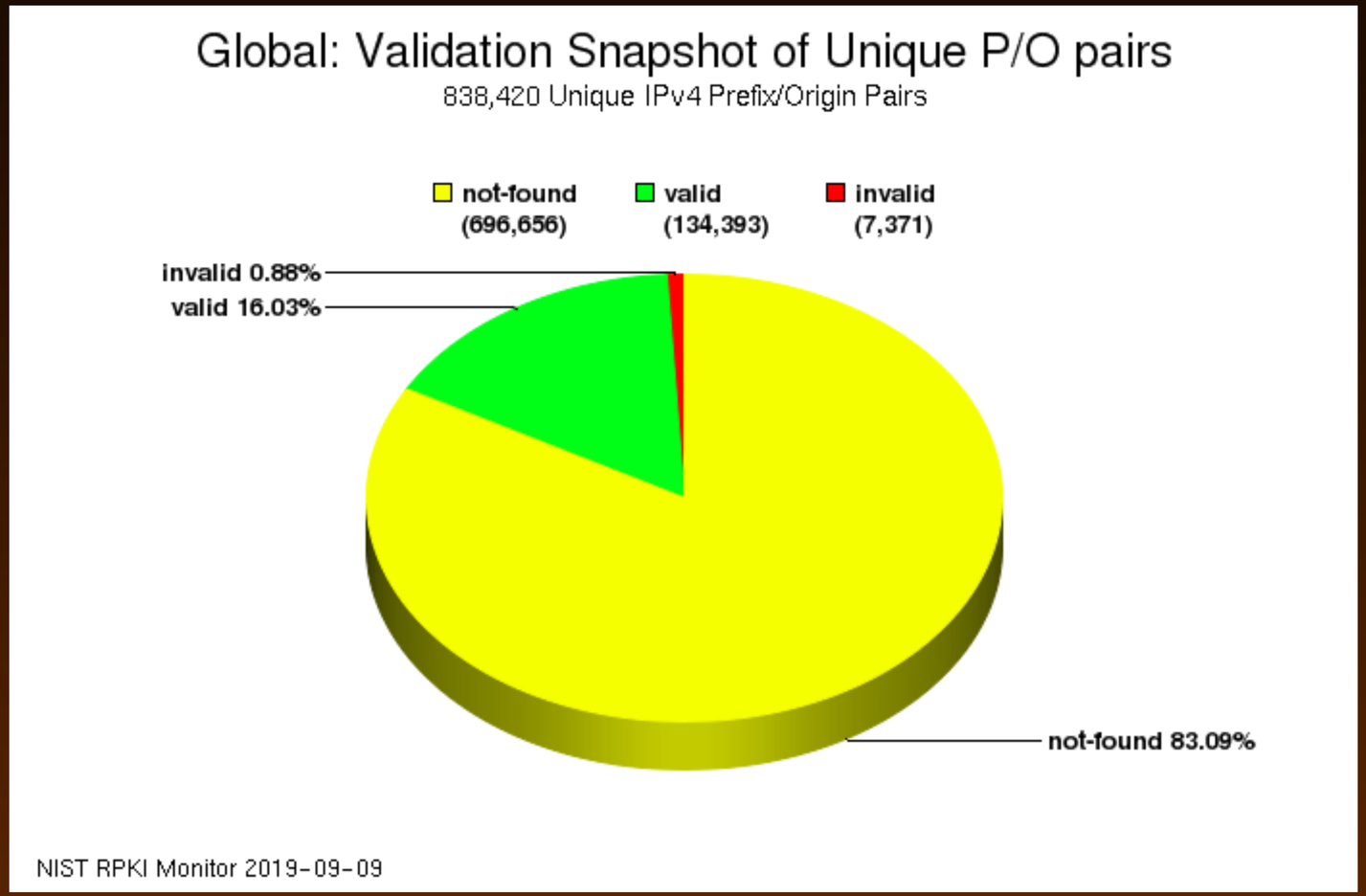
- Resource (AS-nummer of IP-prefix) Public Key Infrastructure
- Prefixhouder krijgt een certificaat van RIR
- Genereert dan een Route Origin Authorization (ROA)
- ROA specifeert welk AS-nummer prefix mag adverteren
- "Relying party software" bij network operator downloadt certificaten en ROAs, controleert de signatures en genereert filter
- Filter wordt naar routers gestuurd met "RPKI to router protocol"
- RPKI weigert ongeldige "originations" **en more specifics**

https://tools.ietf.org/html/rfc6480

RPKI (2)

- Dus: zorg dat klanten die een eigen adresblok hebben altijd ROAs genereren
  - dit gaat via het LIR-portal van RIPE
- Wel opletten bij anti-DDoS-voorzieningen zoals NaWas
  - bijvoorbeeld:
    - klant heeft 100.64.0.0/22 en 100.64.1.1 wordt aangevallen
    - anti-DDoS-voorziening adverteert 10.64.1.0/**24** om het aanvallende verkeer naar zich toe te trekken en "wast" het
    - *dan moet er wel een ROA zijn die dit toestaat*
- Zelf BGP filteren op basis van RPKI is ook wenselijk, maar ingewikkelder

Wereldwijde status RPKI ROAs



https://rpki-monitor.antd.nist.gov

Route leaks

- De meeste route leaks komen door "valleys" (RFC 7908 types 1 - 4)
- Het BGP AS-pad laat wel zien welke netwerken het pad vormen van A naar B
- Maar niet de business-relatie tussen deze netwerken
- Het is dus niet mogelijk een fout verderop alsnog te detecteren en herstellen
- Binnen de IETF nu voorstellen om deze informatie ofwel in BGP zelf te stoppen ofwel in RPKI zodat hierop filteren wel mogelijk wordt
- Maar... de IETF is niet erg snel, moet daarna nog in apparatuur geïmplementeerd worden

BGPsec

- Lange adem: zo'n 20 jaar aan de specificatie gewerkt
- Doel: het AS-pad in BGP beschermen tegen manipulatie
  - het AS-pad is een lijst van alle "hops" (netwerken/ISPs) om bij de bestemming te komen
- Problemen:
  - aanvallen kunnen op dit moment ook effectief zijn zonder deze manipulatie
  - lastig te zien hoe je BGPsec in stappen in kan voeren
  - BGPsec is een heel "zwaar" protocol dat veel geheugen een CPU-capaciteit gebruikt
    - routermakers implementeren het (nog?) niet

https://tools.ietf.org/html/rfc8205

Vragen?

iljitsch@muada.com

http://www.bgpexpert.com/presentations/nivo-bgp-rpki-2019-09.pdf