ECP

Platform voor de InformatieSamenleving

Masterclass Internet

Alles wat u al wilde weten maar nooit durfde te vragen

Internet is een containerbegrip. Want eigenlijk bestaat het internet uit een enorm scala aan grote en kleine onderwerpen, de ene nog complexer dan de ander: van standaarden en technische toepassingen tot toegankelijkheidsvraagstukken en criminaliteit. Van privacy en veiligheid tot bestuurlijke vragen en ethiek. Nationaal en internationaal. Het doorgronden van de werking, de problemen en oplossingen vereisen veel achtergrondkennis. En die is niet altijd even toegankelijk.

Daarom organiseerde ECP op 28 juni 2018 een Masterclass Internet. Professor Michel van Eeten (TUDelft) en Michiel Steltman (DINL) gaven in deze masterclass antwoord op echt alle vragen over internet.

Prof. dr. Michel van Eeten is hoogleraar Bestuurskunde bij de sectie Organisation & Governance (OG) aan de TU Delft, en specialist in internetveiligheid.
Hij adviseerde het ministerie van Economische Zaken, de Internationale Telecommunicatie Unie en de OESO over onder meer beheer, beveiliging en betrouwbaarheid van kritieke infrastructuur.

Michiel Steltman is directeur van Stichting DINL.
In die functie brengt hij de belangen van de Nederlandse digitale infrastructuur sector onder de aandacht. Belangrijke thema's zijn daarbij de promotie van Nederland als vestigingsplaats voor online diensten, het bijdragen aan goed IT-onderwijs en digitale innovatie en het werken aan vertrouwen en informatieveiligheid. Zijn omvangrijke inhoudelijke kennis van zaken en technische achtergrond geeft hem een voorsprong bij menig thema. Hij is tevens columnist en blogger en spreekt met regelmaat en met passie over de ins en outs van de Nederlandse online sector.

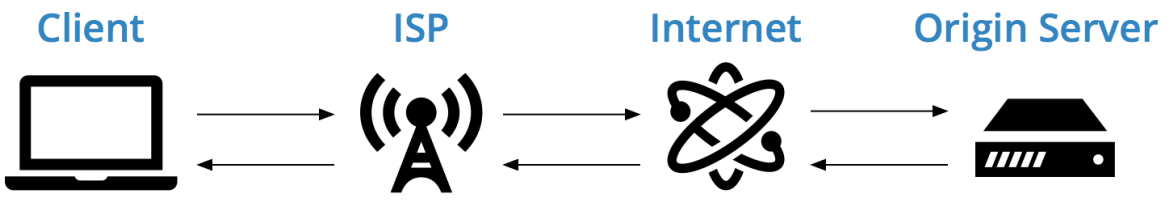
1. Hoe ziet de digitale online wereld eruit?

Om deze vraag te kunnen beantwoorden begint Michiel Steltman eerst bij de anatomie van de digitale wereld:

De digitale wereld bestaat uit een infrastructuur (datacenters, glasvezel, servers etc.) en daarop draaien digitale services (digitale diensten) en de gebruikers noemen we de digital enabled society.

2. Hoe maakt een pc connectie met internet?

Michiel Steltman legt aan de hand van onderstaand simplistisch schema uit welke route zo'n connectie aflegt**:**



Client: is de laptop/pc of smartphone van de gebruiker.
ISP: Internet Service Provider verbindt de gebruiker aan het internet: de ISP levert een transit dienst. Voorbeelden van ISPs zijn Ziggo en KPN.
Internet: het internet is een netwerk van netwerken; is het netwerk waar de ISP verbinding mee maakt om informatie op te halen. Dit is een samenraapsel van 55.000 netwerken.

IP Adres: over het algemeen heeft ieder huishouden 1 IP adres. IP adressen worden per router uitgegeven.

Router: Meestal staat dit kastje in je meterkast. Deze zorgt ervoor dat alle apparaten thuis verbinding kunnen maken met het internet (via dit kastje). Dit kastje noem je ook een accespoint.

Origin Server: de plek waar de informatie staat die de gebruiker nodig heeft of zoekt.

3. Welke verbindingen zijn er?

Volgens Michiel Steltman zijn er 3 soorten verbindingen:

Transit verbinding: Als u het internet op wilt vraagt u als client om data. Via uw router verbindt de ISP uw computer/device aan het internet en levert hiermee een transit dienst. Transit is dus een netwerk waarbij u thuis aansluit op het grote internet/ world wide web.

En 2 soorten peering verbindingen:

Peering is een term die gebruikt wordt om netwerken aan elkaar te knopen.

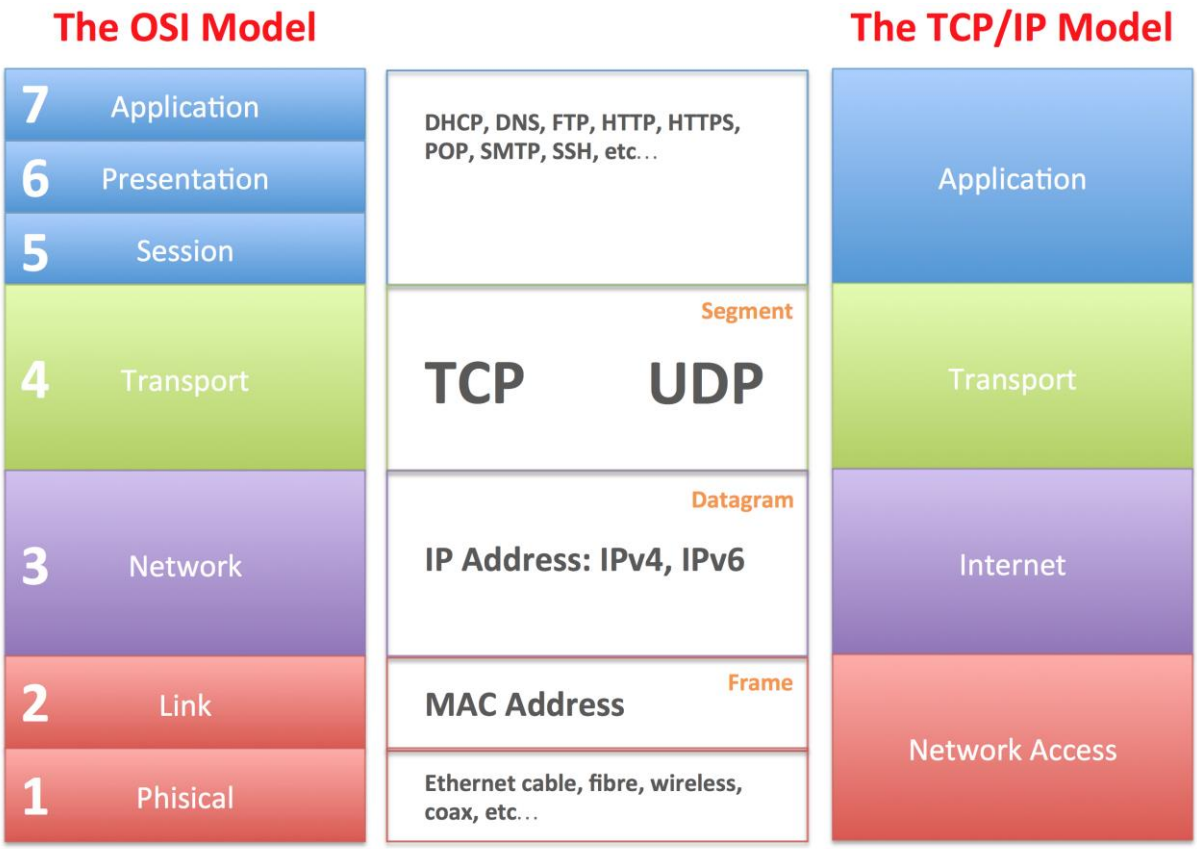
- **Private Peering**: voorbeeld: Ziggo maakt onderling afspraak met Netflix en koppelt dan rechtstreeks in het datacenter. Een kabel van de ene server naar de andere.
- **Public Peering**: dan wordt gekoppeld via een internetknooppunt (AMS-IX). Bijvoorbeeld, KPN koppelt via AMS-IX met Facebook. Van deze knooppunten (zoals AMS-IX) zijn er tientallen ter wereld. Je kunt ze ook vergelijken met een kroonsteentje in een elektriciteitsnetwerk.

Door de vele netwerken zijn ook veel routes over het internet mogelijk. Maar sommige routes zijn goedkoper.
Nu de verkeersstromen groter worden, wordt steeds meer aan private peering gedaan in datacenters, dus rechtstreeks. De route is dan korter, dit is efficiënter, sneller en goedkoper. De response tijd is afhankelijk van hele keten, maar als kabels korter zijn, is het sneller. Hoe dichterbij de client, hoe sneller.

Voorbeeld:
Het datacenter van Google in Delfzijl heeft een grote aantrekkingskracht op andere internetspelers. Google heeft daar in de Eemshaven in 2016 een eigen datacenter neergezet. Dit gebied groeit nu enorm omdat er steeds meer andere bedrijven in de buurt willen zitten zodat zij door middel van private peering kortere connecties kunnen maken.
Ditzelfde gebeurt in Amsterdam met de Amsterdam Internet Exchange (AMS-IX). Netflix heeft daar data centers staan vanwege deze belangrijke internet hub, en omdat Nederland zoveel afnemers van Netflix heeft (dicht bij de client dus).

4. Wat is OSI?

Als we pakketten (of data) willen uitwisselen via het internet moeten we standaarden afspreken. Dat gebeurt op basis van het OSI (Open Systems Interconnection) model, zo vertelt Steltman. Dit is een conceptueel model om de communicatie functies van telecommunicatie of computersystemen te karakteriseren en standaardiseren onafhankelijk van de onderlinge interne structuren en technologie. Het originele model bestaat uit 7 lagen. Een laag dient de laag erboven en die laag dient op zijn beurt weer de laag daarboven.



Uitleg OSI Model:

1. **fysieke laag**: internet verbinding: ethernet (hoe ziet de kabel eruit, hoeveel volt, hoe ziet de stekker eruit)
2. **datalink laag / frame:** hoe kunnen apparaten elkaar herkennen. MAC adress. Elk apparaat heeft een uniek nummer (hardware). Hoort bij apparaat en dat identificeert het apparaat. Internationale standaard voor uitgave van mac-adressen.
3. **netwerk laag / datagram: IP adress** (internet)
4. **transport laag /segment:** TCP en UDP. Dit zijn transport protocollen. TCP : wordt gebruikt voor e-mail. Bij e-mail is het belangrijk dat je weet dat je bericht is aangekomen. TCP geeft een bevestiging van ontvangst terug. UDP wordt veelal voor gaming en streaming gebruikt want die geeft geen bevestiging van ontvangst terug (daar is de dienst ook veel te 'zwaar' voor), maakt niet uit of alle pakketjes aankomen.
5. **sessie laag**

6. **presentatie laag / protocolstack**
7. **applicatie laag / toepassingen: afhankelijk van wat je wilt doen, maak je afspraken.**

De lagen 5,6 en 7 gaan met name over de vragen: wat wil je doen? Het zijn sessies. Zoals http: protocol. Client stuurt verzoek naar de server die begrijpt wat het moet doen en die server stuurt terug (ik heb hem ontvangen en weet wat ik moet doen).
HTTPS: zelfde protocol maar versleuteld.
SMTP: email protocol.
POP: mail ophalen (gebruikten we vroeger veel).

5. Ik hoorde dat de IP adressen op zijn, klopt dat?

De uitleg wordt gegeven door Michiel Steltman:

Wat is een IP adres?
Een IP adres is een groot getal. Bestaande uit 4 porties van 254 nummers, zogenaamde IPv4 nummers. U kunt zich voorstellen dat dit gigantisch veel unieke nummers oplevert. Doorgaans heeft ieder huishouden of kantoor een eigen IP adres, dat is ook heel haalbaar. Zogenaamde *prefix brookers* handelen in IPv4 adressen, mocht u er 1 nodig hebben.

Zijn alle IP adressen niet al op?
Alle IP adressen zijn al uitgegeven maar nog niet allemaal in gebruik. We kunnen nog wel even door. ISP's geven ook dynamische IP adressen uit. Dynamische IP-adressen kunnen door meerdere abonnees worden gebruikt. Daarnaast zijn computers van bedrijven en instellingen vaak via één IP adres met internet verbonden. Daarom is naast een IP adres ook een datum en tijd belangrijk. De echte IP adressen zitten aan de Transit kant.

Wat is de oplossing?
IPv6 is de oplossing. Dat zijn IP adressen die zijn opgebouwd uit 6 porties. Echter kent implementatie van deze adressen wat hobbels. Zo moet eigenlijk een schaduw internet over het oude worden gelegd, zogenaamd *dual stack*. Bovendien moeten alle apparaten dan IPv6 kunnen verzenden en ontvangen. IPv6 heeft meer ingebouwde beschermingsmogelijkheden. Maar IPv6 betekent op dit moment nog niet dat je geen certificaten nodig hebt, want IPv6 wordt nog niet overal goed gebruikt.

6. Wat is VPN in bovenstaand verhaal?

VPN staat voor Virtual Private Network. Niet de inhoud, maar de gehele boodschap/verbinding wordt versleuteld, vertelt Steltman.
In de praktijk betekent dit dat er een privénetwerk van computers gecreëerd kan worden met de infrastructuur van een publiek netwerk. Over het internet wordt dan een versleutelde beveiligde verbinding gemaakt tussen verschillende lokale netwerken en/of computers. Hierdoor is het mogelijk om op een veilige manier data uit te wisselen tussen verschillende computers en netwerken.

7. Wat is boarder gateway protocol (BGP)?

Daar kan Michiel Steltman kort over zijn: een routing protocol.
Dit is het belangrijkste routeringsprotocol van het internet; het wordt gebruikt om verkeer tussen verschillende providers te routeren. Het is een methode om aan andere BGP-routers te vertellen dat bepaalde prefixes bereikbaar zijn via de router (ze worden als het ware geadverteerd). De daadwerkelijke routering gebeurt binnen dat netwerk en wordt via interne routeringsprotocollen gedaan. Als 2 BGP-routers een sessie opzetten, dan zijn ze elkaar 'peers'. Als er niet betaald wordt, noem je dit peering. Adverteren van wie je bent en wat je kan en welke IP adressen achter mij zitten: is essentie van BGP (*prefixes* laten weten). Maar als de verkeerde informatie wordt geadverteerd, kan het zijn dat je de verkeerde informatie krijgt.

Voorbeeld:
Een kleine handmatige menselijke fout kan er voor zorgen dat bijvoorbeeld alle verzoeken voor Youtube filmpjes uitkomen bij 1 bepaald netwerk en dit netwerk daar niet op berekend is en dan plat gaat (in plaats van dat ze geblokkeerd worden). Zo gebeurde in 2008 in Pakistan. Een Pakistaanse ISP adverteerde met de verkeerde informatie waardoor al het verkeer bestemd voor YouTube bij hen uitkwam. Hun netwerk kon het niet aan en YouTube was 2 uur onbereikbaar.
Bron: CNET https://www.cnet.com/news/how-pakistan-knocked-youtube-offline-and-how-to-make-sure-it-never-happens-again/

Voorbeeld: In 2017 gebeurde het dat grote delen van Japan geen internettoegang hadden doordat Google een verkeerde BGP advertentie had verstuurd. Waarschijnlijk was dit een menselijke fout. Hierdoor werden 135.000 verkeerde prefixes verstuurd waardoor internetverkeer dat voor andere netwerken was bedoeld, via het netwerk van Google ging. Maar liefst zeven miljoen klanten ondervonden internetproblemen. Echter duurde deze maar 40 minuten.
Bron: Tweakers https://tweakers.net/nieuws/128833/google-fout-met-bgp-protocol-leidde-tot-internetproblemen-bij-veel-japanners.html

8. Wat is het geheim van het internet?

Het internet hangt samen met protocollen en soms gaat het mis, zoals bijvoorbeeld met de BGP. Maar het gaat eigenlijk al 25 jaar goed, zegt Michel van Eeten. De community is heel sterk. Problemen worden adhoc opgelost en het principe van vrij, veilig en open wordt breed uitgedragen. Juist het internet met Ducttape en pleisters aan elkaar hangt is ook de kracht ervan, aldus Van Eeten.

9. Hoe ziet de digitale infrastructuur er uit?

Onderstaand schema van Michiel Steltman geeft duidelijkheid:

10.Wat zijn hosters, resellers en datacenters?

Michiel Steltman legt uit:

Hoster: verhuurt de ruimte op een server. Dit groeit vaak uit tot een datacenter door meerdere servers op 1 plek te zetten .

Reseller: is een hosting bedrijf, maar gebruikt van servers van anderen. Veel voorkomend voorbeeld: een Nederlands hosting bedrijf met servers in Oekraïne.

Datacenter: een fysiek plek waar meerdere servers staan.

11.Zeekabels?

Ja, zeekabels, vertelt Steltman. Om internetverkeer van het ene naar het andere continent te krijgen liggen er daadwerkelijk kabels op de bodem van de oceaan, zogenaamde zeekabels. De kabel bestaat uit glasvezels in gebed in een gel van aardolie met daaromheen verschillende lagen. Dat biedt een goede bescherming tegen o.a. het zout en de hoge druk op de bodem. Deze kabels gaan ongeveer 25 jaar mee. Zeekabels kun je kopen maar worden veelal gehuurd.

12.Internet en landsgrenzen Hoe zit dat nou precies?

Zelfs in de simpelste vorm van cybercrime heb je al snel te maken met apparaten die zich in diverse landen bevinden, legt Van Eeten uit. Je kunt die herleiden en dat heeft dus een geografische verschijning. Dus op basis van fysieke aanwezigheid van apparaten kan je routering zien.
Een IP adres hoort bij hostingbedrijf x en dat bevindt zich in NL en dan moet ik bij Nederlandse politie zijn. Wij hebben geen andere model dan een geografisch model gebaseerd op jurisdictie. Wel wordt gebruik gemaakt van extra territoriale jurisdictie: ik geef mezelf recht om in het buitenland in computers te mogen. Dat doet Nederland maar ook andere landen.

13.Hoe weten bepaalde landen grip op internet te krijgen?

Verschillende landen doen dat op verschillende manieren, zegt Michel van Eeten.

Bijvoorbeeld Rusland: Als zij alle IP adressen van buiten Rusland zouden blokkeren zijn ze ook diensten kwijt die Russische bedrijven gebruiken. Dat is slecht voor de Russische Economie. Je zou dat 'neven schade' kunnen noemen. Rusland kiest er dan ook voor om gerichter te blokkeren. Zo willen zij bijvoorbeeld berichtenservice Telegram weren. Rusland geeft bevel aan de betreffende ISP. ISP voert bevel uit en blokkeert alleen het IP adres van Telegram. Maar Telegram gaat gewoon andere IP adressen gebruiken, dus dat schiet niet op.

Bijvoorbeeld China: Zij zijn wat meer meedogenloos. China staat ook wel bekend om zijn 'Great firewall of China". Dat betekent dat al het verkeer in en uit China wordt gecensureerd. Zij blokkeren dus alle IP adressen van buiten hun land. Maar hebben dan ook hun eigen marktplaats (Ali express), zoekmachine (Baidu) om de diensten die hun burgers wensen wel te kunnen leveren.

14.Hoe verhouden IP adressen zich tot locatie?

Michel van Eeten ziet twee antwoorden:

- Antwoord 1 zou zijn: er is geen relatie
- Antwoord 2 is: die is er eigenlijk wel: Bij de uitgave van IP adressen zijn de adressen verdeeld in blokken en die zijn per continent verspreid. Dus je zou kunnen zeggen dat IP adressen uit serie X bij continent Y horen. Nu zijn er bedrijven die er een sport van maken om te kijken waar die IP adressen zijn. Dat doen ze door er tegen te 'praten' en dan de 'trace route' te volgen (de route van het pakketje). Bijvoorbeeld: What is my IP.com
  Als je beheersing van internet wilt bemoeilijken moet je IP adressen gaan verhandelen. En dat gebeurt. Dus IP adressen van continent laten wisselen.

De organisatie die de IP adressen in Europa beheerd is RIPE NCC.

15.Wordt het moeilijker om internet te controleren voor landen?

Zoals Van Eeten al vertelde in het voorbeeld van Rusland in vraag 15 helpt controle op gebied van IP-adressen niet.
Hoe kan je dan wel grip krijgen? Door hoger in OSI model te kijken naar grote spelers, zegt Van Eeten. Grip op internet is grip op Google, WhatsApp, Facebook etc. Deze bedrijven kan je proberen onder druk te zetten, mee te onderhandelen, wetgeving op los te laten. Voor kleine spelers geldt dit minder, zij zijn hier niet zo vatbaar voor. Zij stappen op en beginnen in een ander land opnieuw. Zij verplaatsen veel en switchen steeds van hosters.

Voorbeeld: Pirate Bay. Een website die muziek, films, games en software gratis te downloaden aanbiedt. Het was/is een frustratie van de filmwereld. Sinds de oprichting in 2003 verhuizen ze steeds van hoster. Het werd een kat en muis spel. Steeds weer dook de website op, of via een andere server (omdat ze in beslag waren genomen) of via onder een nieuwe naam, of met nieuwe domeinnamen. Het is
een civiel rechtelijk probleem. Internet aanbieders hebben namelijk wettelijke bescherming en zijn niet verantwoordelijk voor de inhoud van wat ze hosten. Zij mogen dus de content 'gewoon' doorgeven en hoeven hun klanten niet te weren.

16.Hoe komen internetstandaarden de wereld in?

Er is een wereldwijde Internetstandaarden producent, de Internet Engineering Task Force (IETF), vertelt Michel van Eeten. Echter wordt 95 % van hun werk genegeerd omdat er geen behoefte aan is. Het zijn mooie standaarden, maar ze hebben last van de 'wet van de remmende voorsprong'. Veel internetstandaarden worden niet opgepakt, omdat je er pas wat aan hebt als iedereen het doet.

Voorbeeld: Phishing: 15 jaar geleden zijn al standaarden ontwikkeld die phishing tegengaan. Iedereen moet dan wel die standaard invoeren en dat kost tijd en werk. De protocollen van de mailserver moeten bijvoorbeeld worden aangepast. Maar als niet iedereen dat doet (want kost tijd en geld), dan werkt het niet.

17.Wat zijn AS nummers?

Michel van Eeten geeft antwoord:

AS staat voor Autonomous System: autonome systemen. Het internet bestaat uit 55.000 netwerken ofwel Autonome systemen. Maar hoe weet ik naar wel AS mijn pakketje moet? Daarvoor zijn er ASnummers, zoals AS4 1-2-3-4-5.

Router AS1 zegt tegen AS2 dat als je een bepaalde reeks zoekt, moet je bij mij zijn. Dit heet adverteren (pre-fix, zie ook vraag 8 BGP). Dit gebeurt op basis van vertrouwen en wordt automatisch doorgezet. Dat klinkt naïef: in de praktijk valt dat wel mee. Mensen bouwen zelf

mechanismen in. Zit veel veerkracht in omdat veel bottumup gedaan wordt en veel met de hand bijgestuurd.

Voorbeeld: beheerder van AS neemt niet altijd automatisch de advertenties over.
Er wordt met de hand bijgestuurd; uit economisch perspectief: als je moet betalen uit AS2 wil je dat niet en wil je alleen AS3 doorzetten.

18. Wanneer zou je eigen AS willen?

Als je zelf wilt sturen op de routing van je product, antwoordt Michel van Eeten.
Stel je hebt meerdere locaties (meerdere spullen in meerdere locaties) zoals Netflix.
Het is voor hen niet echt handig als de Netflix in NL klanten in Japan antwoord gaat geven.
Als zij hun eigen AS hebben, kunnen zij zelf bepalen welk verkeer ik naar welk onderdeel gaat.

19. Standaarden: soms best lastig om die een stap verder te krijgen; zelfde geldt bij IPv6. Zitten we vast?

Ja, zegt Van Eeten eerlijk. Transitie in de internetwereld gaat heel traag. Pas als de noodzaak er is dan gebeurt er wat. De clou is dat íedereen het moet doen, anders werkt het niet. Dat geldt voor standaarden, maar ook voor de overstap naar IPv6.
Investeringen nu hebben geen zin als niemand nog IPv6 gebruikt.
Noodzaak is hoog in Azië. Daar is een tekort aan IPv4 adressen en dus is IPv6 uitrol al gedaan. Maar voorlopig is IPv4 nog 10 jaar bruikbaar, zo voorspelt Van Eeten.

20. Slotvraag:
Het internet bestaat uit briljante protocollen omgeven door lapmiddelen. Stel we zouden opnieuw beginnen. Wat zou je willen veranderen?

Michiel Steltman:
Michiel kijkt vooral naar de lessen van Kees Neggers, sleutelfiguur in de ontwikkeling van het internet in Nederland en sinds 2013 opgenomen als Internet Pioneer in de Internet Hall of Fame, die zegt dat er verandering moet komen in de IP adressering en een onderverdeling in gebruikszones. Denk bijvoorbeeld aan het gebruik van TCPIP voor het uitwisselen van wetenschappelijke data.

Michel van Eeten:
Michel zou niets veranderen . Belangrijke reden waarom het nu goed werkt, is omdat het juist ooit bedacht is zonder toestemming.
Juist die lapmiddelen zijn het geheim van het internet. Het werkt zo goed omdat het evolutionair is. Het knip en plak werk. De chaos die we hebben is een zege. Bij poging tot ontwrichting is deze teringbende moeilijk te ontregelen. Het vindt altijd wel weer zijn weg door al die duizenden netwerken.