dialogic
innovatie • interactie

Netwerkneutraliteit: stand van zaken in Nederland

In opdracht van:
Ministerie van Economische Zaken
DGET - TM

Project:
2008.071
Publicatienummer:
2008.071-0905
Datum:
Utrecht, 10 juni 2009

Auteurs:
Dr. Rudi Bekkers
Ir. Reg Brennenraedts
Ir. Stein Smeets
Drs. Robbin te Velde

Inhoudsopgave

1 Inleiding

1.1 Aanleiding

Netwerkneutraliteit staat al een aantal jaar op de agenda. De discussie is begonnen in de Verenigde Staten en wordt daar, om verschillende redenen[1], nog altijd het meest intensief gevoerd. Echter, ook in Europa krijgt het onderwerp steeds meer aandacht: bij de herziening van het huidig Europees regelgevend kader is netwerkneutraliteit een belangrijk onderwerp en in haar beleidsbrief convergentie van augustus 2008 besteedt het Ministerie van Economische Zaken er expliciet aandacht aan.[2]

Naar aanleiding van die beleidsbrief heeft het Ministerie van Economische Zaken Dialogic gevraagd de stand van zaken wat betreft netwerkneutraliteit in Nederland in kaart te brengen. Want het onderwerp mag dan al een tijd lang bediscussieerd worden, het blijft onduidelijk in hoeverre netwerkneutraliteit ook in de praktijk tot problemen leidt. Aansluitend gaat het onderzoek nader in op de rol die de overheid in deze problematiek speelt en kan spelen, met name met betrekking tot het vergroten van transparantie over netwerkneutraliteit.

In deze eindrapportage komen deze onderwerpen als aparte hoofdstukken terug:

- **De huidige marktsituatie**. Hoe kijken verschillende belanghebbenden aan tegen netwerkneutraliteit? Welk beleid voeren telecommunicatieaanbieders ten aanzien van netwerkneutraliteit? In hoeverre spelen er in Nederland problemen met netwerkneutraliteit? Zie hoofdstuk 3.
- **Transparantie** over netwerkneutraliteit. In hoeverre levert de huidige mate van transparantie voor eindgebruikers problemen op? Hoe kan het vergroten van transparantie vorm gegeven worden? Zie hoofdstuk 4.
- **De toekomstige marktsituatie**. Hoe zal netwerkneutraliteit zich in de Nederlandse markt naar verwachting ontwikkelen? Hoe kan het Ministerie van Economische Zaken bij deze ontwikkeling(en) betrokken blijven? Zie hoofdstuk 5.

In dit hoofdstuk komen achtereenvolgens de onderzoeksvragen (paragraaf 1.2) en de onderzoeksmethodiek (paragraaf 1.3) aan de orde. Hoofdstuk 2 geeft een inleiding in het debat over netwerkneutraliteit en – essentieel om dat debat goed te kunnen volgen – een globale beschrijving van de werking van het internet. Hoofdstuk 6 vat de belangrijkste leerpunten samen.

1.2 Onderzoeksvragen

Overeenkomstig de drie centrale hoofdstukken van dit rapport heeft onderliggend onderzoek drie doelstellingen, zie hieronder.

---

[1] Er lijkt consensus te bestaan dat netwerkneutraliteit in de Verenigde Staten meer in het geding is dan in Europa. Verder in dit rapport gaan we daar dieper op in.

[2] Ministerie van Economische Zaken (2008). *Beleidsbrief convergentie*. http://www.ez.nl/dsresource?objectid=158451&type=PDF

Doelstelling 1: Schetsen van de huidige marktsituatie
Onderzoeksvragen:

a. Welke problemen worden momenteel gesignaleerd met netwerkneutraliteit in Nederland? Hoe verhoudt zich dat tot ervaringen uit het buitenland?

b. Hoe kijken verschillende stakeholders (toegangsaanbieders, netwerkeigenaren, content - en dienstenaanbieders, consumenten) aan tegen (schendingen van) netwerkneutraliteit?

c. Wat voor beleid m.b.t. netwerkneutraliteit voeren netwerkeigenaren en toegangsaanbieders op de vaste en mobiele markt?

    i. Welk type verkeer wordt op welke wijze gediscrimineerd of geblokkeerd?

    ii. Welke motivatie ligt daaraan ten grondslag?

Doelstelling 2: Vergroten van transparantie
Onderzoeksvragen:

d. Hoe transparant zijn marktpartijen over netwerkneutraliteit en hun eventuele ingrepen daarin? Is het voor consumenten en content- en dienstenaanbieders helder welke content en diensten geblokkeerd of gediscrimineerd worden?

e. Beoordelen de verschillende belanghebbenden de huidige mate van transparantie als voldoende? Worden er tekortkomingen ervaren, zo ja welke?

f. Zijn effecten van niet-transparante aanbieders zichtbaar?

g. Wat zijn de eventuele kosten en nadelen van het vergroten van transparantie? Is het vergroten van transparantie inderdaad een no-regret optie?

h. Hoe kan het vergroten van transparantie het beste (effectief, efficiënt, duurzaam) vormgegeven worden?

    i. Wat zou precies transparant moeten zijn? Wat is zinvol en haalbaar om transparant te maken?

    ii. Moet er een onderscheid gemaakt worden tussen content en diensten?

    iii. Moet er een onderscheid gemaakt worden tussen vaste en mobiele markten?

    iv. Welke partijen moeten transparant zijn?

    v. Naar welke partijen moet transparant gecommuniceerd worden?

i. Welke rol heeft de overheid bij het vergroten van transparantie, bijvoorbeeld door het stimuleren van zelfregulering of door transparantie vast te leggen in regelgeving?

Doelstelling 3: Monitoren van de toekomstige marktsituatie
Onderzoeksvragen:

j. Verwachten betrokkenen dat de situatie aangaande netwerkneutraliteit in de toekomst significant zal veranderen?

k. Hoe kan het Ministerie van Economische Zaken de markt het beste blijvend monitoren?

1.3 Aanpak

Binnen onderliggend onderzoek zijn drie verschillende onderzoeksmethodieken ingezet. Een deel van het rapport is tot stand gekomen op basis van desk research. Dat behelsde een analyse van wetenschappelijke papers (zowel uit de VS, Europa als Nederland), een analyse van (online) artikelen en een analyse van internetfora over het onderwerp. Een overzicht van geraadpleegde literatuur is te vinden in bijlage A.

Bevindingen uit desk research zijn aangevuld op basis van semi-gestructureerde interviews met twintig (voornamelijk Nederlandse) belanghebbenden en experts. Er is gesproken met zes aanbieders van content en diensten, met zes aanbieders van vaste en mobiele ISP-diensten, met drie vertegenwoordigers van eindgebruikers en met vijf (technisch) experts. Interviewverslagen zijn in de meeste gevallen teruggekoppeld aan de betreffende interviewees en zonodig aangepast. Een overzicht van geïnterviewde personen is te vinden in bijlage B.

De uitkomsten van desk research en interviews zijn getoetst tijdens een validatieworkshop. Overigens lag de focus van die workshop op de tweede onderzoeksdoelstelling: transparantie. Er is uitgebreid stilgestaan bij de noodzaak en mogelijkheden om transparantie te vergroten. Voor de workshop zijn de interviewees uitgenodigd en de leden van het Overleg Post en Telecom van het Ministerie van Economische Zaken. Een overzicht van de aanwezigen tijdens de workshop is te vinden bijlage C.

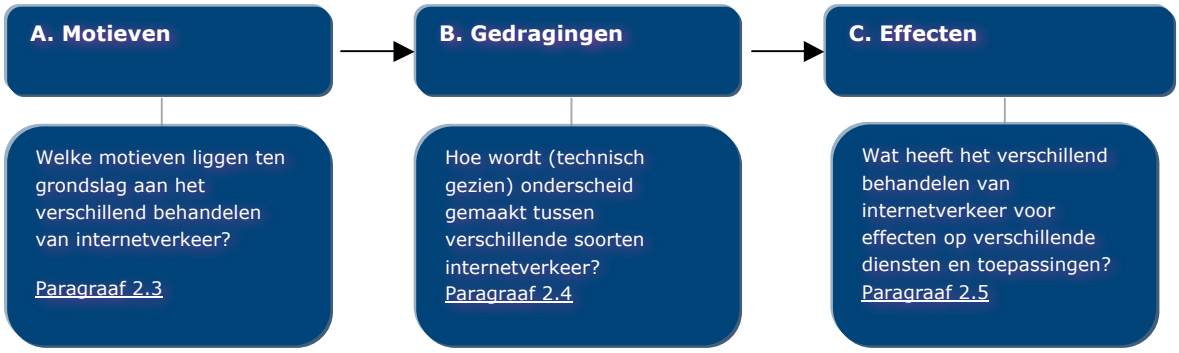
2 Netwerkneutraliteit: een inleiding

2.1 Inleiding

Dit hoofdstuk gaat dieper in op het begrip netwerkneutraliteit, in essentie een discussie over de mate waarin *het verschillend behandelen van internetverkeer* toelaatbaar wordt geacht. De meningen over welke (technische) gedragingen wel of niet tot een schending van netwerkneutraliteit moeten worden gerekend lopen sterk uiteen. Dat kan leiden tot sterk gepolariseerde debatten waarin de voor- en tegenstanders van netwerkneutraliteit langs elkaar heen lijken te praten.

Paragraaf 2.3 bespreekt welke verschillende motieven operators hebben om internetverkeer verschillend te behandelen. In paragraaf 2.4 komt de manier aan bod waarop dit technisch wordt vormgegeven. Paragraaf 2.5 gaat in op de vraag welke effecten deze technische gedragingen (kunnen) hebben op de prestaties van verschillende typen internetdiensten en –toepassingen. We sluiten af met een discussie over de (complexe) verbanden tussen motieven (paragraaf 2.3), gedragingen (paragraaf 2.4) en effecten (paragraaf 2.5).

Een en ander is weergegeven in onderstaand conceptueel model (zie Figuur 1). We proberen het begrip netwerkneutraliteit aldus in de volle breedte te behandelen. Daarmee wordt de discussie misschien niet simpeler, maar wel beter te overzien.



Figuur 1. Conceptueel model van dit onderzoek

Voornoemde definitie geeft het al aan: netwerkneutraliteit zegt iets over hoe om te gaan met internetverkeer.[3] Om de discussie (vooral over de technische gedragingen en onderliggende motieven) in perspectief te kunnen plaatsen is het een vereiste om een

[3] In dit rapport wordt alleen naar content en diensten gekeken die via het publieke internet worden aangeboden; alleen dan kan er immers over *net*neutraliteit worden gesproken. Daar komt bij dat de vergelijking met diensten die niet via het publieke internet worden geleverd (zoals 'interne' VoIP-diensten, maar ook analoge telefonie, analoge televisiedistributie en DVB digitale televisie) zowel technisch en anderszins lastig is. Dat neemt niet weg dat verschillende rapporten en discussiestukken deze afbakening niet zo duidelijk maken en wel diensten meenemen die niet via het publieke internet lopen (zie bijvoorbeeld Tweakers (2009). *FCC vraagt Comcast om opheldering over 'voortrekken eigen voip-dienst'*. http://tweakers.net/nieuws/57958/fcc-vraagt-comcast-om-opheldering-over-voortrekken-eigen-voip-dienst.html).

grondig begrip te hebben van zaken als routering, congestie en interconnectie. Deze begrippen worden in paragraaf 2.2 eerst toegelicht.

2.2 Globale werking van het internet

Het (publieke) internet is een verzameling gekoppelde netwerken waarover pakketten met informatie van de ene computer[4] naar de andere computer vervoerd worden. Deze paragraaf is aan de hand van die constatering gestructureerd:

- Paragraaf 2.2.1 geeft een korte beschrijving van IP-pakketten.
- Paragraaf 2.2.2 beschrijft het transport van internetverkeer (pakketten) *binnen* autonome systemen (netwerken). Een voorbeeld hiervan is het netwerk van een ISP. Daarbij zijn met name de wijze van routering en het risico op congestie interessant.
- Paragraaf 2.2.3 beschrijft het transport van internetverkeer *tussen* autonome systemen (netwerken), de zogenaamde interconnectie. Daarbij wordt met name ingegaan op de financiële afspraken die over de uitwisseling van verkeer gemaakt worden.

2.2.1 IP-pakketten

Computers die over het internet informatie willen uitwisselen, knippen die informatie op en versleutelen het tot IP-pakketten. Zo'n pakket bestaat uit verschillende *headers* en de *body*. De headers bevatten informatie over de afkomst en bestemming van het pakket (de computers, beide beschikken over een uniek adres), de lengte van het pakket, de *time to live* (een pakket wordt na een bepaalde tijd vernietigd omdat het anders, mocht het de weg kwijt raken, voor eeuwig over het internet zou blijven zwerven), et cetera. De body bevat een deel van de te versturen informatie. Deze pakketten worden los over het internet getransporteerd. Als we in latere paragrafen over internetverkeer spreken, bedoelen we het transport van IP-pakketten.

2.2.2 Internetverkeer binnen netwerken

Een netwerk is een systeem voor communicatie tussen twee of meerdere computers. Het bestaat uit fysieke transportmedia (kabels) en zogenaamde *routers*. Voor netwerkneutraliteit zijn vooral de routers van belang.

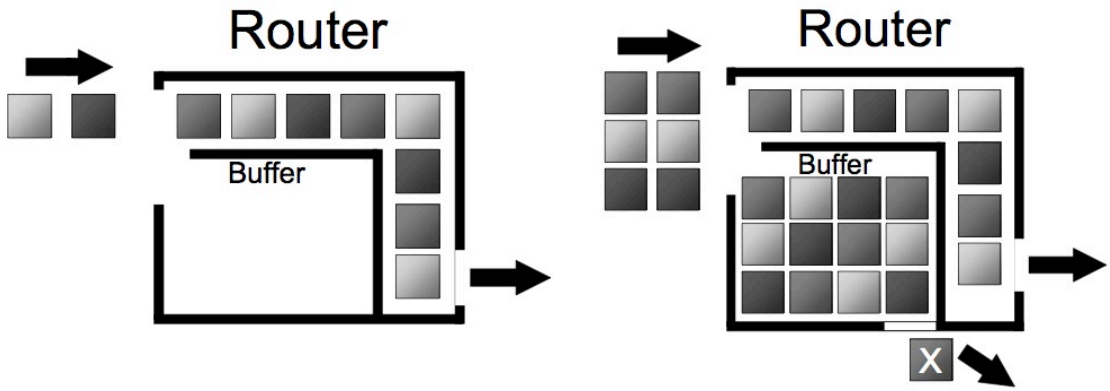
Routering

De router is het netwerkonderdeel dat op basis van het bestemmingsadres van een IP-pakket het verkeer routeert van zender naar ontvanger. Een router heeft een aantal poorten. Na binnenkomst van een pakket op een van de ingaande poorten zal de router de bestemming daarvan lezen en vervolgens, op basis van routeringtabellen, het pakket naar de juiste uitgaande poort sturen. Een typische internetsessie verloopt via een groot aantal routers: dat begint bij de router die bij de eindgebruiker thuis staat (of bij de organisatie waar de eindgebruiker werkt), via de routers van de ISP, via de routers van een of meer peering- of transitpartijen (zie paragraaf 2.2.3), via de routers van de ISP van de ontvangende partij, naar de router die de ontvangende partij zelf heeft geïnstalleerd.

[4] We bedoelen computer in de brede zin van het woord, dus ook mobiele handsets, servers, et cetera.

Congestie

Het is in de router dat er een inherent risico op vertraging of verlies van pakketjes bestaat. Stel (dit is een gesimplificeerde weergave) dat alle poorten een gelijke capaciteit hebben en dat deze poorten direct aan eindgebruikers zijn gekoppeld. Als nu van een groot aantal gebruikers pakketten arriveren die allemaal naar dezelfde gebruiker moeten worden doorgestuurd, doet zich congestie op de betreffende uitgaande poort voor. In een dergelijke situatie kan de router binnenkomende pakketten tijdelijk in een interne buffer opslaan. Op het moment dat er weer ruimte is, kunnen de pakketten uit de buffer alsnog bezorgd worden. Houdt de situatie waarin het aanbod groter is dan de capaciteit van de uitgaande poort echter lang aan, dan is het onvermijdelijk dat de buffer op een gegeven moment vol raakt. Blijven er dan nog nieuwe pakketten binnenkomen, dan zullen er pakketten verloren gaan: de buffer wordt overschreven. Figuur 2 laat een router zien waarin geen sprake is van congestie (links) en waarin wel sprake is van congestie (rechts).



Figuur 2. Congestie in een router[5]

Op een of andere wijze moet in de router zijn bepaald welke pakketten in het geval van congestie worden overschreven. Deze regels duiden we aan met de term *policy*. Het kan zijn dat berichten simpelweg in volgorde van binnenkomst worden overschreven (*first in first out* - FIFO). Maar het kan ook zijn dat de router rekening houdt met andere criteria, zoals de afkomst of de bestemming van het pakket, het type toepassing dat het pakket verstuurde, et cetera. Hier raken we aan de netwerkneutraliteit discussie: *router policies* zijn een mogelijke manier om het verschillend behandelen van internetverkeer te operationaliseren (zie verder paragraaf 2.4) en congestie is een motief om dat te doen.

De mate waarin congestie voorkomt hangt overigens ook af van de capaciteit van de andere netwerkelementen: de verbindingen *tussen* de computers en routers. Voor beiden geldt dat het risico op congestie afneemt naarmate er meer in capaciteit wordt geïnvesteerd. Maar het is meestal niet haalbaar (lees: financierbaar) om congestie volledig te voorkomen: een zekere blokkeringskans is inherent aan de aan de manier waarop het internet is ontworpen.[6]

---

[5] OECD (2007). *Internet traffic prioritisation: an overview*. http://www.oecd.org/dataoecd/43/63/38405781.pdf

[6] Zelfs bij telefonienetwerken is sprake van een zekere blokkeringkans – een centrale heeft een bepaalde capaciteit in termen van *Busy Hours Call Attempts* (BHCA) en ook de capaciteit van de

2.2.3 Internetverkeer tussen netwerken: interconnectie

Het internet is een aaneenschakeling van een groot aantal autonome netwerken (*Autonomous System* - AS), momenteel meer dan 25.000. Een autonoom systeem kan het netwerk van een ISP zijn, maar het kan ook gaan om een hosting provider, een universiteit, school, hospitaal of andere organisatie. Elk autonoom systeem heeft een uniek (AS-) nummer en een reeks toegewezen IP-adressen. Verkeer wordt ofwel uitgewisseld binnen één autonoom systeem (zie paragraaf 2.2.2), ofwel tussen twee autonome systemen onderling. Een autonoom systeem (de naam zegt het) is vrij te beslissen met wie het verkeer uitwisselt.

```
Bezig met het traceren van de route naar newzealand.govt.nz [202.175.128.234]
via maximaal 30 hops:

  1     1 ms    <1 ms    <1 ms  dsl.easynet.nl [213.201.203.57]
  2   234 ms   222 ms   222 ms  212.0.227.36
  3    10 ms    10 ms    10 ms  po1.br10.encap.nl.easynet.net [193.238.248.16]
  4    29 ms    45 ms    68 ms  po1.br10.encap.nl.easynet.net [193.238.248.16]
  5   227 ms   150 ms    10 ms  ge3-0-0-111.gr10.encap.nl.easynet.net [87.86.71.
192]
  6    18 ms    18 ms    18 ms  te5-0-0.gr11.telon.uk.easynet.net [87.86.77.28]

  7    18 ms    18 ms    18 ms  ge-7-16.car5.London1.Level3.net [212.187.170.229
]
  8    18 ms    31 ms    18 ms  ae-31-55.ebr1.London1.Level3.net [4.68.116.158]

  9    19 ms    18 ms    19 ms  ae-1-100.ebr2.London1.Level3.net [4.69.132.118]

 10    89 ms    89 ms    89 ms  ae-43-43.ebr1.NewYork1.Level3.net [4.69.137.74]

 11   117 ms   112 ms   165 ms  ae-81-81.csw3.NewYork1.Level3.net [4.69.134.74]

 12    98 ms    90 ms   114 ms  ae-84-84.ebr4.NewYork1.Level3.net [4.69.134.121]

 13   158 ms   160 ms   162 ms  ae-2.ebr4.SanJose1.Level3.net [4.69.135.185]
 14   167 ms   161 ms   162 ms  ae-74-74.csw2.SanJose1.Level3.net [4.69.134.246]

 15   158 ms   158 ms   164 ms  ae-12-79.car2.SanJose2.Level3.net [4.68.18.76]
 16   159 ms   159 ms   198 ms  TELECOM-NEW.car2.SanJose2.Level3.net [4.59.4.26]

 17   159 ms   158 ms   161 ms  so-1-2-0.0-sjbr2.global-gateway.net.nz [202.37.2
46.202]
 18   296 ms   296 ms   288 ms  so6-2-0.akbr4.global-gateway.net.nz [202.50.232.
29]
 19   295 ms   295 ms   295 ms  so1-2-0.tkbr9.global-gateway.net.nz [203.96.120.
74]
 20   514 ms   348 ms   285 ms  datacom-systems-int.tkbr9.global-gateway.net.nz
[202.50.238.234]
 21   282 ms   293 ms   292 ms  ww2.webportal.govt.nz [202.175.128.234]
 22   283 ms   282 ms   295 ms  ww2.webportal.govt.nz [202.175.128.234]
 23   294 ms   293 ms   283 ms  ww2.webportal.govt.nz [202.175.128.234]

De trace is voltooid.
```

Figuur 3. Verkeersstroom tussen netwerken, in dit geval tussen Dialogic en een website in Nieuw-Zeeland

Figuur 3 laat zien via welke netwerken verkeer tussen ons kantoor in Utrecht en een website in Nieuw-Zeeland wordt getransporteerd. Wat al snel duidelijk wordt: niet alle autonome systemen zijn direct met elkaar verbonden.[7] Vaak wordt internetverkeer indirect, via één of meerdere andere autonome systemen, uitgewisseld. Wanneer twee systemen op elkaar aansluiten, kondigen ze allebei de routes aan die zij kunnen verzorgen (*announce routes*), zowel naar bestemmingen binnen het eigen netwerk als – indirect – naar bestemmingen binnen andere netwerken. Overigens zijn veel autonome systemen op meerdere andere autonome systemen aangesloten. Het kan dus voorkomen dat een

transportverbindingen tussen centrales is begrensd. Bij telefonie lopen gebruikers echter zelden tegen deze beperkingen aan.

[7] Dat kan eigenlijk ook niet: in het geval van 25.000 autonome systemen zouden er 312.487.500 symmetrische directe verbindingen nodig zijn.

bepaalde bestemming via meerdere routes bereikt kan worden (redundantie). Middels *route filtering* wordt een keuze voor de meest optimale route gemaakt.[8] Daarbij zullen vaak financiële motieven een rol spelen en dat brengt ons bij de kern van deze paragraaf: wat voor afspraken maken partijen over de uitwisseling van verkeer? Een belangrijk verschil is dat tussen *peering* en *transit*.[9]

Peering

Er is sprake van peering[10] als twee partijen (autonome systemen) overeenkomen *direct* verkeer met elkaar uit te wisselen, zonder elkaar daarvoor kosten in rekening te brengen. Essentieel is dat een peering afspraak in beginsel alleen over verkeer gaat van of naar klanten die direct op de twee betreffende partijen zijn aangesloten. Peering afspraken worden dus niet gebruikt om vanuit je eigen netwerk A via netwerk B naar netwerk C te komen.

De kosten om het verkeer naar de peering locatie te transporteren worden door de partijen zelf gedragen. Vaak is deze locatie een Internet Exchange, maar dat hoeft niet.[11] Doordat hier veel netwerken samenkomen, kan er efficiënt gekoppeld worden. Het maximale verkeersvolume dat kan worden uitgewisseld, is afhankelijk van de capaciteit van de verbinding tussen de partijen. Op die manier kan dus een zekere bovengrens worden ingesteld.[12] Ook maken partijen soms aanvullende afspraken over eventuele beperkingen van het type peering verkeer. Zo kan men bijvoorbeeld overeenkomen dat zakelijk verkeer buiten de overeenkomst valt.

Het aangaan van een peering overeenkomst is een vrijwillige aangelegenheid voor beide partijen. Alleen als beide partijen een zeker voordeel zien in het uitwisselen van verkeer met gesloten beurzen – met andere woorden als de kosten (het leggen van de verbindingen) lager zijn dan de financiële voordelen (het niet hoeven betalen voor de uitwisseling van verkeer) – zullen partijen hiertoe besluiten. Maar bij deze overweging is ook van belang hoe de partijen elkaars voordeel van de overeenkomst en de relatieve onderhandelingssituatie die daar het gevolg van is inschatten. In tegenstelling tot wat soms wel wordt gedacht, speelt de balans in de verkeersstromen (loopt er evenveel verkeer van partij A naar partij B als andersom) nagenoeg geen rol. Als een van de partijen besluit de peering overeenkomst te verbreken dan spreken we van de-peering.

Transit

Transit komt in beeld wanneer een partij A (autonoom systeem) verkeer wil uitwisselen met een partij B waarmee het zelf geen directe verbinding heeft. Partij A wendt zich dan tot een transit provider, die er – tegen vergoeding! – voor zorgt dat al het aangeboden

---

[8] Het is een hardnekkig misverstand dat internetpakketjes ieder onafhankelijk hun weg zoeken van oorsprong tot bestemming en dus via allerlei verschillende netwerken worden getransporteerd. In werkelijkheid loopt het verkeer via de route die de ISP heeft gekozen en ingesteld. Overigens is ook de route van het verkeer binnen de netwerken van ISP's grotendeels vastgelegd.

[9] Deze paragraaf is onder meer gebaseerd op: Van der Berg (2008). *How the net works*. http://arstechnica.com/guides/other/peering-and-transit.ars

[10] De volledige term is *settlement free peering*.

[11] In Europa vindt peering vaak op een Internet Exchange plaats, in de VS vaker op private peering locaties.

[12] Als de verbinding op een Internet Exchange plaatsvindt is het niet altijd mogelijk om een bovengrens in te stellen. Stel dat partij A, B en C ieder een 10 Gbps aansluiting op die exchange hebben en alle drie een peering-overeenkomst zijn aangegaan, dan kunnen ook B en C onderling met 10 Gbps verkeer uitwisselen.

verkeer bij partij B wordt bezorgd. Deze transit provider gaat daartoe met een aantal autonome systemen directe verbindingen aan. Om de overige autonome systemen te kunnen bereiken gaat ze overeenkomsten aan met een aantal andere transit providers. De transit provider vraagt normaal gesproken een vergoeding (*transit fee*) in ruil voor een bepaalde gereserveerde verkeerscapaciteit.[13] Als twee partijen via een transit provider verbonden zijn, betalen zij allebei een transit fee. In beginsel hoeft een transit provider geen 'eigen' gebruikers te hebben, hoewel het niet is uitgesloten dat een bedrijf tegelijkertijd de rollen van ISP en transit provider vervult.[14]

Pay to Peer

Als twee partijen (bijvoorbeeld twee ISP's, of een ISP en een contentprovider) verkeer uitwisselen via een transit provider betalen ze als gezegd beide een transit fee. Dat is precies de prikkel voor beide partijen om een peering overeenkomst aan te gaan. Recent is er discussie gaande over het verschijnsel *pay to peer*. Dit is een vorm van peering waarbij een van de partijen (in de regel de ISP) een vergoeding verlangt. Dit is dus in tegenstelling tot 'normale' peering overeenkomsten waar met gesloten portemonnee verkeer wordt uitgewisseld. Er blijft echter wel een belangrijke onderscheid met transit: bij pay to peer is het bereik van het uitgewisselde verkeer beperkt tot bestemmingen die *direct* zijn aangesloten op de partijen die verkeer uitwisselen. Als een contentprovider zich in een relatief zwakke onderhandelingspositie bevindt ten opzichte van een ISP, dan zou deze ISP een verzoek om peering kunnen afwijzen, maar aangeven wél met pay to peer akkoord te gaan. (Het kan hier een contentprovider betreffen die reeds een peering overeenkomst met de ISP had, maar ook een die eerder via transit verkeer aanbood of zelfs nog helemaal geen overeenkomst had.) De ISP gebruikt als argument dat zijn pay to peer aanbod voor de contentprovider nog steeds goedkoper uitpakt dan het verkeer via een transit provider indirect af te laten leveren. De voordelen voor de ISP zelf zijn tweeledig: niet alleen wordt er een extra inkomstenstroom gegenereerd, maar de ISP hoeft zelf ook geen transit fee meer af te dragen voor het betreffende verkeer.[15]

Pay to peer is onderwerp van verhitte discussies en sommige commentatoren stellen dat het onwenselijk zou zijn. Opmerkelijk is echter dat weinigen er stil bij lijken te staan dat ook de (algemeen geaccepteerde) transit overeenkomsten in beginsel hetzelfde effect kunnen hebben. De transit fees zijn namelijk de uitkomst van onderhandelingen. Stel dat (bepaalde groepen) ISP's systematisch in staat blijken lagere transit fees te bedingen dan (bepaalde groepen) content- of applicatieproviders dan fungeren de transit providers feitelijk als een soort geldstroom van IAP/ICP (*Internet Application Provider* en *Internet Content Provider* – respectievelijk aanbieders van diensten en content) naar ISP.

---

[13] De bandbreedte kan daarbij 'hard' gelimiteerd zijn op een bepaalde waarde, maar het is ook mogelijk dat de afnemer meer bandbreedte afneemt dan deze gereserveerd heeft en voor het extra gebruik een boete betaalt.

[14] Er kunnen verschillende soorten transit providers worden onderscheiden. Bovenaan in de hiërarchie vinden we de zogenaamde tier-1 partijen. Deze bedrijven zijn in staat verkeer af te leveren aan alle bestaande autonome systemen, zonder dat ze daarbij transit fees aan anderen hoeven af te dragen. Dat kan in feite alleen door zelf peering overeenkomsten te hebben met alle andere tier-1 partijen. Zogenaamde tier-2 partijen kopen verkeer deels in en betalen daarvoor transit fees en wikkelen verkeer deels direct af middels peering. Zogenaamde tier-3 partijen kopen al het verkeer naar andere autonome systemen in en betalen daarvoor transit fees. Momenteel zijn er circa acht tier-1 partijen.

[15] Met andere woorden: de geldstroom van de content provider richting de transitpartij wordt verlegd naar de ISP.

2.3 Motieven

Een ISP kan verschillende motieven hebben om internetverkeer verschillend te behandelen. Opvallend is dat in recente literatuur over netwerkneutraliteit vaak slechts een deel van de – in onze ogen – relevante motieven wordt besproken. Literatuur met de nadruk op economische motieven (business models) gaat vaak volledig voorbij aan technische motieven, die echter heel legitiem kunnen zijn. Beveiligingsmotieven komen überhaupt nauwelijks aan bod. Wij onderscheiden vier categorieën van motieven, te weten (1) beveiliging, (2) schaarste, (3) business en (4) morele principes.

2.3.1 Beveiliging

Om gebruikers van het netwerk te beschermen, kan het nodig worden geacht om bepaalde beveiligingen door te voeren. Doorgaans is beveiliging gekoppeld aan *straight blocking*. Zo kunnen bepaalde IP-adressen of poorten volledig worden geblokkeerd. Maar een netwerk kan er ook voor zorgen dat spam en virussen centraal worden afgeblokt. Een aanval op systemen in het netwerk, bijvoorbeeld door middel van een Denial-of-Service aanval[16] (DoS-attack), kan ook een reden zijn om bepaald verkeer te weren.

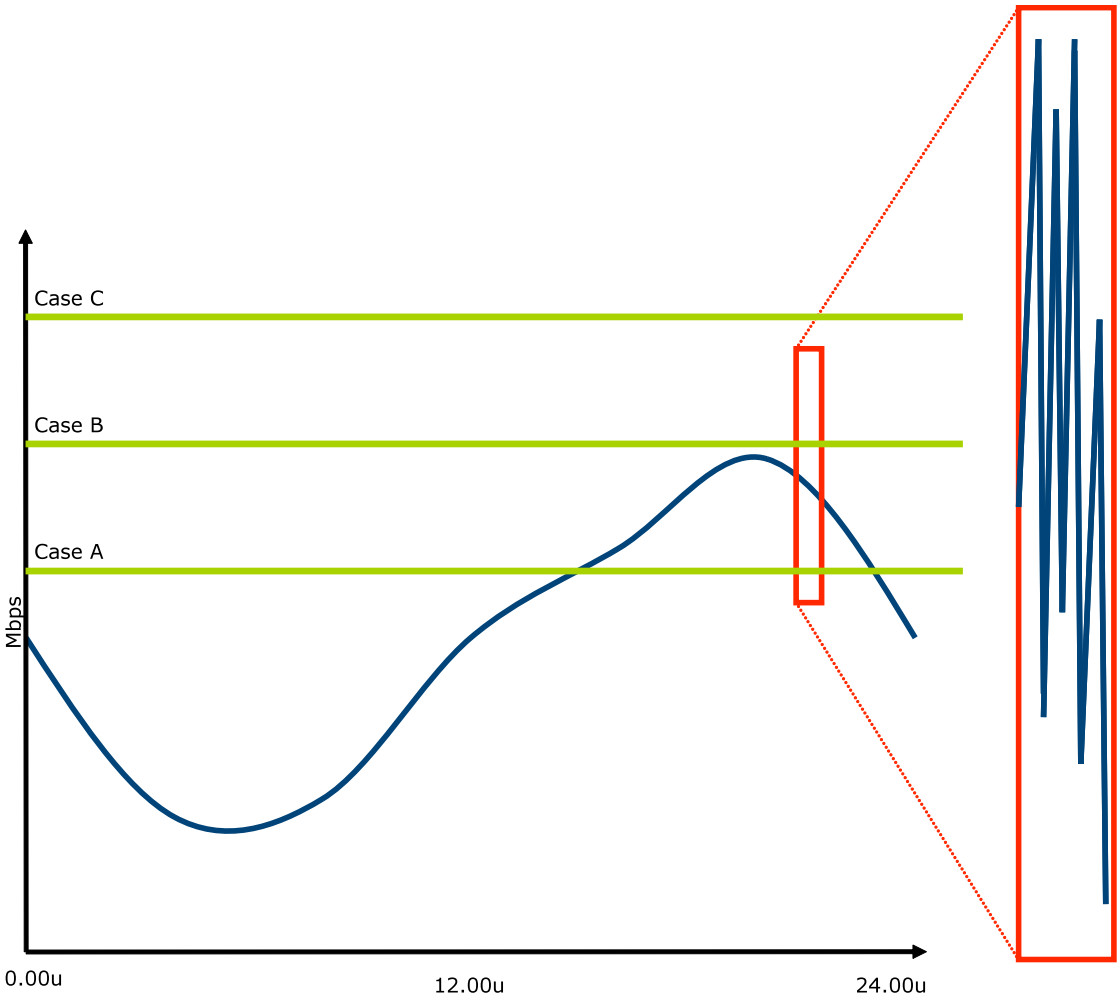
2.3.2 Schaarste

Indien er in een netwerk sprake is van schaarste van bandbreedte, speelt de onvermijdelijke vraag van prioritering. Welke verkeer krijgt de voorkeur? Dit kan willekeurig, door gebruik te maken van FIFO (zie paragraaf 2.2.2), maar er kunnen ook complexere methodes worden gebruikt. In Figuur 4 toont de blauwe lijn het verloop van het internetverkeer over een fictief netwerk, verdeeld over de tijdspanne van een dag. De lijn geeft de waarde van de gemiddelde benodigde bandbreedte in een seconde aan. Als we een kortere tijdspanne nemen, dan komt het 'bursty' karakter van het internet naar voren. Het verkeer kent zeer grote variaties als we het onder een vergrootglas houden (zie de rode box). In het figuur zijn drie cases (groene lijnen) onderscheiden. Deze geven de maximale capaciteit van de verschillende netwerken aan. Op basis van dit figuur kunnen we twee verschillende schaarste-gerelateerde motieven onderscheiden.

2a. Structurele overbelasting netwerk (case A)

In case A heeft het netwerk van de operator tussen circa 14u en 23u te weinig bandbreedte om het verkeer af te handelen. Er is in dit netwerk dus geen sprake van overdimensionering. Vooral bij mobiele netwerken is (over)capaciteit kostbaar en speelt dit vaak. Er moet dan een afweging worden gemaakt bij het inzetten van de beschikbare capaciteit. Dat kan met behulp van het zogenaamde need-based prioritisation policy (zie paragraaf 2.4.2). Door te anticiperen op de kwaliteit zoals gebruikers die ervaren, kan er bijvoorbeeld voor gekozen worden om VoIP-verkeer een hogere prioriteit toe te kennen dan P2P verkeer. Hierdoor kan de gebruiker blijven bellen, maar verschuiven de downloads naar de nachtelijke uren.

[16] DoS-attack. Er wordt dan zoveel verkeer naar een bepaalde server gestuurd dat deze uiteindelijk onbereikbaar wordt of zelfs uitvalt. Door het blokkeren van het verkeer van een bepaalde afzender kan de aanval worden afgewend. Als de aanval echter tegelijkertijd vanaf veel aparte afzenders komt (bijvoorbeeld een groot aantal PC's dat met een virus is besmet dat op een bepaalde tijd een aanval uitvoert) dan is het afwenden van de aanval veel lastiger. Dit laatste type aanval staat bekend als een DDoS-attack (Distributed Denial of Service Attack).



Figuur 4. Het verloop van het internetverkeer over een fictief netwerk

2b. Tijdelijke overbelasting netwerk (case B)

In case B heeft het netwerk van de operator in principe voldoende bandbreedte om het verkeer af te handelen. Maar door de grote fluctuaties in verkeer (zie rode box in Figuur 4), ontstaan er tijdens piekuren kortdurende opstoppingen in het netwerk. Hierdoor kan er een pakketje met data verloren gaan, of een pakketje vertraging oplopen. Voor sommige soorten verkeer maakt dit niet veel uit. Een email die twee seconde vertraagd en met horten en stoten arriveert, valt niemand op. Voor andere diensten is het wel een probleem. Een telefoonconversatie of live voetbalwedstrijd die twee seconden vertraagd en met horten en stoten arriveert, zorgt voor grote irritatie. De beheerder van het netwerk kan ervoor kiezen om – eventueel tegen extra betaling – bepaalde soorten verkeer voorrang te geven. Dit kan door middel van need-based prioritisation of active prioritisation (zie paragraaf 2.4.3).

Voor de volledigheid, in case C heeft het netwerk van de operator altijd voldoende bandbreedte om het verkeer af te handelen. Deze operator heeft dus geen schaarste-gerelateerde motief.

Schaarste-gerelateerde motieven en economische motieven kennen een onderling verband. Immers, door onderinvesteringen in een netwerk ontstaat er schaarste en omgekeerd. Schaarste-gerelateerde motieven worden dan ook geregeld in twijfel worden getrokken door sceptici: "*De operator heeft de schaarste bewust veroorzaakt om bepaalde technische gedragingen in het netwerk te legitimeren*". Daarom is het interessant om te kijken naar de plaats waar schaarste optreedt in het netwerk. Wij maken onderscheid tussen drie soorten schaarste.

Schaarste in het aansluitnetwerk

De capaciteit van het aansluitnetwerk hangt af van de gebruikte techniek, de netwerk-topologie en andere technische en architecturale beslissingen. Met name bij mobiele netwerken zal de schaarste primair in het aansluitnetwerk (lees: het radionetwerk) liggen. Vergroting van de capaciteit in het aansluitnetwerk vergt aanzienlijke investeringen.

Schaarste in het transportnetwerk

De capaciteit van het transportnetwerk (*backhaul*) hangt af van de capaciteit van de ingezette verbindingen en de gebruikte routers en andere apparatuur. Vergroting van de capaciteit is – vergeleken met de capaciteit van het aansluitnetwerk - relatief eenvoudig en snel te realiseren.

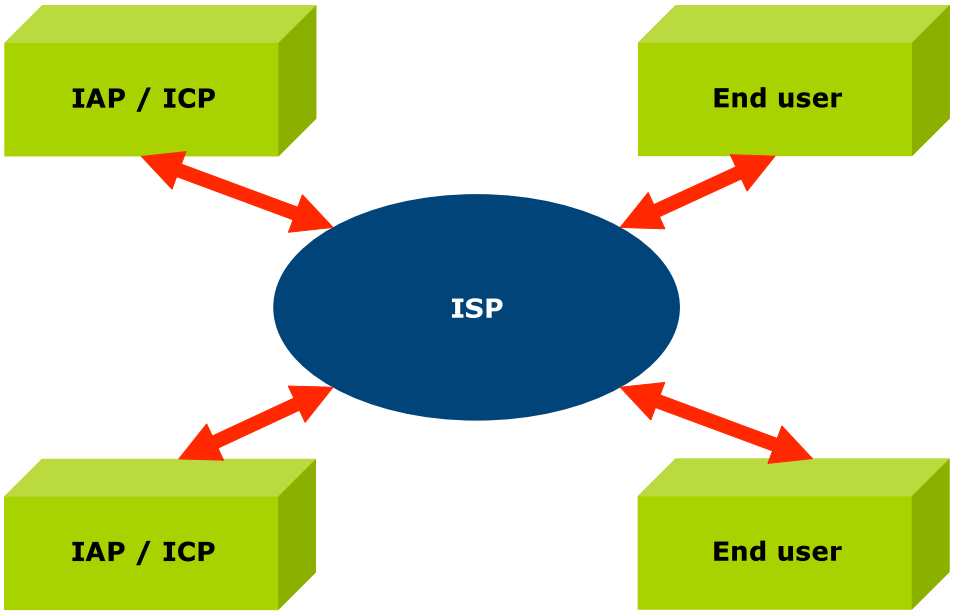
Schaarste bij interconnectie

De interconnectiecapaciteit is de som van de capaciteit van de peering- en transitverbindingen. Verschillende partijen realiseren directe verbindingen met hun peering- en transitpartners maar in Nederland worden verbindingen vaak ook op de Amsterdam Internet Exchange (AMS-IX) aangegaan. ISP's en anderen kunnen zich daar met (één of meerdere) poorten aansluiten, die ieder een capaciteit van 1 Gbps of 10 Gbps hebben. Vergroting van de capaciteit is relatief eenvoudig door meer poorten af te nemen. Als daar echter verkeer over gaat waarvoor een transit fee moet worden betaald kan dat wel een flink hogere transit-rekening opleveren.

Box 1. Relatie tussen schaarste-gerelateerde motieven en economische motieven.

2.3.3 Business model

Om dit motief goed te kunnen plaatsen, introduceren we een sterk gesimplificeerd model van het internet (Figuur 5). Daarin staat de ISP centraal en maken we onderscheid tussen twee soorten gebruikers: aanbieders van diensten en content (IAP/ICP) versus eindgebruikers. Hoewel het internet in beginsel geen onderscheid maakt tussen verschillende soorten gebruikers en eindgebruikers elkaar ook onderling diensten en content (bijvoorbeeld via P2P-applicaties), is het karakter van deze partijen in de waardeketen zo verschillend dat het zinvol is dit onderscheid te maken. Uit deze sterk vereenvoudigde weergave is direct een interessant fenomeen af te leiden: het betreft een zogenaamde *two-sided market*. Dit is een markt (vaak een netwerk, maar het kan ook om een platform gaan) waarin een centrale partij *twee* gebruikersgroepen bedient, die *allebei* waarde aan de markt toevoegen. Een bekend voorbeeld is het platform voor creditcardbetalingen, waarbij zowel de kaarthouders als de winkeliers voor elkaar een zekere waarde vertegenwoordigen. De centrale partij kan in een dergelijke markt haar revenuen aan één van beide 'kanten' of aan beide kanten genereren, maar ook aan beide kanten geld verdienen. Binnen de internetmarkt is van dat laatste vooralsnog beperkt sprake: IAP's en ICP's betalen een relatief geringe vergoeding voor de aansluiting en als ze aantrekkelijk genoeg zijn voor de ISP (omdat ze veel traffic genereren) betalen ze soms zelfs helemaal niets.



Figuur 5. een gesimplificeerd model van het internet

Binnen dit kader zijn drie gedragen te onderscheiden:

3a. prijsdifferentiatie richting eindgebruikers

Dit motief verwijst naar situaties waarbij de ISP verschillende toegangsproducten, tegen verschillende prijzen en voorwaarden, op de markt brengt. Met name active prioritisation en straight blocking (zie paragraaf 2.4.4) sluiten hier op aan. Door verschillende prioriteiten te geven aan verschillende abonnementen kan er effectief in toegangsdiensten worden gedifferentieerd. Ook kan de ISP besluiten te differentiëren naar eindgebruikerapparatuur (zie paragraaf 2.4.5), zoals momenteel bij mobiele telefoons versus mobiel internet via een laptop het geval is.

3b. prijsdifferentiatie richting IAP's & ICP's

Dit betreft de situatie waarbij de ISP nadrukkelijker vergoedingen wil innen aan kant van de IAPs en ICPs. Zij kunnen tegen betaling verbeterde dienstverlening afnemen waarmee zij hun diensten beter in de markt kunnen zetten. Dit wordt door sommigen ook wel met 'Access tiering' aangeduid.[17] Active prioritisation is de voor de hand liggende methode.

3c. Beperken van concurrentie

Een aantal ISP's is zelf ook IAP of ICP en is dus een verticaal geïntegreerde partij.[18] Zij kunnen andere IAPs en ICPs als concurrent zien. De wens om de omzet op eigen content- of applicatiediensten te beschermen, of die van partijen waarmee (exclusieve) afspraken zijn gemaakt, leidt ertoe dat de verkeersstroom beïnvloed wordt. Active prioritisation of straight blocking lijken de voor de hand liggende methodes.

---

[17] Zie onder meer: Kocsis & De Bijl (2007). *Network neutrality and the nature of competition between network operators*. http://www.cpb.nl/nl/org/homepages/vks/kocsis-de-bijl_network_neutrality_2007 .pdf

[18] Die verticale integratie kan ook indirect zijn, via allerlei financiële constructies.

2.3.4 Morele principes

Dit vierde motief is bijzonder in de zin dat het niet (alleen) bij ISP's ligt. Hierdoor staan ISP's in meer of minder mate onder maatschappelijke druk om in te grijpen in het verkeer. Vanuit bijvoorbeeld overheden kan er druk zijn om bijvoorbeeld bepaalde content niet naar eindgebruikers door te laten. Een voorbeeld hiervan is de lijst met websites die de KLPD opstelde om toegang tot kinderporno weren. Ook content die (potentieel) inbreuk maakt op auteursrechten kan afgeblokt worden. Aan de andere kant kan men op principiële gronden argumenteren dat er juist *niet* in verkeer wordt ingegrepen (recht op meningsuiting, privacy/briefgeheim et cetera).

2.4 Technische gedragingen

Waar de vorige paragraaf inging op de motieven voor het verschillend behandelen van internetverkeer, gaat deze paragraaf in op de feitelijke technische gedragingen om dit te bewerkstelligen. We grijpen daarvoor terug op de eerder geïntroduceerde router policies.[19] Een eenvoudige manier om verkeer verschillend te behandelen is namelijk om verkeer verschillende prioriteiten toe te kennen bij verwerking door de router. Maar ook andere manieren om internetverkeer verschillend te behandelen komen aan de orde. Box 2 noemt een aantal kenmerken van internetverkeer die aan de basis kunnen liggen van verschillende benaderingen.

2.4.1 First in first out (FiFo)

Deze policy wordt ook wel *best effort* genoemd en is de standaardinstelling (*default setting*) van veel routers. Plaatsing van pakketten in de buffer en verwijdering van pakketten uit de buffer gebeurt louter op basis van de volgorde van de binnenkomst van die pakketten in de router. Er is dus geen sprake van het bewust verschillend behandelen van internetverkeer.

2.4.2 Need-based prioritisation

Plaatsing van pakketten in de buffer en verwijdering van pakketten uit de buffer gebeurt op basis van prioriteiten die worden toegekend aan die pakketten. Alleen als er sprake is van feitelijke congestie wordt prioritering toegepast. De prioriteiten kunnen gebaseerd zijn op verschillende technische kenmerken, zoals afzender, bestemming en (veronderstelde) applicatie. Bij het gebruik van deze policy kan een optimalisatie van de gebruikerservaring centraal staan (geen vertraging), maar kunnen ook andere (bedrijfseconomische) motieven spelen.

2.4.3 Active prioritisation

Deze policy wordt ook wel als *non-minimal traffic shaping* aangeduid. De capaciteit van de router wordt vooraf in twee of meer gebieden (*tiers*) opgedeeld. Voor de eerste tier wordt bijvoorbeeld 80% van de capaciteit gereserveerd, de andere tier krijgt de resterende 20% toegewezen. Op basis van prioriteiten (die op basis van technische kenmerken zijn toegekend aan pakketten) worden pakketten in een van de tiers ondergebracht. Een belangrijk verschil met need-based prioritisation is dat ook als er *geen* sprake is van congestie high-priority verkeer meer prioriteit krijgt dan low-priority verkeer. Pakketten

[19] We bouwen daarbij met name voort op het werk van Felten (2006). *Nuts and bolts of net neutrality*. http://itpolicy.princeton.edu/pub/neutrality.pdf

Internetverkeer heeft een groot aantal kenmerken op basis waarvan het verschillend behandeld kan worden. Hieronder een – niet uitputtend – overzicht:

- IP-adres (geeft zowel de afzender als de bestemming aan);

- Laag-4 poort (tot op zekere hoogte een indicatie voor de gebruikte applicatie);

- Laag-4 protocol (o.a. TCP, UDP);

- Laag-7 protocol (o.a. HTTP, FTP);

- SIP domain suffix (indicatie voor het gebruik van VoIP);

- Aantal simultane verbindingen dat een applicatie aanvraagt (indicatie voor het gebruik van P2P);

- Aantal gelijksoortige verbindingen dat een applicatie in een bepaalde tijdsperiode aanvraagt (indicatie voor het gebruik van VoIP);

- Traffic flow (pakketjes van een gelijke lengte die met een grote regelmaat langskomen zijn een indicatie voor het gebruik van VoIP);

- Verkeersvolume van een klant in een bepaalde periode;

- Door de gebruiker gekozen prioriteits-instellingen.

Een aantal van deze kenmerken kan niet uit de header van een pakket (zie paragraaf 2.2.1) worden opgemaakt. In dergelijke gevallen moet het pakketje worden geopend en de inhoud zelf worden geanalyseerd. Apparatuur die dat mogelijk maakt wordt met de term deep packet inspection aangeduid. Dergelijke apparatuur wordt door gespecialiseerde bedrijven geleverd (voorbeelden zijn Ipoque, Qosmos en Cloudshield) maar tegenwoordig ook door netwerkleveranciers als Alcatel-Lucent, Cisco en Ericsson. De apparatuur kan door een ISP in het netwerk worden opgenomen en, indien gewenst, bepaalde typen verkeer verschillend behandelen. De nieuwste generatie van deze apparaten hebben een zodanige capaciteit en snelheid dat dit mogelijk is zonder dat het andere verkeer er hinder van ondervindt. Leverancier Ipoque produceert bijvoorbeeld Deep Packet Inspection systemen met een continue doorvoercapaciteit van 120 Gbps (ter vergelijking: dat is meer dan de aansluitcapaciteit van de grootste Nederlandse ISP op de Amsterdam Internet Exchange). De latency is nul, wat wil zeggen dat inkomende pakketten direct worden doorgegeven of weggegooid, zonder een buffer te passeren.

Box 2. Internetverkeer en haar kenmerken

met een lage prioriteit lopen het risico te worden vertraagd of weggegooid, óók in gevallen waarbij de capaciteit gereserveerd voor pakketten met een hoge-prioriteit nog (lang) niet volledig is bezet. Vandaar de term 'non-minimal'.[20]

2.4.4 Straight blocking

Op basis van technische kenmerken worden bepaalde pakketten onvoorwaardelijk geblokkeerd. Hierdoor komt dit verkeer niet door de routers en kunnen de achterliggende diensten feitelijk niet gebruikt worden in het netwerk.

[20] Overigens kan hetzelfde worden bereikt door verschillende subnetwerken 'naast elkaar te bouwen' en/of richting specifieke partijen verbindingen met hoge capaciteit te realiseren.

2.4.5 Beperkingen in de user-device[21]

Een telefoon met een simlock is het meest bekende voorbeeld van een beperking in de user-device. Alleen verkeer van een bepaalde mobiele operator kan via de telefoon worden afgehandeld. Een ander bekend voorbeeld is de modem die ISP's leveren aan hun klanten. Deze apparatuur kan zo ingesteld worden dat het de verkeersstroom beïnvloedt. Een derde voorbeeld zijn mobiele operators die data-abonnementen aanbieden die alleen in combinatie met een mobiele telefoon mogen worden gebruikt. Gebruik in combinatie met een laptop – ofwel door de mobiele telefoon als modem voor die laptop te gebruiken ofwel door de simkaart in een laptopmodem te steken – is niet mogelijk of wordt erg lastig gemaakt.[22] Indirect worden hier data-intensieve toepassingen (bijvoorbeeld P2P of direct downloads) door benadeeld. Dat zijn immers toepassingen die met name in combinatie met een laptop zullen worden gebruikt.

2.5 Effecten

Internetdiensten en –toepassingen kunnen verschillend reageren op de eerder uiteengezette technische gedragingen (zie paragraaf 2.4). Dat komt doordat niet alle diensten en toepassingen dezelfde eisen stellen aan *data rate* en de kwaliteit van het verkeer.

2.5.1 Data rate

De data rate is een maat voor het aantal pakketten dat binnen een bepaalde tijdsduur over het netwerk getransporteerd kan worden. Dit is, met andere woorden, de snelheid van het netwerk. Toepassingen die om een hoge data rate vragen zijn onder andere interactieve games, videoconferencing en IPTV en *video on demand*. Gebruikers die veel grote bestanden downloaden (muziek, films, games), willen vaak ook een hoge data rate hebben om de wachttijd te beperken. Toepassingen als e-mail en VoIP hebben een veel minder snel netwerk nodig.

2.5.2 Kwaliteit

Er wordt onderscheid gemaakt tussen verschillende kwaliteitsaspecten, meest belangrijk zijn *delay* of *latency*, *jitter* en *packet loss*.

- Delay of latency verwijst naar de vertraging tussen verzenden en ontvangen van een bepaald pakket. Interactieve toepassingen, zoals interactive gaming en VoIP reageren er kritisch op. Een telefoongesprek is immers niet goed mogelijk als er tussen vraag en antwoord teveel tijd zit. Bij het bekijken of beluisteren van live voetbalwedstrijden via internet komt het voor dat de stream enige tijd achter loopt. Zo hoor je de buren eerder juichen bij een doelpunt.
- Jitter verwijst naar de variatie in delay, het is hoog wanneer pakket A met een zeer lage vertraging aankomt en pakket B met een zeer hoge. Een televisiedienst is hier gevoelig voor. Het maakt niet uit als een televisiestream pas na enkele seconden start (als, met andere woorden, de delay groot is) maar als pakketten met een

[21] Beperkingen in de user device vallen buiten het netwerk en hebben in feite dus niets met netwerkneutraliteit te maken. Toch behandelen we dit onderwerp hier omdat de beheerder van het netwerk vaak enige macht heeft om het user device te beïnvloeden.

[22] De mate waarin mobiele operators deze beperking daadwerkelijk afdwingen verschilt. Apple's iPhone kan – naar het schijnt onder druk van mobiele operators – simpelweg niet als modem voor een laptop worden gebruikt. In andere gevallen wordt de beperking slechts in de algemene voorwaarden genoemd.

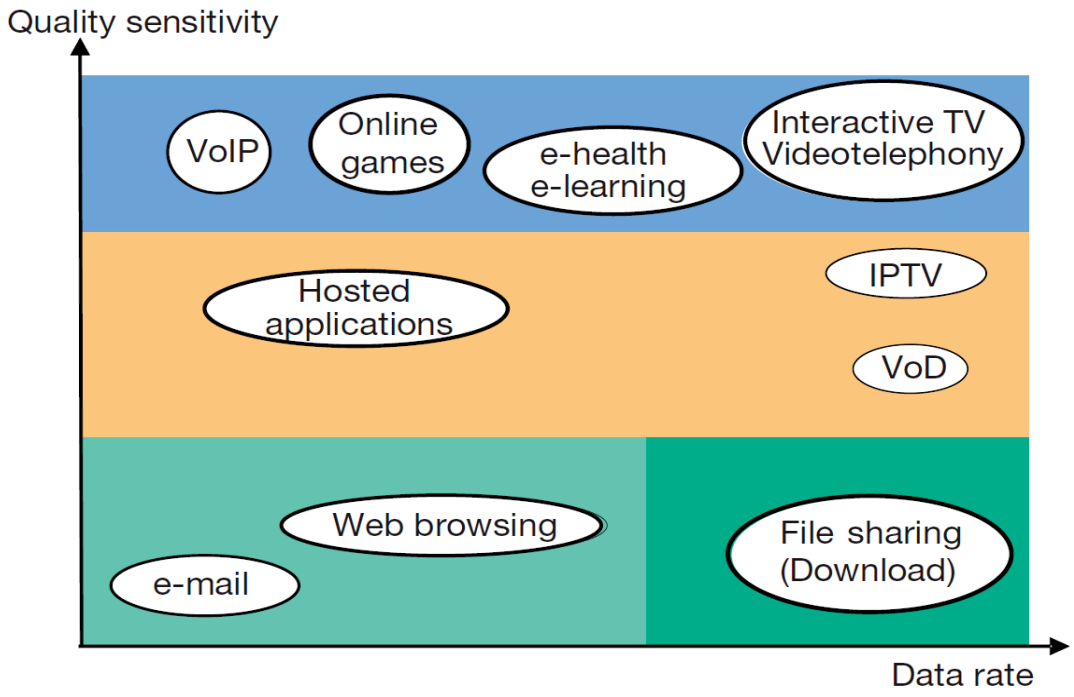
verschillende vertraging en dus in de verkeerde volgorde aankomen zal de dienst problemen ondervinden. Ook voor telefonie is dit een groot probleem.

- De gevoeligheid van een toepassing voor packet loss hangt met name af van het gebruikte protocol. Toepassingen als browsers en P2P-programma's maken in de regel gebruik van het TCP-protocol. Komt een verwacht pakket niet aan, ook niet na even wachten, dan wordt er een verzoek om hertransmissie gestuurd. Indien nodig herhaalt zich dat tot ofwel alle pakketjes binnen zijn. Dergelijk toepassingen zijn daardoor relatief ongevoelig voor packet loss, hoewel het gebruiksgemak van bijvoorbeeld een SaaS-toepassing (*Software as a Service)* sterk zal afnemen als die toepassing door een grote packet loss erg traag wordt.

  Real-time applicaties of quasi real-time applicaties (VoIP, video on demand) gebruiken daarentegen vaak het UTP protocol. Dit protocol kent geen her-transmissie en in geval van verlies van pakketten probeert de applicatie zo goed als het kan de sessie voort te zetten. Houden de problemen echter aan dan zal de transmissie worden stopgezet.

2.5.3 Date rate versus kwaliteit

Onderstaande figuur (Figuur 6) geeft voor verschillende toepassingen de gevoeligheid voor enerzijds voornoemde kwaliteitsaspecten en anderzijds data rate weer.



Figuur 6: gevoeligheid van verschillende applicaties voor kwaliteit versus data rate[23]

[23] Kruse (2008). *Network neutrality and quality of service*. http://www.springerlink.com/content/u3p060p126355275/

2.6 Relatie tussen motieven, gedragingen en effecten

In deze paragraaf behandelen we de relatie tussen motieven, gedragingen en effecten. Daarom presenteren we nogmaals het conceptueel model.

Het model toont dat motieven leiden tot gedragingen en de gedragingen op hun beurt weer bepaalde effecten hebben. Indien men wil toetsen of een operator onwenselijk beleid voert dan moet er worden teruggeredeneerd: (c) er is een negatief effect op de kwaliteit van de diensten van de eindgebruiker, dat (b) te wijten is aan het gedrag van de operator en (a) aan een – vermeend – motief gekoppeld is. Er bestaat een aantal uitdagingen in deze keten, welke we in deze paragraaf behandelen.

2.6.1 Complex om effecten aan gedragingen te koppelen

Het is als eindgebruiker vaak niet eenvoudig om de prestaties van een bepaalde dienst te koppelen aan gedrag van de ISP. Een geavanceerde gebruiker zal vrij snel doorhebben ofde ISP op grote schaal straight blocking of restricties op user devices toepast. Maar als het gaat om need-based prioritisation en active prioritisation is het veel lastiger om dit waar te nemen.

2.6.2 Complex om inzicht te krijgen in gedragingen

Het is veelal niet mogelijk om compleet inzicht in alle gedragingen van de ISP. Van buitenaf is het niet altijd mogelijk om dit te meten en de transparantie hierover is niet altijd toereikend.

2.6.3 Complex om gedragingen aan motieven te koppelen

In Tabel 1 worden de verschillende motieven gekoppeld aan de eerder geïntroduceerde verschillende behandelingen van internetverkeer: need-based prioritisation, active prioritisation, straight blocking, en user-device restricties en fair-use policies. De tabel toont welke gedragingen het meest voor de hand liggen indien er een specifiek motief is. Het is dan ook niet onmogelijk dat een operator vanuit eenzelfde motief voor een andere oplossing kiest.

Tabel 1 laat meteen zien waarom het niet eenvoudig is om vanuit gedragingen terug te redeneren naar motieven. Op basis van de technische gedraging a*n sich* kan niet gesteld worden welk motief erachter zit. Dit is een problematisch punt omdat juist het achterliggende motief zo belangrijk is. Een bepaalde handeling kan vanuit beveiligingsoverwegingen legitiem zijn, maar is onwenselijk wanneer ingezet door een dominante partij met de doelstelling concurrentie te verminderen. Indien bijvoorbeeld need-based prioritisation wordt waargenomen, volgt hieruit nog niet of dit werd ingezet vanuit het motief ‘structurele overbelasting netwerk’, ‘tijdelijke overbelasting netwerk’, ‘(prijs)differentiatie eindgebruikers’, ‘(prijs)differentiatie IAPs en ICPs’ of ‘beperken concurrentie hogere lagen’.

Tabel 1: Gedragingen en motieven bij het verschillend behandelen van verkeer

Gedragingen → / ↓ Motieven	Need-based prioritisation	Active prioritisation	Straight blocking	User device restricties
1. Beveiligen tegen misbruik			X	X
2a. Structurele overbelasting netwerk	X		X[a]	X[a]
2b. Tijdelijke overbelasting netwerk	X		X[a]	X[a]
3a. (Prijs)differentiatie eindgebruikers	X	X	X	X
3b. (Prijs)differentiatie IAPs en ICPs	X	X	X	X
3c. Beperken concurrentie hogere lagen	X	X	X	X
4. Ideologische en principiële uitgangspunten			X	X

[a] Hoewel het vanuit technisch oogpunt voor de hand ligt om in het geval van schaarste need-based prioritisation te gebruiken, kunnen we ons ook voorstellen dat straight blocking of beperkingen in de user devices in sommige gevallen een kostenefficiënt alternatief kunnen zijn. Denk bijvoorbeeld aan applicaties die evident veel bandbreedte gebruiken (peer to peer applicaties) op mobiele netwerken.

2.6.4 Geen consensus over de motieven

Er is in de literatuur geen consensus over welke motieven onwenselijk zijn. De discussie over welke motieven legitiem en welke motieven *onwenselijk* zijn en daarmee wat wel en wat niet een schending van netwerkneutraliteit is, is een morele discussie. Deze discussie zijn nadrukkelijk geen onderwerp van dit onderzoeksrapport.

3 Huidige marktsituatie

3.1 Inleiding

In dit hoofdstuk staat het eerste onderzoeksdoel centraal, namelijk het in kaart brengen van de huidige marktsituatie in Nederland. Ter vergelijking beschrijven we daarnaast ook de situatie in het buitenland. Meer specifiek komt het volgende aan de orde:

- Het Nederlandse debat over netwerkneutraliteit (paragraaf 3.2).
- De feitelijke Nederlandse situatie wat betreft netwerkneutraliteit: structurele en incidentele gevallen van het verschillend behandelen van verkeer (paragraaf 3.3).
- De Nederlandse situatie in relatie tot de situatie in het buitenland (paragraaf 3.4). We besteden hier met name aandacht aan de situatie in de Verenigde Staten en Canada.
- Een analyse en conclusies (paragraaf 3.5).

Paragraaf 3.2 en 3.3 zijn met name gebaseerd op de interviews, paragraaf 3.4 op desk research.

3.2 Het Nederlandse debat over netwerkneutraliteit

Hoe kijken verschillende partijen tegen het debat over netwerkneutraliteit aan? In deze paragraaf vatten we de belangrijkste standpunten en meningen samen zoals die tijdens de gesprekken zijn geuit.

Veel van de ISP's vinden de aandacht voor netwerkneutraliteit sterk overdreven. In hun ogen is er in Nederland geen sprake van een probleem en is de discussie 'theoretisch' of 'hypothetisch'. Ze vinden ook dat partijen de discussie van netwerkneutraliteit aangrijpen om andere zaken op de agenda te krijgen, zoals geschillen over peering (zie ook de beschrijving van een incident aangaande peering verderop in dit hoofdstuk).

Een aantal gesprekspartners (waaronder ook ISP's zelf) geeft echter wel aan dat netwerkneutraliteit in de toekomst een belangrijk issue *kan* worden (we gaan hier in hoofdstuk 5 dieper op in). Met name naarmate diensten van derde partijen (zoals VoIP) steeds meer gaan concurreren met de eigen diensten. In sommige gevallen is de ISP immers sterk afhankelijk van deze diensten (zoals spraaktelefonie of televisiedistributie).

Het is voor sommige respondenten een vraag of een volledig neutraal internet ooit heeft bestaan: verkeersmanagement is van alle tijden. Het verschillend behandelen van soorten verkeer (bijvoorbeeld op basis van het gebruikte protocol) wordt door veel gesprekspartners als rationeel beschouwd – in ieder geval niet als iets wat zondermeer onwenselijk is. Een interessant gegeven is dat deze mening niet alleen wordt geuit door de ISP's zelf, maar ook door een aantal applicatie- en contentproviders en door gesprekspartners die meer het belang van de consument vertegenwoordigen. Ook partijen die zich hard maken voor een 'open internet' wijzen traffic management bij congestie en differentiatie met verschillende SLA's niet bij voorbaat van de hand – zolang het gedrag maar goed inzichtelijk is voor de eindgebruiker. Prioritering op basis van de bron of bestemming van het verkeer ligt wél gevoelig; daar is het immers onduidelijk in hoeverre deze maatregelen een antwoord zijn op een technische noodzaak.

Sommige respondenten wijzen er ook op dat het niet zondermeer juist is om verschillende typen content en diensten als gelijk te beschouwen. Een P2P-programma houdt zich bijvoorbeeld zelden aan de 'etiquette' van het internet en opent niet een of twee, maar grote aantallen verbindingen (connecties). Het kan daarmee een buitenproportionele aanspraak doen op de aanwezige capaciteit – en doet dat vaak ook. Dit vertaalt zich in het problematisch functioneren van applicaties die wél netjes een enkele verbinding openen.

Structurele netwerkschaarste lijkt bij vaste netwerken vooralsnog niet of nauwelijks een rol te spelen. Met de aanwezigheid van AMS-IX zijn de interconnectiekosten relatief laag vergeleken met een land waar de ISP's veel meer op directe interconnectie zijn aangewezen. Ook de transit fees in Nederland zijn relatief laag omdat de AMS-IX leidt tot een ruim aanbod aan transit aanbieders en daarmee tot een forse concurrentie. De marges van ISP's staan wel in zekere mate onder druk. Door de hoge concurrentiedruk op de ISP-markt en de daaruit volgende scherpe consumententarieven wordt vaak zorgvuldig naar uitgaven gekeken zoals extra capaciteit in het aansluitnetwerk, capaciteit in het transportnetwerk/backhaul en de inkoop van transit-verkeer.

Er is ook een aantal partijen dat stelt dat er morele principes in het geding zijn. Juist de relatieve neutraliteit van het internet in het verleden zou hebben geleid tot een ongekend bloeiend netwerk. Zo zijn er allerlei nieuwe applicaties en toepassingsgebieden opgekomen die reguliere marktpartijen waarschijnlijk nooit zouden hebben geïntroduceerd. Het internet kent een grote dynamiek en het kan de dood in de pot betekenen als het verschillend behandelen van internetverkeer schering en inslag wordt. Een ander principieel punt is dat van privacy, mogelijke censuur[24] en dat de vervoerder "geen boodschap aan de boodschap mag hebben".

Een vaak gehoorde conclusie is dat er in Nederland een behoorlijke mate van feitelijke concurrentie tussen ISP's bestaat en dat het verschillend behandelen van internetverkeer al snel zal leiden tot een golf van negatieve reacties van intensieve gebruikers op bijvoorbeeld internet-blogs. Dat heeft snel gevolgen voor de concurrentiepositie en reputatie van de ISP. Met andere woorden: mocht de ISP een misstap begaan dan wordt dat snel afgestraft.

3.3 Verschillend behandelen van internetverkeer: structurele en incidentele gevallen

3.3.1 Structureel verschillend behandelen van internetverkeer

Tijdens de gespreksronden is de verschillende ISP's gevraagd of ze internetverkeer[25] verschillend behandelen; met andere woorden: wordt internetverkeer geprioriteerd of op een andere manier beïnvloed. Ook is ISP's gevraagd in hoeverre ze op de hoogte zijn van de situatie bij andere ISP's in binnen- en buitenland. Andere respondenten is dezelfde vraag gesteld. Tijdens dit onderdeel van de vraaggesprekken is zo feitelijk mogelijke informatie verzameld met betrekking tot de technische gedragingen van de ISP (zie paragraaf 2.4), dus nog los van de vraag welk motief aan die gedraging ten grondslag lag en in hoeverre dat motief als legitiem wordt gezien.

---

[24] Er zijn een paar gevallen bekend van (buitenlandse) ISP's die de toegang naar internetpagina's afsloten waarop negatieve berichten over het eigen bedrijf te lezen waren.

[25] Nogmaals: er is gevraagd naar *internettoegangsverkeer,* met andere woorden: het verkeer van de gebruiker van en naar het publieke internet (via transit, via peering of naar andere 'gewone' klanten van de ISP). Eigen diensten die van het internetprotocol gebruik maken maar niet die het publieke internet lopen, vallen hier buiten.

Vaste ISP's

Een belangrijke deel van de ISP's die *vaste diensten* aanbiedt, geeft aan dat ze internetverkeer in beginsel niet verschillend behandelen. De enige uitzondering daarop betreft blokkeringen in het kader van beveiliging van netwerk en eindgebruiker. Veel ISP's blokkeren daartoe bijvoorbeeld de poorten 135 tot en met 139.[26] Sommige ISP's blokkeren daarnaast poort 25 (de 'SMTP-poort'). [27] Het blokkeren van deze poorten is ook internationaal heel gebruikelijk.[28] Ook geven operators aan in te grijpen in het geval van aanvallen zoals de DoS-attack, of onverwachtse calamiteiten. Veel partijen geven ook aan centrale spam- en virusfilters in te zetten. Dit beschermt niet alleen de klanten, maar voorkomt ook dat de operator op internationale zwarte lijsten komt met als gevolg dat geen van de abonnees nog mail kan versturen. Soms is er sprake van blokkering op basis van de gebruikte randapparatuur bij de eindgebruiker. Dat wordt onder andere gedaan om te voorkomen dat gebruikers capaciteit van hun internettoegang doorverkopen aan andere consumenten.

Afgezien van bovenstaande beveiligingsmaatregelen geven ISP's internetverkeer niet verschillend te behandelen. Deze partijen melden ook dat ze verschillend behandelen problematisch zouden vinden omdat ze zich niet in staat achten om (a) te bepalen wat er – dan wel in de ogen van klant dan wel in hun eigen ogen – afgeknepen zou moeten worden en (b) om het specifieke verkeer op een betrouwbare manier te herkennen. In hun ogen is de beschikbare technologie (waaronder *deep packet inspection*) niet goed genoeg en kan het niet de capaciteit aan van een grootschalig netwerk.

Een aantal andere ISP's die vaste diensten aanbiedt zegt op drukke momenten wél aan 'network management' of 'traffic shaping' te doen. Dat gebeurt bij sommigen alleen in gevallen van congestie en bij andere op min of meer vaste perioden van de dag waarop het verkeer in het netwerk het meest intensief is. Deze partijen geven aan dat ze weliswaar volop aan netwerkinvesteringen doen maar desondanks de kwaliteit voor 'de reguliere gebruiker' niet kunnen garanderen vanwege de capaciteitsvraag van zware gebruikers (die in de regel aan P2P bestanduitwisseling doen). Hoewel de betrokken bedrijven ons niet in detail konden aangeven hoe de gedetailleerde filter-policies er uit zagen, is het wel duidelijk dat vooral P2P-verkeer afgeknepen wordt. Deze gedragingen vallen in de categorie need-based prioritisation (zie paragraaf 2.4.2). Op basis van onze gesprekken schatten we in dat ongeveer eenderde van de internetabonnees in Nederland te maken krijgt met need-based prioritisation. De onderliggende motieven lijken samen te hangen met de gebruikte technologie. Afhankelijk van de exacte werking van het netwerk doen zich op verschillende punten in het netwerk bottlenecks voor in de up- en downstream capaciteit. Deze bottlenecks kunnen vervolgens aanleiding geven om need-based prioritisation toe te passen. Hierbij merken we op dat de in Nederland gebruikte transportnetwerken voor ISP-diensten technische behoorlijk van elkaar verschillen. Bij diensten via de kabel liggen de capaciteitsbeperkingen vooral in het aansluitnetwerk, bij

---

[26] Daar wordt onder meer het zogenaamde NetBios-verkeer afgehandeld; verkeer dat in lokale netwerken belangrijk is voor bijvoorbeeld het delen van harde schijven maar waarvoor het sterk af te raden is ze toegankelijk te maken via het internet vanwege het grote risico op misbruik

[27] Poort 25 wordt vooral gebruikt voor uitgaande email via SMTP (dit is het protocol dat vaak in combinatie met POP3 wordt gebruikt, een populair en relatief simpel protocol voor inkomende email). Om SPAM te voorkomen, accepteren SMTP-servers zelden uitgaande e-mailberichten van klanten die zich niet op het eigen netwerk bevinden. Het is daarom ook amper een issue dat dergelijk uitgaand verkeer tegengehouden wordt.

[28] Akamai (2008). *The state of the internet, Q4 2008*. http://www.akamai.com/html/awe/login.html?&curl=/dl/whitepapers/akamai_state_of_the_internet_q4_2008.pdf

ADSL netwerken speelt dat minder maar kan er sprake zijn van capaciteitsbeperkingen in de zogenaamde backhaul (het transportnetwerk), terwijl bepaalde op glasvezel gebaseerde netwerken weer ergens anders beperkingen kennen. Hoewel die beperkingen vaak oplosbaar zijn is steeds de vraag hoeveel een netwerkexploitant moet investeren om een bepaalde capaciteitsbeperking te overwinnen.

Tijdens interviews werd er tot slot op gewezen dat er soms ook door randapparatuur of systemen wordt gefilterd, zonder toedoen van operators. Genoemde voorbeelden waren de toekomstige Philips IPTV-portal en de Microsoft Mediaserver.

Mobiele ISP's

ISP's die internetdiensten bieden over *mobiele netwerken* geven aan internetverkeer op diverse manieren verschillend te behandelen. Ten eerste wordt er bij de meeste mobiele aanbieders met specifieke abonnementsprofielen gewerkt. Bij de goedkoopste profielen is het vaak alleen mogelijk een aantal door de aanbieder vastgestelde websites (URL's) te bezoeken of zijn vastgestelde URL's gratis te bezoeken. Voor ander verkeer worden kosten gerekend. Bij de duurdere profielen is er sprake van een onbeperkte toegang, in feite vergelijkbaar met vaste toegang. Er wordt dan niet gefilterd. Sommige mobiele aanbieders laten VoIP-verkeer (Skype) toe, maar andere aanbieders doen dat niet.[29] Sommige mobiele aanbieders bieden zowel abonnement aan die Skype toelaten en abonnementen die het niet toelaten.

Verschillende mobiele ISP's geven aan dat bepaalde abonnementen alleen in combinatie met een telefoon als randapparaat mogen worden gebruikt en niet in combinatie met een laptop (of een telefoon doorverbonden aan een laptop, iets wat ook wel 'tethering' wordt genoemd). Ons is niet bekend in hoeverre mobiele aanbieders hier ook op controleren. Wel is bekend dat aanbieders van bepaalde mobiele telefoons tethering proberen te voorkomen. Voorbeeld is de recent geïntroduceerde Apple iPhone 3G, waarvan het flat-rate data-abonnement wel kan worden gebruikt in combinatie met de telefoon zelf, maar niet wanneer de telefoon verbonden is met een laptop. Daarbij komt ook de interessante vraag bovendrijven welke partij in de waardeketen de feitelijke beperking doorvoert en welke partij in de waardeketen daarvan profiteert. Dat hoeft namelijk niet dezelfde partij te zijn. In het genoemde voorbeeld is het bijvoorbeeld Apple die een blokkering doorvoert om de mobiele netwerken (een belangrijke business partner) ten dienste te zijn.[30]

Aanbieders van mobiele communicatie geven aan dat de capaciteit van mobiele netwerken veel meer aan grenzen is gebonden dan de capaciteit van vaste netwerken en dat het aanleggen van extra capaciteit in mobiele netwerken een kostbare aangelegenheid is. Als de omvang van het verkeer te groot wordt (bijvoorbeeld omdat mensen grootschalig P2P-applicaties via mobiele netwerken gaan gebruiken) kunnen ze in een situatie geraken waar 'traffic shaping' onontkoombaar is. In hun visie mag het niet zo zijn dat een klein aantal gebruikers het internetgebruik voor alle andere gebruikers zo goed als onmogelijk maakt. Overigens kan het zo zijn dat het strikt naleven van een 'fair use' policy hier voldoende is.

---

[29] Na de afronding van het onderzoek waarop dit rapport is gebaseerd ontstond er een publiek debat over het al dan niet blokkeren van Skype door mobiele operators; verschillende operators hebben als reactie daarop aangegeven Skype wel toe te gaan laten.

[30] Voor een gedetailleerde beschrijving van dit voorbeeld zie MacRumors (2008). *NetShare unlikely to return to US App Store*. http://www.macrumors.com/2008/08/08/netshare-unlikely-to-return-to-u-s-app-store/

Internet community

Op basis van gesprekken met *aanbieders van content en diensten* komt een beeld over het verschillend behandelen van internetverkeer naar voren dat grotendeels identiek is aan het beeld dat op basis van gesprekken met ISP's ontstaat. Deze partijen houden nauwgezet bij in hoeverre hun content of diensten goed hun weg vinden naar de eindgebruiker. Met systemen wordt continu de prestaties en throughput via de diverse netwerken gemonitord. Al met al geven ze aan bij het verspreiden van hun content weinig tot geen problemen te ondervinden die duiden op het structureel verschillend behandelen van internetverkeer. Daarbij moeten we wel opmerken dat subtiele vormen van tegenwerking misschien onopgemerkt zullen blijven. Enkele ICP/IAP's geven aan het vermoeden te hebben dat bepaalde vaste ISP's VoIP verkeer afknijpen, maar dat is niet met voldoende zekerheid te zeggen omdat overbelasting in het netwerk ook tot het haperen van een VoIP-dienst kan leiden.

Verschillende experts bevestigen bovenstaand beeld. Een interessant onderzoek[31] richt zich op de zogenaamde RST-berichten (ook wel bekend als 'TCP-reset'): een bericht dat aangeeft dat er iets verkeerd is gegaan in een communicatiesessie en dat de communicatie moet worden afgebroken. Deze berichten hebben een reguliere rol in het internetverkeer, maar een ISP kan ook besluiten 'valse' RST-berichten aan het verkeer toe te voegen om bepaalde soorten verkeer (zoals P2P) te frustreren. Daarmee is de inzet van RST-berichten een van de meest expliciete vormen van discriminerende verkeersbehandeling. Een recent onderzoek brengt het aantal RST-berichten bij P2P-verkeer in verschillende netwerken in kaart. Ongewoon hoge aantallen RST-berichten duiden daarbij op 'valse' berichten die door de ISP zijn toegevoegd. Nederlandse ISP's komen zo goed als niet voor op de lijst waar het aantal RST-berichten ongebruikelijk hoog is. Bij een ander, vergelijkbaar onderzoek, uitgevoerd door medewerkers van het Max Planck Institute for Software Systems, bleken geen Nederlandse servers te worden gevonden die TCP-resets gebruikten.[32] Het is belangrijk op te merken dat deze methode niet de enige manier is om P2P-verkeer te beperken; deze resultaten laten onverlet dat bepaalde ISP's P2P op bepaalde momenten van de dag beperken (*need-based prioritisation*), zoals eerder aangegeven.

3.3.2 Incidenten

Naast het structurele beleid van ISP's ten aanzien van internetverkeer hebben zich in de laatste jaren enkele situaties voorgedaan die we hier met 'incidenten' aanduiden.

Het meest bekende incident is zonder twijfel dat van de 'NOS Sportzomer'.[33] In de zomer van 2008 verspreidde de Nederlandse Publieke Omroep (NPO) live streams van circa 800kbps van de Tour de France, het EK voetbal en andere sportevenementen. Tienduizenden streams werden tegelijkertijd bekeken en er was – zo geven de betrokkenen aan – een servercapaciteit van circa 80 Gbps opgetuigd.[34] Met de meeste Nederlandse ISP's was er een peering-overeenkomst. Hierin was afgesproken om met gesloten portemonnee de

---

[31] Zie http://cache2.vuze.com/docs/internet_future/First_Results_from_Vuze_Network_Monitoring_Tool.pdf

[32] Dischinger et al. (2008). *Detecting bittorrent blocking*. http://doi.acm.org/10.1145/1452520.1452523 & http://broadband.mpi-sws.org/transparency/results/. Zie ook paragraaf 3.4.

[33] In de context van streaming van beeld en geluid heeft zich nog een vergelijkbaar, zij het kleiner, incident voorgedaan aangaande de verspreiding van Radio538-signalen.

[34] Dat is een substantiële capaciteit. Ter vergelijking: afhankelijk van hun grootte zijn ISP's in een land van de omvang van Nederland met een capaciteit van ergens tussen de 10 Gbps en de ongeveer 100 Gbps aan de buitenwereld verbonden.

gegevens aan te leveren. Terwijl sommige ISP's zich in staat achtten het verkeer zonder problemen door te geven, was er een grote ISP die stelde dat de hoeveelheid doorgestuurde informatie zo groot was dat deze niet door het netwerk kon worden afgeleverd zonder de kwaliteit van het internetverkeer van andere gebruikers nadelig te beïnvloeden. Er ontstond vervolgens een discussie tussen de betreffende ISP en NPO. De ISP gaf aan deze hoeveelheid verkeer niet te kunnen verwerken zonder extra investeringen en dat het een vergoeding verlangde voor deze extra investeringen. Anders zou ze besluiten de bestaande peering-overeenkomst te verbreken. Als NPO zou willen verzekeren dat alle abonnees van deze ISP toch de streams konden blijven kijken, zou ze het verkeer via de reguliere weg (ofwel via een transit aansluiting) aan moeten leveren, een optie die de NPO veel geld zou kosten. Over de discussie over het meebetalen aan extra investeringen en de precieze uitkomt van de zaak verschillen de lezingen van de betrokken partijen enigszins. Naar verluid heeft NPO niet extra willen betalen en zijn de beelden uiteindelijk verspreid met een maximum van 10.000 gelijktijdige kijkers.

Hier rijst de vraag: is een dergelijk conflict over peering en transit onderdeel van de discussie over netwerkneutraliteit? Het is zondermeer een interessante discussie of het verkrijgen van gratis toegang tot een ISP via peering een recht of een gunst is. Er zou zelfs – in het geval van een ISP met een dominante positie – een rol voor de overheid kunnen zijn. Maar in onze optiek gaat het hier niet over het *verschillend* of *discriminerend* behandelen van specifieke pakketjes binnen een verkeersstroom en dus niet over netwerkneutraliteit. Het moet bovendien benadrukt worden dat het een wat uitzonderlijke situatie betreft. De hoeveelheid verkeer die 10.000 streams genereren is ongewoon groot; het vormt zelfs een substantieel deel van de totale hoeveelheid verkeer die een ISP kan afwikkelen. Daarbij hanteerde NPO het argument dat zij gezien haar publieke functie niet de mogelijk had om beperkt te distribueren. Een 'gewone' commerciële partij heeft wel de keuze om te betalen voor transit dan wel een dienst met een kleinere 'footprint' uit te rollen.

3.4 Verschillen tussen Nederland en het buitenland

De concrete aanleiding voor dit onderzoek was de intensieve discussie over netwerkneutraliteit die in sommige andere landen wordt gevoerd. Deze paragraaf bespreekt daarom kort hoe de Nederlandse situatie zich verhoudt tot de situatie in het buitenland. Waarom is de situatie daar anders als in Nederland? Of is deze juist vergelijkbaar?

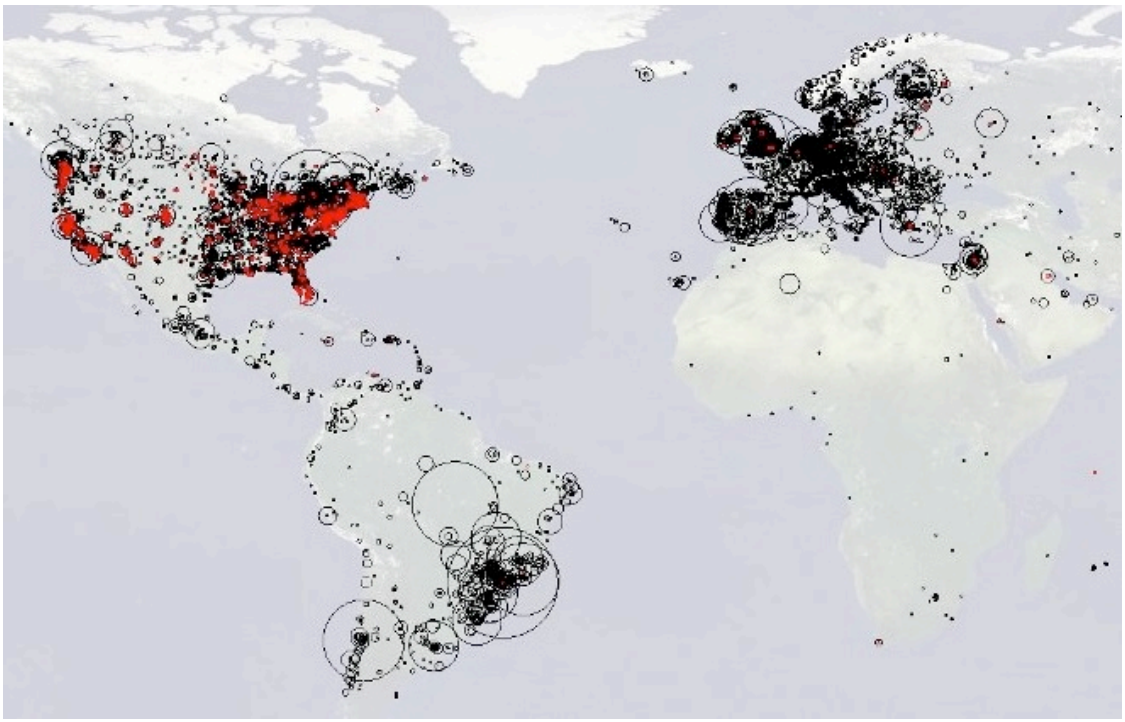
Allereerst gaan we in op de situatie in de VS. Zonder twijfel is dat het land waar de discussie aangaande netwerkneutraliteit het meest intensief wordt gevoerd. Een aantal jaar geleden gingen er zelfs stemmen op om niet-neutraal gedrag volledig te verbieden. Een wet wist in de zomer van 2006 echter niet de benodigde stemmen te halen in het U.S. House of Representatives. Naar verluidt ging het daarbij om een Republikeins nee: een verbod op het verschillend behandelen van internetverkeer werd als te zwaar overheidsingrijpen beschouwd. Maar dat wil niet zeggen dat de Federal Communications Commission (FCC) sindsdien niets meer heeft gedaan inzake netwerkneutraliteit. In verschillende gevallen van vermeende schendingen van netwerkneutraliteit heeft de FCC ingegrepen op basis van de "Four Internet Freedoms".[35] Dit zijn (1) Freedom to Access Content, (2) Freedom to Use Applications, (3) Freedom to Attach Personal Devices en (4) Freedom to Obtain Service Plan Information.[36] Op basis van deze vrijheden heeft de FCC onder meer

[35] Powell (2004). *Preserving internet freedom: Guiding principles for the industry*. http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-243556A1.pdf.

COMCAST gelast het afknijpen van P2P-verkeer te beëindigen. Maar die beslissing is niet onomstreden. COMCAST en andere betrokken marktpartijen trekken in twijfel of de Internet Freedoms wel de juridische status hebben om ze af te kunnen dwingen. De betreffende zaak loopt nog.[37]

In Canada besloot de regulator (CRTC) in 2008 dat het toelaatbaar (!) was dat Bell Canada op drukke tijden specifieke typen internetverkeer afkneep. Snel daarna bleken alle grote ISP's het beleid van Bell Canada over te nemen: inmiddels heeft het overgrote deel van de Canadese particuliere internetgebruikers te maken met een ISP die onder meer P2P-verkeer anders behandeld dan regulier verkeer.[38]

Het afknijpen van P2P-verkeer (vaak 'throttling' genoemd) is inmiddels redelijk gebruikelijk in de VS en Canada. We verwezen eerder in dit hoofdstuk al naar onderzoek over het afknijpen van P2P-verkeer met behulp van TCP-reset. Een soortgelijk onderzoek is gevisualiseerd in Figuur 7. Nogmaals, TCP-resets zijn niet de enige manier is om P2P-verkeer te beperken.



Figuur 7: Servers die door middel van valse TCP reset berichten P2P verkeer afknijpen (weergegeven in rood).[39]

In Europa en andere delen van de wereld komen het afknijpen van P2P-verkeer veel minder voor, aldus de onderzoeken naar TCP resets en diverse informatie op het internet. Een vaak gehoorde verklaring is dat er in de VS minder concurrentie is, er is in feite

---

[37] Ars Technica (2009). *Senator to FCC: time for black-and-white net neutrality rules*. http://arstechnica.com/tech-policy/news/2009/05/senator-pressures-fcc-on-net-neutrality.ars

[38] Ars Technica (2009). *How Canadian ISP's throttle the internet*. http://arstechnica.com/business/news/2009/01/how-canadian-isps-throttle-the-internet.ars

[39] Deze kaart is een uitsnede van de kaart weergegeven op http://broadband.mpi-sws.org/transparency/. Een interessant verschil met het eerder genoemde onderzoek van Dischinger et. al. is dat voor dit onderzoek al het verkeer van een vast punt kwam en dat zo op een betrouwbare manier 'valse' RST en andere RST van elkaar onderscheiden konden worden.

sprake van een duopolie. De (regionale) markten worden steeds beheerst door één incumbent telefonie-aanbieder en één kabelbedrijf. Omdat (in tegenstelling tot Europa) geen van deze ondernemingen de verplichting heeft andere ISP's op hun netwerk toe te laten, is de concurrentie zeer beperkt. In Nederland is er aanzienlijk meer mededinging, zie ook Box 3.

Een belangrijke maat voor mededinging is de concentratiegraad, waarbij wordt gekeken naar het aantal (onafhankelijke) aanbieders van producten of diensten in een bepaalde afgebakende (geografisch en o.b.v. product) markt. Nederland kent weliswaar een groot aantal ISP's maar die zijn echter niet allemaal onafhankelijk: na diverse acquisities is de ISP-markt nu voor 49% in handen van KPN. Daarnaast is ongeveer 40% in handen van de kabelbedrijven. Ongeveer 8% van de markt wordt bediend door andere ISP's met een eigen netwerk en de resterende 3% door ISP's zonder eigen netwerk.[40] Daar staat tegenover dat enkele KPN-dochters een zichtbaar eigen beleid voeren (XS4ALL is wat dat betreft een goed voorbeeld). Ook creëren de diverse glasvezelinitiatieven weer mededingingsdruk en zorgen Europese toegangsregels voor continue druk van potentiële toetreders. We concluderen dat de Nederlandse markt voor ISP-diensten een behoorlijke mate van mededinging kent, zeker in vergelijking met de VS.

Box 3. Mededinging in de Nederlandse markt voor ISP-diensten

3.5 Analyse en conclusies

In dit hoofdstuk stond het eerste onderzoeksdoel centraal: de huidige marktsituatie in Nederland en een vergelijking met die in het buitenland. Aan de hand van een analyse van de interviews en aanvullende bronnen en een toets in de validatieworkshop concluderen we het volgende:

In welke mate wordt internetverkeer in Nederland verschillend behandeld?

Bij ongeveer tweederde van de Nederlandse abonnementen voor vaste diensten zegt de ISP geen enkele vorm van prioritering, blokkering of traffic shaping/management toe te passen, met enkele uitzondering betreffende de veiligheid van de eindgebruikers. Bij ongeveer eenderde van de Nederlandse abonnementen voor vaste diensten vinden er vormen van traffic shaping plaats op de drukke momenten van de dag (*need-based prioritisation*). Eenderde is de meest ongunstige schatting; we gaan er dan vanuit dat de betreffende aanbieders traffic shaping toepassen voor *al* hun abonnees.

Bij de internetdiensten via mobiele netwerken vinden er diverse vormen van verschillend behandelen van verkeer plaats: afhankelijk van het abonnement worden bepaalde diensten zoals VoIP en bepaalde bestemmingen niet toegestaan en/of geblokkeerd (*active prioritisation* of *straight blocking*). Bij goedkopere abonnementen wordt het vaak niet toegestaan een laptop als randapparaat te gebruiken of een telefoon met een laptop te verbinden. Opmerkelijk is dat sommige producenten van randapparatuur meewerken aan dit verbod om de mobiele ISP's ter wille te zijn.

Hoe kijken verschillende stakeholders aan tegen (schendingen van) netwerkneutraliteit?

De mate waarin internetverkeer in Nederland momenteel verschillend behandeld wordt, wordt over het algemeen niet als problematisch beschouwd. De algemene opinie is dat het

[40] Actualiteiten Mededingingsrecht (2007). *Concentratie KPN-Tiscali: één ADSL-aanbieder minder.* http://www.mahleraandeamstel.nl/documenten/Actualiteit_Mededingingsrecht_07_10.pdf.

verschillend behandelen van internetverkeer *op basis van technische gronden* (zoals congestie) toelaatbaar is, mits er geen sprake is van bewuste onderinvestering in de capaciteit van een netwerk. Dat lijkt in Nederland vooralsnog niet het geval. Structurele prioritering (*active priorization*) op bron of bestemming ligt wel een stuk gevoeliger maar gebeurt bij vaste netwerken nauwelijks. Mede daarom vinden verschillende partijen de discussie op dit moment min of meer onnodig. Wel verwachten diverse partijen – waaronder ook ISP's – dat de discussie in de (nabije) toekomst veel belangrijker gaat worden (waarom dat zo is bespreken we nader we in hoofdstuk 5).

Hoewel bepaalde blokkeringen bij mobiele communicatie duidelijk zijn ingegeven door commerciële gronden (extra capaciteit is relatief duur) en niet door technische gronden, worden er door weinig van de interviewees bezwaren geuit. Blijkbaar beschouwt men dergelijke keuzen als toelaatbaar.

Hoewel er zich in de afgelopen jaren enkele incidenten hebben voorgedaan bij de doorgifte van internet-content, concluderen we dat het hier om uitzonderlijke omstandigheden ging. In het meeste bekende geval betrof het een *interconnectiegeschil*. Partijen kunnen het oneens zijn over de mate waarin ze elkaar gunstige peering-overeenkomsten aanbieden, maar zolang er via de reguliere weg (transit) nog steeds interconnectie wordt geboden gaat het ons inziens niet om het verschillend behandelen van verkeer.

Volgens verschillende respondenten is het uitblijven van structurele problemen te wijten aan de alerte en mondige internetgemeenschap. Een misstap van een ISP leidt al snel tot veel commentaar en kan snel leiden tot een concurrentienadeel of reputatieschade.

Hoe verhoudt de Nederlandse situatie zich met die in het buitenland?

In een aantal landen – met name de Verenigde Staten en Canada vallen op – wordt internetverkeer betrekkelijk vaak verschillend behandeld. De discussie over netwerkneutraliteit is er veel intenser en is gezien het feitelijk gedrag van partijen (bijvoorbeeld het afknijpen van P2P) ook niet theoretisch.

De gedragingen in de VS worden toegeschreven aan de relatief lage mate van concurrentie. In de meeste gebieden in de VS liggen twee netwerken: een telefonienetwerk en een kabelnetwerk. Omdat de beheerders van deze netwerken niet verplicht zijn toegang tot hun netwerk te verlenen, zijn ze tevens de enige aanbieders van internettoegang in hun markt. Er is dus sprake van een duopolie. De verschillen met Nederland kunnen deels verklaard worden door de hogere mate van mededinging. Maar dat is wellicht niet de enige reden. Het is mogelijk dat er in de VS en Canada (1) minder in capaciteit is geïnvesteerd en men nu meer moeite heeft de vraag te kunnen volgen[41] en/of (2) ISP's meer commerciële druk ervaren omdat derde partijen (zoals Vonage, een alternatieve VoIP-aanbieder) al een substantieel marktaandeel hebben opgebouwd. Daarmee is mogelijk ook de prikkel groter om internetverkeer verschillend te behandelen.

[41] Om diverse redenen zijn de kosten voor het vergroten van capaciteit in de VS groter, denk aan (1) demografische omstandigheden, (2) minder investeringen in het recente verleden en (3) het ontbreken van wat in Nederland de AMS-IX is, met als gevolg dat partijen tegen hoge kosten onderling fysieke verbindingen moeten aanleggen om verkeer uit te wisselen.

4 Transparantie

4.1 Inleiding

In dit hoofdstuk wordt de tweede doelstelling van onderliggend onderzoek behandeld: het vergroten van transparantie over het verschillend behandelen van netwerkneutraliteit. Achtereenvolgens komt aan de orde:

- De *rationale* achter transparantie (paragraaf 4.2). De onderliggende vraag is waarom in Europa (inclusief Nederland) vooral op het vergroten van transparantie wordt ingezet terwijl in de VS de nadruk ligt op een directere aanpak van netwerkneutraliteit.
- Het *huidige niveau van transparantie* in Nederland (paragraaf 4.3). Er is onderzocht (1) hoe transparant internetaanbieders richting toekomstige klanten communiceren over het verschillend behandelen van internetverkeer, (2) hoe transparant internetaanbieders zichzelf vinden en (3) hoe transparant andere belanghebbenden internetaanbieders vinden.
- Hoe *transparantie vergroot zou kunnen worden* (paragraaf 4.4). We introduceren (1) een aantal uitgangspunten voor het vergroten van transparantie en behandelen (2) de rol van de overheid bij het vergroten van transparantie en (3) de kosten en baten van het vergroten van transparantie.

4.2 Rationale achter transparantie

Eerder in dit rapport werd de discussie over netwerkneutraliteit gekenschetst als een debat over de mate waarin internetverkeer verschillend behandeld mag worden. Enigszins gepolariseerd kunnen we stellen dat het een strijd is tussen ISP's en de voorstanders van een neutraal internet (Google, Microsoft, et cetera). De ISP's vinden het wenselijk of zelfs noodzakelijk om internetverkeer verschillend te behandelen. Redenen daarvoor zijn onder andere netwerkbeveiliging, toenemende netwerkschaarste (door meer gebruikers die meer verkeer veroorzaken) en marges die steeds meer onder druk staan. Aan de andere kant staan de voorstanders van een neutraal internet: zij vrezen dat het open karakter van het internet (en daarmee het innovatiepotentieel) in gevaar komt als ISP's – in plaats van de consumenten – gaan bepalen welke content, diensten en toepassingen onbeperkt toegankelijk zijn en welke niet.

4.2.1 Amerika versus Europa: wel of niet direct ingrijpen?

De vraag waar de overheid voor staat is in welke mate zij zich moet mengen in dit debat, en wanneer ze eventueel moet ingrijpen in de markt. Belangrijk daarbij is dat overheidsingrijpen in beginsel een reactie is op marktfalen: de situatie waarbij de markt 'uit zichzelf' geen optimale uitkomst tot stand brengt. Marktfalen kan verschillende redenen hebben[42] maar meest waarschijnlijk in het geval van netwerkneutraliteit is (a) afnemers niet de mogelijkheid hebben om te kiezen tussen aanbieders, ofwel omdat er onvoldoende

[42] In de economische literatuur staande volgende oorzaken van marktfalen centraal: (1) er is geen of slechts beperkt sprake van mededinging, (2) de betrokken partijen beschikken niet over volledige informatie, (3) er zijn toe- en uittredingsbarrières, (4) er is sprake van transactiekosten, of (5) de markt bestaat uit niet homogene producten.

mededinging is ofwel omdat er sprake is van substantiële overstapdrempels en/of (b) afnemers niet weten in welke mate verschillende aanbieders internetverkeer verschillend behandelen. Ingrijpen moet gericht zijn op het wegnemen van marktfalen, meestal door de oorzaken van het marktfalen te adresseren. Daarbij is er tevens het criterium van proportionaliteit: ingrijpen gaat gepaard met kosten (bij de overheid, bij marktpartijen en/of bij consumenten) en deze kosten mogen niet groter zijn dan de baten die worden gerealiseerd bij het wegnemen van het marktfalen.

De Amerikaanse en Europese markt voor internettoegang verschillen. Deze verschillen resulteren in een andere aanpak van netwerkneutraliteit. De Amerikaanse markt kent een beperkte mate van mededinging (er is in de VS op de meeste plaatsen sprake van een duopolie; zie paragraaf 3.4). De mate van mededinging kan niet op een eenvoudige wijze worden vergroot. Dat betekent een grote kans op marktfalen. Om die reden heeft men er (tot op zekere hoogte; zie opnieuw paragraaf 3.4) voor gekozen direct in te grijpen in netwerkneutraliteit door een poging om harde grenzen aan niet-neutraal gedrag op te leggen (in paragraaf 3.4 bespreken we in welke mate men er in geslaagd is deze regelgeving ook daadwerkelijk te adopteren).

In de Europese context liggen de zaken anders. Hier is in de meeste gevallen wél sprake van voldoende mededinging – zeker in het geval van Nederland.[43] Door gereguleerde toegang tot het kopernetwerk van de incumbent en de brede uitrol van coaxkabel hebben de meeste consumenten de keuze uit een aantal verschillende internetaanbieders. Dat geldt ook voor mobiel internet.[44] De oorzaak van het falen van de markt in Europa is eerder toe te schrijven aan het ontbreken van informatie, en dan met name bij de gebruikers. Het ingrijpen in de vorm van een verplichting tot transparantie is dan meer op zijn plaats. Een tweede argument tegen direct ingrijpen (harde grenzen stellen) heeft betrekking op de proportionaliteit van dat ingrijpen. Het zal naar verwachting gepaard gaan met aanzienlijke kosten. De kosten die de overheid (voor het implementeren van het ingrijpen) en de marktpartijen maken zullen uiteindelijk gedragen worden door de consumenten, in de vorm van belastingen en tarieven. Op korte termijn zal door minder productdifferentiatie de markt vermoedelijk minder goed bediend worden.[45] Op langere termijn bestaat het risico dat ISP's minder bereid zullen zijn te investeren in netwerken[46] en kan innovatie binnen het netwerk belemmerd worden. Deze kosten staan naar verwachting niet in verhouding tot de baten van direct ingrijpen.

Daar komt nog bij dat het stellen van de grens in het geval van direct ingrijpen lastig is. Er is een gebrek aan consensus wat betreft de vraag in welke mate verschillende soorten internetverkeer verschillend behandeld mogen worden. Dat komt onder meer omdat er

---

[43] Zie het eerder genoemde rapport van de OECD, alsmede Box 3.

[44] Er zijn drie aanbieders met een eigen mobiel netwerk, en daarnaast zijn verschillende *virtuele* aanbieders (MVNO's) actief.

[45] Ter illustratie: momenteel bieden Nederlandse mobiele ISP's internetabonnementen voor ca. €10. Die abonnementen kennen in bepaalde gevallen beperkingen ten aanzien van het gebruik van VoIP. De ISP's bieden ook duurdere abonnementen aan die deze beperking niet kennen. Zou het verschillend behandelen van internetverkeer niet langer worden toegestaan dan verdwijnt deze mogelijkheid tot productdifferentiatie en bestaat de kans dat het goedkope abonnement verdwijnt. Klanten die helemaal niet geïnteresseerd zijn in VoIP gaan er zo wel aan meebetalen.

[46] Ter illustratie: Als ISP's niet wordt toegestaan om bijvoorbeeld P2P-verkeer verschillend te behandelen, terwijl ze de andere diensten op een bepaald kwaliteitspeil willen houden, kunnen ze geconfronteerd worden met hogere kosten voor het aansluitnetwerk, het transportnetwerk, of voor de kosten voor de inkoop van verkeer. Dat resulteert in een minder gunstige *business case*, hetgeen de bereidheid tot investeren zal verminderen.

verschillende motieven voor het verschillend behandelen bestaan (zie hoofdstuk 2), er verschillende inzichten bestaan welke motieven daarvan legitiem zijn of niet, en omdat uit een bepaalde handeling niet eenduidig opgemaakt kan worden wat het achterliggende motief voor die handeling is ('Was er een technische noodzaak?' 'Is er bewust ondergeïnverteerd?' 'Probeert men eigen diensten te beschermen?'). Zelfs als er consensus zou bestaan over een bepaalde grens dan kan die grens door technologische ontwikkelingen of door ontwikkelingen in de markt achterhaald raken. Hierbij wordt direct een ander voordeel van een transparantiebeleid duidelijk: de regelgever staat daarbij niet voor de taak de achterliggende motieven te achterhalen en te beoordelen.

4.2.2 Huidig beleid in Nederland

De hierboven beargumenteerde keuze voor transparantie sluit aan bij Europese plannen over netwerkneutraliteit. In de universele-dienstenrichtlijn, die naar aanleiding van de herziening van het regelgevend kader momenteel wordt vernieuwd, is bijvoorbeeld de volgende passage opgenomen:[47] [48]

> *"Lidstaten zien erop toe dat wanneer contracten worden gesloten tussen abonnees en aanbieders van elektronische communicatiediensten en / of -netwerken, bedoelde abonnees alvorens een contract wordt gesloten en op gezette tijden daarna duidelijk worden geïnformeerd over eventuele door de aanbieder opgelegde beperkingen van hun toegang tot wettelijke inhoud of van hun vermogen om dergelijke inhoud te verspreiden of wettelijke toepassingen en diensten van hun keuze te gebruiken."*

Deze lijn wordt ook in enkele recente onderzoeksrapporten over netwerkneutraliteit onderschreven, waaronder het eerder genoemde OECD-rapport en een recent rapport van WIK. WIK[49] adviseert om "informed consumer choice" te stimuleren, naast blijvend in te zetten op concurrentie in de telecommarkt. Het is overigens niet gezegd dat transparantie geen uitdagingen kent (die uitdagingen zijn onderwerp van dit hoofdstuk) maar het is om voornoemde redenen te prefereren boven andere mogelijkheden netneutraliteit aan te pakken, zoals direct ingrijpen.

Wel merken we op dat een goed functionerende markt niet in alle gevallen tot een oplossing van de netwerkneutraliteit problematiek leidt. Zoals eerder aangegeven: de discussie over netwerkneutraliteit is begonnen omdat bepaalde partijen vreesden dat het innovatiepotentieel van het internet in gevaar zou komen. Dat potentieel wordt vaak toegeschreven aan het neutrale of open karakter van het internet.[50] Omdat alle IP-

---

[47] Europese Commissie (2007). *Richtlijn van het Europees Parlement en de Raad tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronische-communicatienetwerken en –diensten*. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0698:FIN:NL:PDF. Overigens is de betreffende passage sinds dit eerste voorstel uit november 2007 al een aantal keer gewijzigd. We komen daar in paragraaf 4.4 op terug.

[48] De Europese plannen zijn overigens tweeledig, de universele-dienstenrichtlijn bevat tevens de volgende passage: "… in bijzondere gevallen [wanneer er geen effectieve mededinging is, red.] moet er eventueel over worden gewaakt dat openbare communicatienetwerken aan minimum kwaliteitsniveaus voldoen teneinde achteruitgang van de dienstverlening, gebruiksbeperkingen en vertraging van het verkeer te voorkomen."

[49] Carter et al. (2008). *Network neutrality: implications for Europe*. http://www.wik.org/content/diskus/Diskus_314.pdf

[50] In hoeverre het innovatiepotentieel van het internet inderdaad aan haar neutrale karakter kan worden toegeschreven is een discussie op zich en geen onderwerp van dit rapport.

pakketten hetzelfde behandeld worden kan iedere aanbieder iedere dienst of toepassing aan iedere klant leveren. Dit is in feite de ultieme vrije markt. Dat neutrale karakter is onder een goed functionerende markt niet per se gewaarborgd. Het is goed denkbaar dat de markt (de consumenten) de 'discriminatie' van internetverkeer tot op zekere hoogte accepteert, in ruil voor een lagere prijs.[51] Het is ook mogelijk dat eindgebruikers een bepaalde vorm van discriminatie niet als nadelig beschouwen omdat de op dat moment populaire diensten en toepassingen er niet onder lijden. Als een nieuwe, innovatieve dienst daar wel last van heeft zal de markt dat niet massaal afstraffen omdat die dienst onder het grote publiek onbekend is.[52] Samengevat: een goed functionerende markt zal naar verwachting leiden tot de juiste mix van prijs- en productdifferentiatie, de juiste verhouding tussen prijs en 'openheid', et cetera. De gevolgen voor investeringen en innovatie (met onderscheid tussen innovatie binnen de netwerken en innovatie in de periferie) zijn minder gemakkelijk te voorspellen. Maar nogmaals: eventuele negatieve gevolgen zullen naar verwachting minder sterk zijn dat in het scenario van direct ingrijpen.

4.3 Huidig niveau van transparantie

Deze paragraaf introduceert allereerst verschillende vormen van transparantie en bespreekt die verschillende vormen vervolgens voor de Nederlandse situatie. Die Nederlandse situatie is vanuit drie perspectieven geanalyseerd:

1. Dialogic heeft 26 internetaanbieders (15 vast en 11 mobiel) in een *mystery guest* onderzoek gevraagd naar de eventuele beperkingen (in termen van diensten of toepassingen) van een nieuwe internetaansluiting.

2. Daarnaast is een vijftal aanbieders in *face-to-face* interviews gevraagd in hoeverre zij transparant zijn over het eventueel verschillend behandelen van internetverkeer.

3. Tot slot zijn andere betrokkenen (aanbieders van diensten en content, vertegenwoordigers van consumenten, internetexperts) gevraagd naar hun mening over het niveau van transparantie.

Een disclaimer is hierbij op zijn plaats. Zoals uit het vorige hoofdstuk bleek, is er in Nederland – vooral op het vaste netwerk – in tweederde van de gevallen nauwelijks sprake van het verschillend behandelen van internetverkeer. Een lastige vraag is wat je in die gevallen als transparantie kwalificeert. Is een ISP die niet aan verschillend behandelen doet en daarom niet over dat onderwerp communiceert transparant? En zo ja: is dat een garantie voor transparantie mocht die ISP in de toekomst internetverkeer wél verschillend gaan behandelen?

---

[51] Ook nu al geeft prijs vaak de doorslag bij de aanschaf van een internetverbinding, aldus de Consumentenbond.

[52] Dit probleem speelt tot op zekere hoogte bij P2P. Dat protocol wordt vaak geassocieerd met het illegaal uitwisselen van muziek en het is goed mogelijk dat veel eindgebruikers het frustreren van P2P om die reden niet als afkeurenswaardig beschouwen. Een relatief onbekende dienst als Joost werkt echter ook op basis van P2P.

4.3.1 Verschillende vormen van transparantie

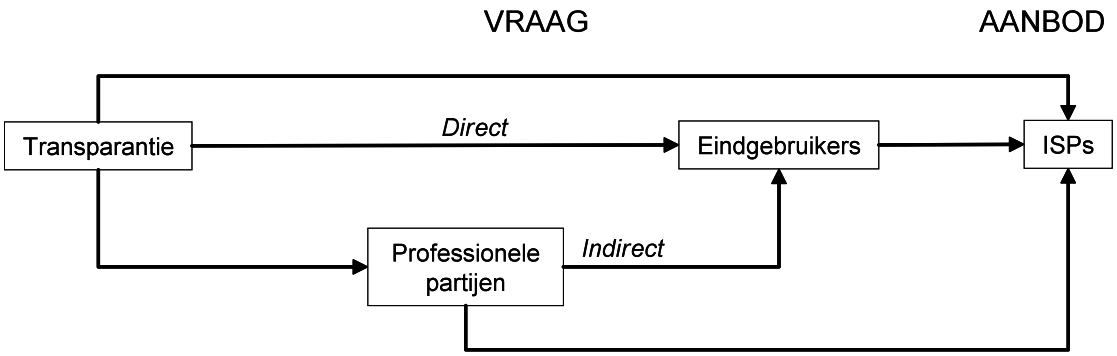
Op basis van het afwegingskader voor transparantie[53] van het Ministerie van Economische Zaken is de volgende definitie voor transparantie denkbaar:

> *Er is sprake van transparantie over het verschillend behandelen van internetverkeer als "consumenten inzicht hebben in de mate waarin verschillende aanbieders internetverkeer verschillend behandelen, zodat zij een afgewogen keuze kunnen maken".*

Nota bene, het gaat hier specifiek om transparantie *over het verschillend behandelen van internetverkeer*, niet over transparantie in het algemeen. De discussie over transparantie ten aanzien van netwerkneutraliteit kan volgens ons niet los worden gezien van de discussie over transparantie over andere eigenschappen van internetdiensten. Dit is een punt dat in hoofdstuk 6 aan de orde zal worden gesteld. In deze studie beperken we ons echter tot het debat over het al dan niet verschillend behandelen van internetverkeer. Wat betreft transparantie gaat het dan om de vraag of en in welke mate eindgebruikers op de hoogte zijn van het feit dat hun ISP internetverkeer al dan niet verschillend behandeld wordt.

Consumenten kunnen op twee manieren inzicht krijgen in de manier waarop ISP's omgaan met internetverkeer. Ten eerste komt het inzicht direct tot stand, in de interactie tussen de ISP en de eindgebruiker. Voorwaarde is dan wel dat de informatie die door de ISP wordt gepresenteerd begrijpelijk is voor "de gemiddelde internetabonnee". Het verschillend behandelen van internetverkeer is complexe materie en het is de vraag of het realistisch is om te verwachten dat consumenten in hun keuze voor een bepaalde aanbieder het verschillend behandelen van internetverkeer expliciet meenemen. In het tweede geval komt het inzicht indirect tot stand, via partijen zoals leveranciers van internetcontent en -applicaties en intermediaire partijen zoals consumentenorganisaties, pers en communities van IT-professionals. Zoals gezegd houden content- en applicatieleveranciers nauwgezet bij of hun content wel goed haar weg vind naar eindgebruiker. Deze leveranciers zijn daar veel beter toe in staat dan een individuele gebruiker, alleen al omdat ze veel meer waarnemingen (meerdere aansluitingen, volcontinu) kunnen doen dan een consument en zo een veel beter overzicht hebben van de markt. De vraag is dan natuurlijk wel in hoeverre de mening van de intermediaire partijen ook het keuzegedrag van de eindgebruikers bepaalt. Tenslotte wijzen we erop dat transparantie niet alleen de vraagkant (consumenten, professionele partijen) maar ook rechtstreeks de aanbodkant kan beïnvloeden. Vanwege reputatie-effecten kunnen ISP's bijvoorbeeld hun gedrag aanpassen, ook als er geen directe aanleiding toe is vanuit de vraagkant. Een en ander is weergegeven in Figuur 8.

[53] Ministerie van Economische Zaken (2002). *Glashelder: meer inzicht in transparantie*. Intern document Ministerie van Economische Zaken.



Figuur 8. Theoretische invloed van transparantie op gedrag van ISP's

In de volgende paragrafen worden de verschillende vormen van transparantie specifiek voor de Nederlandse markt besproken.

4.3.2 Directe transparantie

Om inzicht te krijgen in hoeverre ISP's consumenten direct informeren over het al dan niet verschillend behandelen van internetverkeer zijn vijftien vaste en elf mobiele ISP's namens een *mystery guest* ("de gemiddelde consument") benaderd. Dat is op twee manieren gedaan:

1. De consument heeft tien minuten op de website van de ISP gezocht, o.a. in de algemene voorwaarden en de FAQ, via de zoekfunctie van de betreffende website en via Google.

2. De consument heeft contact gezocht met de helpdesk van de ISP. Waar mogelijk is dat per e-mail gedaan. Daarbij is specifiek en direct naar beperkingen ten aanzien van content en toepassingen gevraagd.[54]

Op de website van de vijftien vaste ISP's is geen informatie gevonden over het verschillend behandelen van internetverkeer. Ook de helpdesks van de vaste ISP's geven – zover zij bereikbaar waren – merendeels aan dat er geen sprake is van het verschillend behandelen van internetverkeer. Eén ISP geeft aan bepaalde nieuwsgroepen te blokkeren. Daarentegen wordt op de website van verschillende mobiele ISP's wél aangegeven dat bepaalde diensten geblokkeerd worden. Op vijf van de elf bezochte websites is te lezen dat bijvoorbeeld VoIP en vormen van modemgebruik geblokkeerd zijn. Ook de helpdesks van mobiele ISP geven meer informatie over het verschillend behandelen van verkeer. Ongeveer tweederde[55] van de helpdesks gaf aan dat er bepaalde blokkeringen (VoIP, modemgebruik) of beperkingen (snelheidsbeperking na gebruik bepaalde datacapaciteit) van toepassing zijn.[56]

Zetten we dit af tegen de mate waarin internetverkeer in Nederland verschillend behandeld wordt (zie hoofdstuk 3) dan blijkt vooral de directe transparantie voor verbetering vatbaar.

---

[54] "Ik ben op zoek naar een nieuwe ISP / mobiele aanbieder en heb een vraag met betrekking tot jullie (mobiele) internetabonnementen. Zijn er bepaalde beperkingen op de toepassingen (bijvoorbeeld P2P of VoIP) die ik kan gebruiken? Of zijn er snelheidsbeperkingen of andere specifieke blokkeringen?"

[55] Hierbij zijn de helpdesks buiten beschouwing gelaten die niet bereikbaar waren.

[56] De laatste soort beperkingen vallen niet onder het verschillend behandelen van dataverkeer.

Ongeveer eenderde van de vaste abonnees krijgt bijvoorbeeld te maken met het afknijpen van P2P en dat wordt onvoldoende inzichtelijk gemaakt.

Interessant is dat Nederlandse ISP's zichzelf wél transparant vinden. Verschillende partijen geven aan dat ze niks hebben om open over te zijn – ze doen immers in het geheel niet aan het verschillend behandelen van internetverkeer.[57] De meeste partijen die internetverkeer wel verschillend behandelen, zeggen daar open over te zijn. Daarbij hoort dan de toevoeging dat de ISP alleen die informatie verstrekt waarvan het denkt dat de gemiddelde consument behoefte heeft. Onderwerpen als netwerkmanagement – kritisch voor dit onderzoek – hoort daar niet altijd bij.

De professionele organisaties (aanbieders van content en applicaties, consumentenorganisaties, experts) zijn beduidend kritischer. Volgens de meeste van onze respondenten is het slecht gesteld met de transparantie. Die mening moet overigens wel in perspectief worden gezien: verschillende respondenten wijzen in hun reactie op het gebrek aan transparantie ten aanzien van met *de overboekingsfactor* van een internetverbinding. Nu verwijst dat laatste naar de manier waarop alle internetverkeer wordt behandeld. Er wordt dus geen verschil gemaakt tussen de verschillende soorten internetverkeer. Welbeschouwd valt dit dan ook niet onder het onderwerp netwerkneutraliteit. Desalniettemin lijkt een aantal respondenten een gebrek aan transparantie ten aanzien van het specifiek behandelen van verkeer af te leiden uit een gebrek aan transparantie ten aanzien van het generiek behandelen van verkeer. Het is de vraag is of dat terecht is.

4.3.3 Indirecte transparantie

Voor ervaren gebruikers en professionele organisaties liggen de zaken anders dan voor de gemiddelde consument. Deze partijen hebben veel aandacht voor het verschillend behandelen van internetverkeer door ISP's. Dergelijk gedrag wordt op internetfora als Tweakers uitgebreid bediscussieerd.[58] Ook aanbieders van internetdiensten en –content nemen actief deel aan die discussies.

Verschillende ISP's geven ook aan deze discussies op de voet te volgen. In een enkel geval hebben ISP's zich zelfs openlijk gemengd in de discussies en gericht informatie gegeven over het beleid dat zij ten aanzien van verschillende typen internetverkeer voeren. ISP's zelf ervaren dit als een meer effectieve vorm van transparantie dan directe transparantie (het op de website publiceren van informatie gericht aan de gemiddelde eindgebruiker).

Tot slot bestaan er verschillende programma's waarmee ervaren gebruikers – de bediening is niet altijd eenvoudig – het verschillend behandelen van internetverkeer binnen het netwerk van de eigen ISP kunnen opsporen. Voorbeelden zijn EFF's Switzerland Network Testing Tool en Google's M-labs.[59]

De vraag is natuurlijk in hoeverre deze informatie ook de gemiddelde consument bereikt. Pas dan is er immers daadwerkelijk sprake van indirecte transparantie. Ervaren gebruikers

---

[57] Nogmaals, wellicht ten overvloede: dan hoeft er nog geen sprake te zijn van transparantie in het algemeen. De consument kan bijvoorbeeld nog steeds niet de kwaliteit van de verschillende diensten van de verschillende aanbieders goed met elkaar vergelijken.

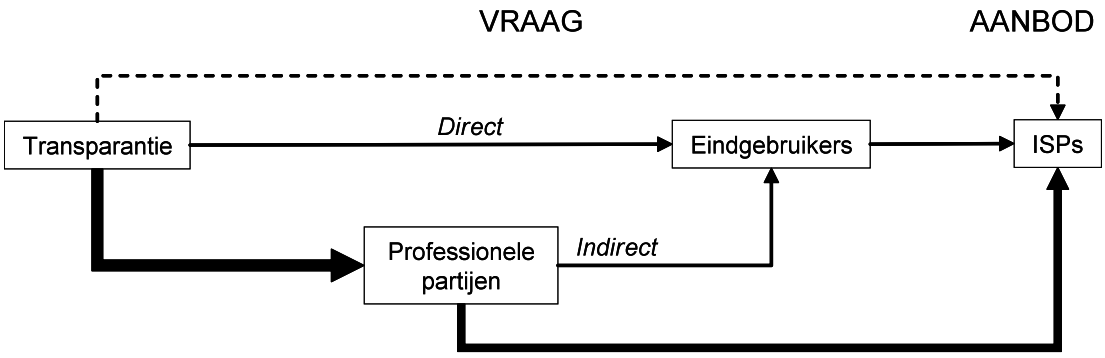
[58] http://tweakers.net/

[59] Zie http://www.eff.org/press/archives/2008/07/31 en http://www.measurementlab.net/. Een interessante vraag is overigens hoe goed dergelijke programma's werken. In een van de gesprekken kwam naar voren dat verschillende Europese ISP's geïnteresseerd zijn in apparatuur die – door genoemde programma's – lastig te detecteren is.

mogen dan op de hoogte zijn van het feit dat eenderde van de vaste abonnees – toch een substantieel aandeel – te maken kan krijgen met het afknijpen van P2P. In de algemene opinie lijkt hier vooralsnog niet of nauwelijks aandacht aan te worden gegeven.

4.3.4 Gedrag consument versus gedrag ISP

Het is onduidelijk of de gemiddelde consument zich momenteel laat beïnvloeden door informatie over het verschillend behandelen van internetverkeer. Buiten het feit dat verschillend behandelen sowieso beperkt voorkomt en dat er niet in alle gevallen volledige transparantie over bestaat, is duidelijk dat consumenten zich bij de aanschaf van een internetverbinding primair door prijs (eventueel in relatie tot andere zichtbare producteigenschappen zoals maximale bandbreedte en opzegtermijn) laten leiden. Het is een teken aan de wand dat zowel bij ISP's als bij consumentenorganisaties tot dusver geen enkele klacht is ontvangen over het verschillend behandelen van internetverkeer. Ervaren gebruikers zullen zich waarschijnlijk wel laten beïnvloeden.



Figuur 9. Feitelijke invloed van transparantie op gedrag van ISP's

De indirecte relatie via professionele organisaties en ISP's lijkt van groter belang te zijn. ISP's geven aan gevoelig te zijn voor de discussie binnen de internet community en hun gedrag daardoor ook te laten beïnvloeden. Andersom geven ook de professionele organisaties (zoals de leveranciers van internetdiensten en –content) aan dat ze verwachten dat ISP's reageren op eventuele klachten over het verschillend behandelen van internetverkeer. Die gevoeligheid van ISP's voor signalen uit de *internet community* wordt door verschillende respondenten genoemd als één van de redenen waarom in Nederland relatief weinig sprake is van verschillend behandelen van internetverkeer.

4.4 Vergroten van transparantie

Op basis van de voorgaande paragraaf concluderen we dat inzetten op het vergroten van transparantie een legitieme beleidskeuze is voor de Nederlandse overheid. Weliswaar is er tot op zekere hoogte sprake van transparantie; ervaren gebruikers zijn veelal op de hoogte en ISP's geven aan gevoelig te zijn voor de mening van deze partijen. Maar er is absoluut ook ruimte voor verbetering. Meest belangrijk: eenderde van de vaste abonnees in Nederland krijgt te maken met het beïnvloeden van P2P-verkeer en de gewone consument is daar vaak niet van op de hoogte. Bovendien – zo werd in paragraaf 4.2 besproken - kent transparantie niet de toch wel aanzienlijk nadelen van direct ingrijpen en is het in lijn met het verwachte beleid van de Europese Commissie.

In de volgende paragrafen werken we de implementatie van transparantie verder uit. We definiëren allereerst een aantal uitgangspunten voor transparantie. Vervolgens behandelen we de mogelijke rol van de overheid en van andere partijen. De voorstellen en

overwegingen daarbij zijn met name gebaseerd op interviews met betrokken partijen en op de resultaten van de validatieworkshop (zie bijlage C).

4.4.1 Uitgangspunten voor transparantie

Allereerst dient het begrip 'transparantie' duidelijk te worden afgebakend. Dan kan in ieder geval volgens drie dimensies: *wie* moet er transparant zijn over *wat* en voor *wie* is die transparantie bedoeld. We stellen hier de volgende uitgangspunten voor:

- *Wie moet er transparant zijn?*
    - De aanbieder van vaste ISP-diensten.
    - De aanbieder van mobiele ISP-diensten.
- *Waarover moet transparantie bestaan?*
    - Over internettoegangsdiensten. IP-telefonie- of IP-televisiediensten die niet via het openbare internet verlopen horen daar niet bij.
    - Over de volledige keten die de ISP verzorgt. Dus van klantaansluiting (of afleverpunt) tot aan de plaats waar interconnectie met andere internetpartijen plaatsvindt.
    - Over het verschillend behandelen van verschillende typen internetverkeer binnen een abonnement. Er hoeft geen transparantie te zijn over de generieke behandeling van internetverkeer, bijvoorbeeld overboekingsfactoren. Ook hoeft niet gerapporteerd te worden over het blokkeren van verkeer in opdracht van de overheid.[60]
- *Voor wie is de transparantie bedoeld?*
    - Particuliere eindgebruikers (hier ligt in de EU richtlijn de nadruk op).
    - Zakelijke eindgebruikers.

Idealiter zou de informatie over het al dan niet verschillend behandelen van internetverkeer naast te voldoen aan voornoemde uitgangspunten zowel begrijpelijk als feitelijk moeten zijn. Met *begrijpelijk* bedoelen we dat consumenten op basis van de geboden informatie direct een overwogen keuze kunnen maken. Dat impliceert informatie over effecten van bepaald gedrag op content en diensten. De consument weet of aanbieder A of aanbieder B de betere keuze is gegeven het belang dat hij/zij aan bijvoorbeeld VoIP en P2P hecht. Met *feitelijk* bedoelen we dat wordt beschreven hoe internetverkeer verschillend wordt behandeld; met andere woorden informatie op het niveau van technische gedragingen. Dat zorgt er onder andere voor dat transparantie controleerbaar is.

Het is op het eerste gezicht een uitdaging deze laatste twee uitgangspunten te verenigen. Wordt een gegeven stuk informatie feitelijk gepresenteerd dan gaat dat snel ten koste van de begrijpelijkheid en andersom. Dat komt doordat de relatie tussen enerzijds technische

[60] Het gaat hier bijvoorbeeld over het blokkeren van kinderporno. ISP's geven aan dat het zeer omslachtig zou zijn al die gevallen te moeten melden. Het kan consumenten bovendien het idee geven uit eigen beweging bepaalde content blokkeert. Omdat alle ISP's verplicht zijn dezelfde blokkeringen door te voeren, is het wat ons betreft niet nodig dat iedere ISP hierover afzonderlijk rapporteert. Een generieke melding dat inhoud op basis van overheidsverplichtingen geblokkeerd kan zijn lijkt afdoende.

gedragingen en anderzijds de effecten van die gedragingen op content en diensten niet eenduidig is en bovendien aan verandering onderhevig (zie paragraaf 2.6).

Ook op Europees niveau lijkt men voor dit dilemma te staan, getuige de verschillen in de voorstellen van enerzijds het Europees Parlement en anderzijds de Raad van Telecomministers voor een transparantieverplichting in de universele-dienstenrichtlijn.[61] Het voorstel van de Raad van Telecomminsters lijkt feitelijkheid na te streven: *"… users should be fully informed of the traffic management policies of the service and/or network provider with which they conclude the contract."* [62] Het gaat dus om informatie over 'traffic management policies', een technische, feitelijke aangelegenheid. Het voorstel van het Europees Parlement, zet vooral in op begrijpelijkheid: *"… users should in any case be fully informed of any limitations imposed on the use of electronic communications services by the service and/or network provider. Such information should, at the option of the provider, specify the type of content, application or service concerned, individual applications or services, or both."* [63] Merk op dat de woorden 'content', 'application' en 'services' direct appelleren aan de belevingswereld van consumenten.

Onderstaand werken we begrijpelijke en feitelijke transparantie eerst uit in aparte formats. We doen vervolgens een voorstel voor het combineren van beide formats.

Begrijpelijke transparantie

Een voorbeeld van begrijpelijke transparantie is weergegeven in Tabel 2. Het is gebaseerd op een voorstel van de OECD[64] en ingevuld voor de Nederlandse aanbieders die P2P afknijpen in geval van congestie:

[61] We baseren ons op de voorstellen zoals die eruit zagen toen dit rapport werd geschreven. Het parlement en de raad zijn echter nog in discussie over de definitieve formulering dus het is goed mogelijk dat er nog andere voorstellen geopperd worden.

[62] Council Common Position van 16 februari 2009

[63] European Parliament Draft Recommendation van 27 februari 2009

[64] OECD (2007). *Internet traffic prioritisation: an overview*. http://www.oecd.org/dataoecd/43/63/38405781.pdf

Tabel 2: begrijpelijk format voor transparantie

Applicatie	Status
Web browsing	Open
Audio	Open
Video	Open
Peer2Peer	Beperkt
Gaming	Open
VoIP	Open
VPN	Open

Een dergelijk format lijkt ideaal; de consument ziet onmiddellijk dat deze ISP iets doet met P2P-verkeer. Tegelijk kent het formaat een aantal beperkingen:

- Het blijft onduidelijk wat er precies gebeurt en dat is problematisch bij applicaties die niet goed in de genoemde categorieën passen. Neem Skype, dat is in principe een VoIP-applicatie (wordt volledig doorgegeven) maar werkt via het P2P-protocol (wordt beperkt). Datzelfde geldt voor Joost, een videodienst (open) op basis van het P2P protcol (beperkt). Dit probleem is voor bestaande applicaties wellicht op te lossen, al gaat dat ten koste van de begrijpelijkheid. Maar er zullen steeds nieuwe internetapplicaties ontwikkeld worden waarvoor mogelijk iets soortgelijks geldt. Het format is dus niet toekomstvast.
- Het format maakt onvoldoende duidelijk in welke mate internetverkeer verschillend wordt behandeld, zowel in de diepte als in de breedte. In de diepte: is bijvoorbeeld P2P altijd geblokkeerd of wordt alleen in het geval van congestie op het netwerk (vaak tussen 17:00 en 21:00) de snelheid teruggeschroefd (of alle mogelijke tussenvormen)? Een consument die de hele dag downloads heeft lopen zal dat laatste niet zo'n probleem vinden; een consument die juist na het eten met buitenlandse vrienden wilt Skypen wel. In de breedte: het is goed mogelijk dat ISP's bepaalde webpagina's blokkeren maar bovenstaand format maakt geen verschil tussen het beperken van één webpagina en het beperken van honderd webpagina's. Het is goed mogelijk dat bovenstaand format alle ISP's dwingt bij *web browsing* 'restricted' in te vullen. Opnieuw: hier is mogelijk een mouw aan te passen, maar dat gaat ten koste van de begrijpelijkheid.

Feitelijke transparantie

Een feitelijk format is vanzelfsprekend gedetailleerder dan een begrijpelijk format. Het zou in ieder geval de volgende soorten gegevens moeten bevatten:

- *Wat voor soort restrictie wordt er toegepast?*
  - volledige blokkade;
  - bepaalde bovengrens aan snelheid (*cappen*);
  - pakketten droppen;
  - TCP reset.

- *Onder welke omstandigheden?*
  - altijd;
  - op bepaalde vaste periodes;
  - in geval van netwerkcongestie.
- *Op basis van welke verkeerskenmerken?*
  - header IP-pakket (bron, bestemming, protocol, …);
  - inhoud IP-pakket (middels *Deep Packet Inspection*);
  - traffic flow

Tabel 3: feitelijk format voor transparantie

Wat is de restrictie?	Onder welke omstandigheden?	Op basis van welke verkeerskenmerken?
volledig blokkeren	altijd	poort 135 t/m 139
cappen	van 17u tot 21u	P2P-verkeer o.b.v. header-informatie, gebruikte poorten en aantal simultane verbindingen

In Tabel 3 is een voorbeeld opgenomen van een feitelijk format. Ook bij dit format kunnen we enkele beperkingen noteren:

- De gepresenteerde informatie is voor de gemiddelde consument waarschijnlijk niet erg begrijpelijk. Dat hoeft geen probleem te zijn. Eerder in dit hoofdstuk noemden we al indirecte transparantie: de consument maakt een keuze op basis van 'een vertaling' door de internet community, consumentenorganisaties of de pers. Dat veronderstelt dan wel dat er de consument door de community wordt bereikt – wat nog meer zeer de vraag is in de huidige situatie.[65]
- ISP's gebruiken mogelijk zeer complexe en wisselende protocollen voor het verschillend behandelen van internetverkeer. Het invullen en voortdurend updaten van een gedetailleerd format zou dan aanzienlijke kosten met zich mee kunnen brengen. Volgens sommige respondenten is dat overigens juist een voordeel: je ontmoedigt daarmee het verregaand verschillend behandelen van internetverkeer. De (fundamentele) vraag is of dat laatste wel een doel op zich moet zijn. Zoals eerder in dit rapport beschreven bestaat er geen consensus dat het verschillend behandelen van internetverkeer in alle gevallen verkeerd is. In dat geval benadeelt het bovenstaande format ISP's die internetverkeer nauwkeurig proberen te behandelen (met als gevolg complexe protocollen) ten opzichte van ISP's die verkeer op een 'lompe' manier verschillend behandelen.

Een combinatie van begrijpelijke transparantie en feitelijke transparantie

Door beide formats te combineren komen we tot een voorstel wat de meeste beperkingen van beide formats mitigeert. ISP's zouden daarbij (1) feitelijke informatie moeten

[65] Een probleem is bovendien dat bepaalde partijen de vertaling naar de gemiddelde consument mogelijk willen beïnvloeden. Het is van belang dat dit voldoende neutraal gebeurt.

presenteren zoals voorgesteld in het tweede format en (2) kort moeten uitleggen wat de effecten zijn van deze gedragingen op de voor de gebruikers belangrijkste categorieën content, diensten en toepassingen.

4.4.2 Rol van de overheid

In haar afwegingskader transparantie stelt het Ministerie van Economische Zaken zich vervolgens de vraag in hoeverre er een rol voor de overheid is bij het vergroten van transparantie. Grotere transparantie – aldus het Ministerie van Economische Zaken - kan tot stand komen door zelfregulering, door stimulering van marktpartijen door de overheid, door actieve informatievoorziening door de overheid en door regelgeving. In dit geval is de keuze in feite al gemaakt: in de universele-dienstenrichtlijn komt een transparantieverplichting en deze zal – meer of minder letterlijk – in de Nederlandse Telecomwet worden getransponeerd.

Dat betekent natuurlijk niet dat het Ministerie van Economische Zaken helemaal geen rol heeft in de discussie over transparantie. Interviews met verschillende ISP's laten zien dat ze niet staan te springen om een transparantieverplichting (hoewel ze zich wel bereid tonen de verplichting na te leven als die er komt). Dat beeld werd in de latere workshop alleen maar bevestigd. Dat zou er voor pleiten ISP's ter zijner tijd actief te betrekken bij de exacte invulling van transparantie. Bij die discussie zouden verschillende vragen een rol moeten spelen. Afhankelijk van de medewerking van de ISP's: hoeveel vrijheid geeft het format? Verschillende ISP's geven aan weinig te zien in zeer stringent format. Als er al een transparantieverplichting komt willen zij de vrijheid hebben zelf aan te sluiten bij de behoeften van hun klanten. Een andere belangrijke vraag is hoe effectief en toekomstvast het format is en wat de neveneffecten zijn van transparantie (zie volgende paragraaf).

Tenslotte is een belangrijke vraag in hoeverre te controleren is of de verplichting tot transparantie daadwerkelijk wordt nageleefd. Dit brengt ons op de tweede rol van de overheid: die van toezichthouder. Dat veronderstelt een norm die te controleren is. In dit geval gaat het om de vraag of een ISP wel voldoende openheid van zaken heeft gegeven over het verschillend behandelen van internetverkeer. Dat is, zoals hiervoor is betoogd, echter geen eenvoudige kwestie. Uit de effecten (verminderde snelheid en/of kwaliteit, zie 2.5) kunnen niet direct de gedragingen worden afgeleid. Een vermindering van kwaliteit *zou* door een bepaalde bewuste gedraging van de ISP in kwestie kunnen worden veroorzaakt maar dat hoeft niet het geval te zijn. Anders dan bij transparantie over prijzen is dus niet zondermeer duidelijk of een ISP ook doet wat vermeld staat.

De volgende praktische afwegingen zijn kortom van belang voor wat betreft controleerbaarheid:

- Het Ministerie van Economische Zaken (of een andere overheidspartij) moet zorgen dat eindgebruikers of aanbieders van content of diensten ergens terecht kunnen met klachten ("ISP A geeft aan alleen P2P-verkeer te hinderen maar ook mijn VoIP-dienst hapert"). Het kan ook zijn dat mensen zich voornamelijk tot bestaande fora wenden, bijvoorbeeld tweakers.nl en in dat geval moeten ook dergelijke worden gemonitord. Daarbij speelt wel de vraag of de klagers wel volledig onafhankelijk zijn.
- Bij aanhoudende klachten over een bepaalde ISP moet een onderzoek kunnen worden ingesteld naar de activiteiten van die ISP. Daarbij geldt dat feitelijke transparantie zo'n onderzoek gemakkelijker maakt dan begrijpelijke transparantie. Als duidelijk beschreven staat hoe een ISP verkeer verschillend behandeld is relatief makkelijk te checken of dat ook gebeurt. Als alleen beschreven staat dat P2P-

verkeer gehinderd wordt is het zoeken naar een speld in een hooiberg. Helemaal omdat Europese (niet zozeer Nederlandse!) ervaring leert dat een aantal ISP's bewust probeert het verschillend behandelen van internetverkeer onzichtbaar te houden.

- Het Ministerie van Economische Zaken moet zich afvragen in hoeverre de expertise die nodig is om klachten te beoordelen en zonodig een onderzoek uit te voeren, binnen haar organisatie aanwezig is of waar die extern gehaald kan worden. Zonder een goede mogelijkheid klachten in te dienen en naar aanleiding daarvan onderzoek in te stellen is een transparantieverplichting een lege huls.

4.4.3 Neveneffecten van transparantie

Tot slot rest de vraag wat de neveneffecten van transparantie zullen zijn. De baten zijn al eerder aan bod gekomen en in onze optiek prevaleren de positieve effecten boven de neveneffecten. Bij het ontwikkelen van beleid moeten echter ook eventuele minder positieve effecten worden overwogen en deze komen in deze paragraaf aan bod.

Het bieden van transparantie zal allereerst kosten met zich mee zal brengen. Die kosten liggen om te beginnen bij de ISP. Het inzichtelijk maken en houden van het beleid van de ISP ten aanzien van het verschillend behandelen van internetverkeer kost tijd en geld. Over de hoogte van die kosten lopen de meningen overigens sterk uiteen. Naast de ISP maakt het Ministerie van Economische Zaken zelf ook kosten. Dat zijn de kosten die voortkomen uit het monitoren van eventuele klachten over gebrekkige transparantie (zowel reactief als pro-actief; op discussiefora, blogs, websites, et cetera) en uit het uitvoeren van handhavingsactiviteiten die naar aanleiding van de klachten eventueel moeten worden ondernomen. Zowel de kosten voor ISP's als de kosten voor het Ministerie van Economische Zaken hangen overigens af van de precieze invulling voor transparantie die gekozen wordt. Waarschijnlijk is feitelijkere transparantie duurder voor de ISP maar vergemakkelijkt het eventueel ingrijpen van het Ministerie van Economische Zaken en vice versa.

Verschillende respondenten wijzen daarnaast op het risico van schijnzekerheid. De transparantieverplichting blijft vooralsnog beperkt tot het verschillend behandelen van internetverkeer. Over andere zaken – die wellicht veel meer invloed hebben op de prestaties van iemands internetverbinding – is men niet verplicht informatie te bieden. Een consument die op basis van informatie aangaande netwerkneutraliteit een bepaalde ISP kiest is dus niet altijd verzekerd van een verbinding die het beste bij zijn/haar eisen past. Overigens menen evenzoveel respondenten dat dat geen argument kan zijn om van transparantie over het verschillend behandelen van internetverkeer af te zien. Het is eerder een argument voor het uitbreiden van de transparantieverplichting. Schijnzekerheid kan volgens één respondent ook ontstaan doordat de overheid onvoldoende in staat is transparantie te controleren op volledigheid en juistheid. Ook in de literatuur wordt van een dergelijke 'toezichtillusie' gesproken.[66] Door partijen nadrukkijker aan te laten geven wat precies het bereik van de hier besproken transparantie is en dat deze verder niets zegt over andere productkenmerken die ook belangrijk kunnen zijn, kan dit nadeel deels ondervangen worden.

[66] Odlyzko (2009). *Network neutrality, search neutrality, and the never-ending conflict between efficiency and fairness in markets*. http://www.rnejournal.com/artman2/uploads/1/odlyzko_RNE_mar09.pdf

Een derde mogelijk neveneffect is dat van strategisch gedrag van derden. Als content- en dienstenaanbieders precieze informatie hebben over blokkeringen en traffic mangement policies, kunnen ze daarom anticiperen en zo proberen te omzeilen. Overigens zullen de voorstanders van een volledig neutraal internet dat eerder als een voordeel beschouwen. Maar we merken opnieuw op dat er geen consensus bestaat over het feit dat het verschillend behandelen van internetverkeer in *alle* gevallen verkeerd is. Ook in die gevallen dat het verschillend behandelen van internetverkeer mogelijk voordelig is (afknijpen van 'asociaal' P2P-verkeer ten gunste van andere soorten verkeer – even los van de discussie of het überhaupt mogelijk is om dat specifieke verkeer eruit te pikken) kan de beperking omzeild worden. De vraag is overigens of content- en dienstenaanbieders eventuele blokkeringen nu niet ook al weten te omzeilen. Uit gesprekken blijkt immers dat content- en dienstenaanbieders vaak al heel goed weten wat voor blokkeringen er van kracht zijn.

Strategisch gedrag kan daarnaast van de ISP's uitgaan. Die ISP's die volledig en eerlijk zijn over het verschillend behandelen van internetverkeer ondervinden mogelijk een concurrentienadeel ten opzichte van de ISP's die deze informatie minder compleet of juist weergeven. Bij een flexibel format zijn deze risico's groter dan bij een strak vastgelegd format.

4.5 Conclusie

In deze afsluitende paragraaf vatten we de belangrijkste uitkomsten van het hoofdstuk samen.

De rationale achter transparantie

Vergeleken met direct ingrijpen (het stellen van eisen aan de afwikkeling aan verkeer) biedt de beleidsrichting van transparantie verschillende voordelen. Binnen een verder goed functionerende markt zal transparantie naar verwachting bijdragen aan een maatschappelijk gunstige mix van prijs- en productdifferentiatie, en de juiste verhouding tussen prijs en 'openheid'. De gevolgen voor investeringen en innovatie (met onderscheid voor innovatie 'binnen' de netwerken en innovatie in de periferie) zijn minder gemakkelijk te voorspellen, maar de verwachting is dat eventuele negatieve gevolgen minder groot zijn dat in het scenario van hard ingrijpen (zie paragraaf 4.2.1 voor details). In Nederland wordt in grote mate voldaan aan de randvoorwaarden voor transparantie (waaronder een concurrerende markt). Ook is het inzetten op transparantie in lijn met verwacht beleid van de Europese Commissie.

Hoe transparant zijn marktpartijen over netwerkneutraliteit en hun eventuele ingrepen daarin?

Transparantie werkt op verschillende manieren – direct of indirect – en kan invloed hebben op het gedrag van verschillende partijen – de consument of de ISP. *Directe* transparantie is duidelijk voor verbetering vatbaar: er zijn gevallen waarin de consument te maken krijgt met het verschillend behandelen van internetverkeer terwijl ze daar door de ISP niet van op de hoogte wordt gesteld. Die gevallen zijn vaak wél bekend bij de professionele partijen, in dat opzicht werkt indirecte transparantie beter. In hoeverre het (overstap)gedrag van consumenten ook beïnvloed wordt door de opinie van de professionals valt echter nog te bezien. Consumenten lijken toch vooral af te gaan op de (in bepaalde gevallen gebrekkige of onvolledige) informatie die hen door ISP's wordt aangeboden. In Nederland blijken ISP's wél gevoelig te zijn voor de opinie van de internet community. Een aantal ISP's geeft aan niet aan het verschillend behandelen van internetverkeer te doen uit angst voor negatieve reacties vanuit de community.

Hoe kan het vergroten van transparantie het beste worden vormgegeven?

Voor de reikwijdte van de transparantie stellen we de volgende uitgangspunten voor:

- De verplichting geldt zowel voor de aanbieders van *vaste* als van *mobiele* ISP-diensten en in beide gevallen zowel voor de *residential* als voor de *zakelijke* markt.
- De verplichting strekt zich uit tot de *gehele keten* die de ISP verzorgt, dus van het interconnectiepunt met andere ISP's tot aan het afleverpunt bij de eindgebruiker.
- De verplichting strekt zich niet uit tot diensten die niet via het *openbare* internet verlopen (zoals een IP-TV dienst die door de ISP zelf wordt aangeboden).
- De verplichting geldt ook niet voor de *generieke* behandeling van internetverkeer (zoals overboeking – er is immers geen sprake van het verschillend behandelen van verschillende typen verkeer).
- Tenslotte geldt de verplichting ook niet voor het verschillend behandelen van internetverkeer dat in opdracht van de overheid plaatsvindt, zoals het blokkeren van internetsites waar strafbare content op staat.

Een belangrijke afweging daarnaast is die tussen begrijpelijke en feitelijke transparantie. Bij begrijpelijke transparantie wordt informatie gegeven over de effecten van bepaald gedrag op content en diensten. Bij feitelijke transparantie wordt op technisch niveau beschreven hoe en in welke mate internetverkeer verschillend wordt behandeld. Beide aspecten zijn niet goed in één format te vangen en daarom stellen we een combinatie voor: ISP's zouden daarbij (1) feitelijk en op een verifieerbare wijze moeten presenteren in hoeverre ze internetverkeer verschillend behandelen en (2) (potentiële) klanten moeten uitleggen wat de effecten zijn van deze gedragingen op de voor de gebruikers belangrijkste categorieën content, diensten en toepassingen.

Welke rol heeft de overheid bij het vergroten van transparantie?

Of er een transparantieverplichting komt en hoe die er – op hoofdlijnen – uit zal zien wordt hoogstwaarschijnlijk op Europees niveau besloten. Voor de preciezere invulling van de transparantieverplichting – een rol van het Ministerie van Economische Zaken – geven we in dit rapport verschillende aanwijzingen. Het is goed de betrokken partijen (ISP's) daarbij nauw te betrekken omdat dat het draagvlak voor een transparantieverplichting kan vergroten; dat is nu nog vrij laag.

Handhaving van de verplichting (of het laten uitvoeren daarvan) is de tweede belangrijke rol van het Ministerie van Economische Zaken. Om deze rol goed vorm te geven is het mede van belang dat het de transparantieverplichting ook feitelijke en verifieerbare (technische) gegevens bevat.

Wat zijn de eventuele kosten en nadelen van het vergroten van transparantie?

Het vergroten van transparantie brengt kosten met zich mee en in de strikte zin van het woord is het daarmee geen *no regret* optie. Die kosten komen deels voor rekening van de ISP's (voor het beschikbaar maken en up-to-date houden van informatie) en deels voor rekening van het Ministerie van Economische Zaken (voor het bieden van een kanaal voor eventuele klachten en mogelijke acties die daarop volgen). Mogelijke niet-monetaire effecten zijn daarnaast schijnveiligheid bij de consument en strategisch gedrag van aanbieders van diensten en content en van ISP's. Wij verwachten echter dat deze verschillende kosten niet opwegen tegen de baten van transparantie.

5 Toekomstige marktsituatie

5.1 Inleiding

Om nieuw beleid zo goed mogelijk vorm te geven, is het noodzakelijk om inzicht te krijgen in de toekomstige marktsituatie. Beleid moet immers niet alleen aansluiten bij de zaken die op dit moment spelen maar moet ook voldoende ruimte bieden om om te kunnen gaan met toekomstige ontwikkelingen. Dit speelt zeker in een dynamische markt als de telecom-markt waarin de ontwikkelingen elkaar snel opvolgen. Na een globale schets van de toekomstige marktsituatie (paragraaf 5.2) beschrijven we hoe de overheid de vinger aan de pols kan houden bij de ontwikkelingen in de markt (paragraaf 5.3).[67] Paragraaf 5.4 presenteert de conclusies.

5.2 Mogelijke ontwikkelingen

Op basis van desk research en interviews zijn verschillende mogelijke ontwikkelingen geïdentificeerd. We behandelen hier de ontwikkelingen waarvan een reële kans bestaat dat deze zich voordoen én die impact kunnen hebben op het verschillend behandelen van internetverkeer. De ontwikkelingen zijn in twee clusters te verdelen: *infrastructuur* en *diensten.*

5.2.1 Infrastructuur

Op het niveau van de infrastructuur zijn tenminste vier relevante ontwikkelingen te noemen. Twee daarvan hebben betrekking op het vaste netwerk, twee op het mobiele netwerk. We bespreken de vier ontwikkelingen hieronder.

Implementatie nieuwe technieken voor vast internet (1)

De implementatie van nieuwe technieken voor vast internet zorgt ervoor dat veel bedrijven en huishoudens een surplus aan bandbreedte krijgen. Hierdoor verdwijnt een prikkel bij aanbieder om verkeer verschillend te behandelen – tenminste, indien die overweging ingegeven was door capaciteitsvraagstukken (zie paragraaf 2.3). De nieuwe technieken die ingezet worden zijn EuroDocsis 3.0, VDSL en glasvezel. Ten opzichte van de huidige kabel- en xDSL-aansluitingen bieden deze technologieën veel meer bandbreedte aan de eindgebruiker. Het 'schaarsteargument' is op deze netwerken dus niet (of nauwelijks) meer van toepassing.

Steeds meer zakelijke en residentiële gebruikers krijgen de beschikking over een glasvezelaansluiting. In Amsterdam worden er honderdduizenden huishoudens aangesloten, maar ook Deventer, Rotterdam en veel andere gemeenten en wijken volgen.[68] Op de zakelijke markt vinden er grote initiatieven plaats die honderden bedrijven aansluiten op glasvezel. Voorbeelden zijn Wij-Zijn-Breed, BreedNet, Fryslânring en NDIX[69].

---

[67] Overigens is het belangrijk om te beseffen dat we niet meer dan een beeld kunnen schetsen van mogelijke ontwikkelingen. In de woorden van Niels Bohr: "Prediction is very difficult, especially about the future."

[68] Zie http://www.glasvezelamsterdam.nl, http://www.glashart.nl/deventer/ en http://www.glasvezelrotterdam.nl/

[69] http://www.wij-zijn-breed.nl/, http://www.breednet.nl/, http://www.fryslanring.nl/ en http://www.ndix.net/

Maar ook de uitrol van EuroDocsis 3.0 krijgt steeds meer vorm. Zo biedt UPC onder de naam FiberPower dit product al op een aantal plaatsen aan.[70]

Onderdimensionering in netwerken voor vast internet (2)

Onderdimensionering in bepaalde netwerken voor vast internet kan leiden tot een schaarste aan bandbreedte op deze netwerken. Een netwerk waarin weinig geïnvesteerd is zal een lagere capaciteit kennen. Indien het capaciteitsplafond is bereikt, moet er een keuze gemaakt worden: Welke pakketten vervallen? Zoals bekend is zet dit een deur open tot het maken van onwillekeurige keuzes en dus het actief verschillend behandelen van internetverkeer. Van onderdimensionering op vaste netten kan sprake zijn als de markt zeer prijsgevoelig is. Er kan zich een ontwikkeling voordoen waarbij een substantieel deel van de markt simpelweg het goedkoopste internetabonnement wil. Een ISP die haar netwerk onderdimensioneert heeft lagere kosten en kan deze klanten op een economisch meer aantrekkelijke manier bedienen. (Deze ontwikkeling is te vergelijken met die van de 'budgetsupermarkten' waar alle producten nog in de dozen staan.) De gebruikers van deze netwerken zullen ervaren dat het netwerk trager wordt tijdens piekuren.

Feitelijk is dit niets anders dan een uiting van een verregaande mate van differentiatie en specialisatie in de markt. De uitruil tussen een vermindering in snelheid en/of kwaliteit tegen lagere kosten is een bewuste keuze van de eindgebruikers. Vanuit macro-economisch oogpunt leidt dit soort diversificatie van het aanbod tot een verbetering van het sociale optimum. Bepaalde groepen gebruikers krijgen toegang tot het internet die dat anders niet hadden gekregen. In het specifieke geval van het internet vormt de hoge mate van afhankelijkheid tussen ISP's wel voor complicaties. Eén ISP die onderdimensioneert kan bij veel andere ISP's tot verkeersproblemen leiden. In het meest radicale geval gaan high-end ISP's ertoe over om zich af te scheiden van het publieke internet waarvan de kwaliteit immers steeds minder goed is te garanderen.

Overigens zijn ontwikkeling (1) en ontwikkeling (2) niet exclusief, het is mogelijk dat ISP's nieuwe technologieën implementeren in de last mile (om klanten te trekken) maar intussen investeringen in de backbone verwaarlozen. De (maximale) prestaties van de local loop technieken zijn immers beter zichtbaar voor de klant dan de prestaties van de backbone.[71]

Toename gebruik mobiel internet (3)

Omdat het gebruik van mobiel internet sterk groeit, zullen steeds meer eindgebruikers de beperkingen van een niet-neutraal netwerk ervaren. Immers, veel abonnementen op mobiel internet leggen beperkingen op aan het type verkeer dat de eindgebruiker kan verzenden en ontvangen. Vaak is bijvoorbeeld het gebruik van VoIP of P2P niet mogelijk.

Het gebruik van mobiel internet groeit sterk. Dit wordt bevestigd door verschillende aanbieders. Zo geeft KPN aan dat de omzet uit mobiele diensten in 2008 met de helft toenam[72] en zag T-Mobile de omzet hieruit in 2008 met bijna 30% groeien[73]. In 2008 heeft het Ministerie van Economische Zaken heeft onderzoeken laten uitvoeren naar de

---

[70] Tweakers (2008). *UPC breidt gebied met 120Mbps-internet sterk uit*. http://tweakers.net/nieuws/57304/upc-breidt-gebied-met-120mbps-internet-sterk-uit.html

[71] Bij de overgang van ADSL naar ADSL2+ bijvoorbeeld was het voor klanten goed zichtbaar dat de maximale snelheid van de aangeboden producten van 8 Mbps naar ruim 20 Mbps steeg.

[72] Webwereld (2009). *KPN presenteert sterke cijfers ondanks crisis*. http://new.webwereld.nl/nieuws/54615/kpn-presenteert-sterke-cijfers-ondanks-crisis.html

[73] Emerce (2008). *Mobiel internet T-Mobile stijgt explosief*. http://www.emerce.nl/nieuws.jsp?id=2764008

consumentenbehoefte van mobiele breedbanddiensten.[74] Hieruit kwam naar voren dat mobiel internet een onvermijdelijke ontwikkeling is.

Veel aanbieders van mobiel internet kiezen ervoor om data-intensief verkeer te hinderen. Ten opzichte van vaste netwerken, zijn de kosten voor het verzenden van een bit op een mobiel netwerk relatief hoog. Dit komt onder andere door licenties voor frequentiebanden, kostbare infrastructuur met een kortere afschrijving en fysieke beperkingen in bandbreedte van het mobiele kanaal. Door verkeer te manipuleren is het mogelijk om voor beperkte kosten een grote groep gebruikers tevreden te stellen, maar dit gedrag kan ook ingegeven zijn door de wens om inkomsten door traditionele diensten in stand te houden door bijvoorbeeld VoIP verkeer te hinderen.

Implementatie nieuwe technieken voor mobiel internet (4)

Nieuwe mobiele technieken kunnen een prikkel wegnemen bij ISP's om principes van netwerkneutraliteit te schenden. Deze ontwikkeling staat dus haaks op de vorige trend. Vierde generatie netwerken zullen ervoor zorgen dat er meer verkeer vervoerd kan worden. Bandbreedte wordt minder schaars en de kosten per verzonden bit dalen. De vraag is echter of de groei in vraag naar bandbreedte (nieuwe mobiele applicaties) het groei in aanbod (vierde generatie netwerken) niet zal overtreffen. Meer aanbod schept over het algemeen meer vraag. Daar komt nog bij dat de grootschalige uitrol van vierde generatie netwerken waarschijnlijk nog enkele jaren op zich zal wachten, al is het alleen maar omdat de vorige generatie netwerken nog niet zijn afgeschreven (zie hiervoor).

5.2.2 Diensten

Ook op het niveau van de diensten kan er een algehele technologische vooruitgang worden verondersteld. Die zal zich in dit geval met name aan de kant van de eindgebruikers voordoen. We bespreken hier drie van dergelijke ontwikkelingen: het beschikbaar komen van betere diensten waarmee eindgebruikers hun verbinding kunnen doormeten, de opkomst van diensten die het business model van ISP's ondermijnen en de opkomst van diensten waarvoor dienstenaanbieders of eindgebruikers additioneel gaat betalen aan de ISP.

Beschikbaar komen van betere diensten waarmee eindgebruikers hun verbinding kunnen doormeten (5)

Er komen steeds meer eenvoudige applicaties waarmee gebruikers hun verbinding kunnen doormeten en dus hun ISP kunnen controleren. ISP's die niet open of niet eerlijk zijn in hun beleid aangaande netwerkneutraliteit kunnen hiervan effecten ondervinden. De transparantie in de markt zal immers verhoogd worden. Hierdoor kunnen klanten een meer weloverwogen beslissing nemen. Alleen in markten waar (te) weinig concurrentie is, zal dit effect uitblijven.

Er zijn in het verleden verschillende diensten verschenen die het voor de eindgebruiker mogelijk maakten om zijn ISP te controleren op schendingen van principes van Netwerkneutraliteit. Zo is er een plug-in van de bittorrent client Azureus (Vuze) die dit probeert te bewerkstelligen.[75] Deze tool meet echter vooral vrij rudimentaire methoden,

---

[74] Senster & De Kort (2007).*Consumentenbehoeften Mobiele communicatie*. http://www.ez.nl/dsresource?objectid=154504&type=PDF

[75] http://azureus.sourceforge.net/plugin_details.php?plugin=aznetmon

zoals de TCP reset die voor in de VS gebruikt werd om P2P-verkeer te ontregelen.[76] In 2008 werd ook het programma Switzerland van EFF gelanceerd. Dit programma kent meer functionaliteiten, maar is vrij complex en niet geschikt voor het grote publiek. Onlangs is er echter een aantal applicaties op de markt gekomen (waaronder met name M-Lab van Google) die de gedragingen van ISP's voor breed publiek ontsluiten.

Opkomst van diensten die business model van ISP's ondermijnen (6)

Een ISP die haar business model ondermijnd ziet worden door de opkomst van nieuwe diensten, heeft een prikkel om deze diensten te hinderen. Zij kan de controle over haar netwerk gebruiken om dit te bewerkstelligen. Dit probleem zal uitsluitend spelen bij ISP's die ook inkomsten genereren uit traditionele diensten. Voorbeelden hiervan zijn de 'kabelaars' (televisiebeelden), mobiele operators (sms en bellen) en aanbieders van vaste telefonie.

De afgelopen jaren zijn er steeds meer diensten op de markt gekomen die – althans in potentie – de huidige business models van ISP's sterk ondermijnen. Voorbeelden zijn VoIP, SMS via websites en via messenger applicaties, internet-TV en het downloaden van films en series. De kwaliteit van deze diensten neemt voortdurend toe. Ze worden steeds meer volwaardige alternatieven voor de duurdere traditionele diensten.

Het conflict in het business model wordt veroorzaakt doordat voor verschillende diensten verschillende kosten per verzonden bit in rekening worden gebracht. Op basis van verwachtingen van het gebruik van verschillende diensten, stellen aanbieders hun business case op. Wanneer afnemers grootschalig de goedkope diensten gebruiken om de dure diensten te ontwijken, ontstaat er een conflict. Odlyzko geeft een aardig (weliswaar gestileerd) voorbeeld van kostendifferentiatie van verschillende telecommunicatiedien-sten.[77] Hierbij moet wel worden aangetekend dat niet alle diensten substituten voor elkaar vormen.

Tabel 4: Geschatte omzet per megabyte voor verschillende diensten

Dienst	omzet per MB
wireless texting	$1000
wireless voice	$1,00
wireline voice	$0,10
residential Internet	$0,01
backbone Internet	$0,0001

Om haar inkomsten te beschermen zal een ISP vaak proberen om eindgebruikers zo hoog mogelijk in de keten te houden. Om dit te realiseren kan zij bijvoorbeeld de controle die zij heeft over end-user devices, zoals mobiele telefoons, inzetten. Zo is het soms niet mogelijk om op een iPhone via een mobiel data-abonnement te bellen. Uiteraard kan dit proces ook op een subtielere manier worden vormgegeven, zoals een bepaald type verkeer prioriteit

[76] Eckersley et al. (2007). *Packet Forgery By ISPs: A Report On The Comcast Affair*. http://www.eff.org/files/eff_comcast_report2.pdf

[77] Odlyzko (2009). *Network neutrality, search neutrality, and the never-ending conflict between efficiency and fairness in markets*. http://www.rnejournal.com/artman2/uploads/1/odlyzko_RNE_mar09.pdf

geven, of een goedkoper alternatief afremmen (bijvoorbeeld P2P-verkeer 'vergiftigen' met TCP-resets).

Opkomst van veeleisende diensten waarvoor dienstenaanbieder of eindgebruiker additioneel gaat betalen aan de ISP (7)

Een toenemende vraag naar steeds hoogwaardigere diensten kan ertoe leiden dat eindgebruikers – en dus indirect dienstenaanbieders – geld over hebben voor een *gereserveerd kanaal*. In dit gereserveerde kanaal gelden hogere kwaliteitseisen en kan de dienst beter worden aangeboden. ISP's laten zich betalen om dit kanaal op te zetten. Een gevolg hiervan is dat een bepaald type verkeer voorrang krijgt boven ander verkeer. Het verkeer wordt dus niet gelijk behandeld.

De laatste jaren komen er steeds meer diensten op die zeer hoge kwaliteitseisen stellen aan de verbinding. Denk aan (beeld)telefonie, online gaming en televisiediensten. Bij dit soort diensten zijn problemen rond de snelheid en/of kwaliteit van het verkeer meteen merkbaar voor de gebruiker en kunnen de gevolgen als zeer negatief worden ervaren. Gesprekspartners zijn niet of nauwelijks te verstaan, cruciale doelpunten worden gemist en virtuele zwaardgevechten kansloos verloren. Tijdens de interviews is naar voren gekomen dat sommige dienstenaanbieders best willen betalen voor dit soort additionele dienstverlening van een ISP. Het idee is dat ze hun klanten dan (veel) beter kunnen bedienen.

Tabel 5: Overzicht van ontwikkelingen en hun effect

Ontwikkeling	**Mogelijk effect op netwerkneutraliteit ("+":positief effect; "-" negatief effect)**
INFRASTRUCTUUR	
1. Implementatie nieuwe technieken voor vast internet	Minder prikkels bij ISP's om soorten verkeer te blokken of prioriteren (+)
2. Onderdimensionering in netwerken voor vast internet	Mogelijkheid dat groep gebruikers (indirect) kiest voor geprioriteerd verkeer (–)
3. Toename gebruik mobiel internet	Toename aantal gebruikers die met blokken en prioriteren van soorten verkeer geconfronteerd worden (–)
4. Implementatie nieuwe technieken voor mobiel internet	Minder prikkels bij ISP's om soorten verkeer te blokken of prioriteren (+)
DIENSTEN	
5. Beschikbaar komen van diensten waarmee eindgebruikers hun verbinding kunnen doormeten	Meer transparantie over blokken of prioriteren van soorten verkeer (+)
6. Opkomst van diensten die business model van ISP's ondermijnen	Meer prikkels bij ISP's om soorten verkeer te blokken of prioriteren (–)
7. Opkomst van veeleisende diensten waarvoor dienstenaanbieder of eindgebruiker additioneel gaat betalen aan de ISP	Meer vraag bij dienstenaanbieders en afnemers naar geprioriteerd verkeer (–)

Een aantal van de ontwikkelingen dat hierboven is geschetst zal waarschijnlijk leiden tot een toename van het verschillend behandelen van internetverkeer en een aantal tot een afname. Tabel 5 geeft een overzicht van de verwachte richting van de trends.

Of er sprake is van een *netto* toe- of afname hangt niet alleen van de optelsom van de positieve en negatieve trends af, maar ook van de individuele gewichten van de trends en van de waarschijnlijkheid dat ze op zullen treden. In Tabel 6 zijn de gewichten en kansen weergegeven. Over alle trends heen speelt de mate van concurrentie op de markt voor internettoegang een grote rol. Wij zijn er in dit hoofdstuk van uitgegaan dat de Nederlandse telecommunicatiemarkt net zo competitief blijft als deze nu is. Een hoge mate van concurrentie tussen ISP's zorgt ervoor dat hun aanbod goed aansluit bij de marktvraag. Ongewenst strategisch gedrag, zoals het blokkeren van bepaalde diensten, wordt dan onmiddellijk door de markt afgestraft. Indien de competitie in de markt echter sterk zou afnemen, kunnen de problemen met netwerkneutraliteit groter worden. Dit is geen ontwikkeling die we op de korte tot middenlange termijn voorzien.

Tabel 6: De termijn, waarschijnlijkheid en mate van impact van de geschetste ontwikkelingen

Ontwikkeling	Termijn	Waarschijnlijk-heid	Positieve impact ("+":positief effect; "-" negatief effect)
1. Implementatie nieuwe technieken voor vast internet	Zeer lang	Groot	Klein (+)
2. Onderdimensionering in netwerken voor vast internet	Kort	Middel	Klein (-)
3. Toename gebruik mobiel internet	Kort	Zeer groot	Groot (-)
4. Implementatie nieuwe technieken voor mobiel internet	Zeer lang	Zeer groot	Middel (+)
5. Beschikbaar komen van diensten waarmee eindgebruikers hun verbinding kunnen doormeten	Kort	Zeer groot	Middel (+)
6. Opkomst van diensten die business model van ISP's ondermijnen	Kort	Zeer groot	Middel – groot (-)
7. Opkomst van veeleisende diensten waarvoor dienstenaanbieder of eindgebruiker additioneel gaat betalen aan de ISP	Kort	Middel	Klein (-)

5.3 Monitoren van toekomstige ontwikkelingen door de overheid

In deze paragraaf wordt beschreven hoe het Ministerie van Economische Zaken het beste de ontwikkelingen kan volgen. We beperken ons daarbij tot het uitwerkingen van de trends uit Tabel 6 die zich op korte termijn met betrekkelijk grote waarschijnlijkheid zullen voordoen en een grote mate van impact zullen hebben.

Toename gebruik mobiel internet (3)

Zoals reeds aangegeven kennen mobiele netwerken meer capaciteitsbeperkingen, terwijl de vraag naar capaciteit (met name door mobiel internet) sterk toeneemt. De overheid kan – in generieke zin – de groei van de vraag bijhouden door op de hoogte te blijven van de diverse marktonderzoeken en andere bronnen op dat gebied. Nog belangrijker is een

vinger aan de pols te houden in hoeverre gebruikers – ook via weblogs en expert websites – zeggen last te ondervinden van het verschillend behandelen van verkeer.

Opkomst van diensten die business model van ISP's ondermijnen (6)

Inzicht in deze ontwikkeling kan gekregen worden door op gezette tijden na te gaan wat de status is omtrent de introductie, beschikbaarheid en gebruik van dergelijke nieuwe, concurrerende diensten (denk aan Skype voor mobiele telefoons). Het is daarbij leerzaam deze ontwikkelingen te vergelijken met die uit het buitenland.

Zoals bij het vorige punt, is het goed de vinger aan de pols te houden in hoeverre gebruikers – ook via weblogs en expertwebsites – zeggen last te ondervinden van het gebruik van deze nieuwe toepassingen.

Beschikbaar komen van diensten waarmee eindgebruikers hun verbinding kunnen doormeten (5)

In tegenstelling tot de bovenstaande ontwikkelingen is dit een positieve ontwikkeling. De opkomst van toegankelijke meetinstrumenten die door een breed publiek kunnen worden gebruikt betekent een aanzienlijke versterking van de directe transparantie (zie paragraaf 4.3.1). In feite fungeren de eindgebruikers als de 'ogen en oren' van de overheid. Het Ministerie van Economische Zaken kan dus geheel in stijl gebruik maken van *The Wisdom of the Crowds.* Veel mensen maken zich zorgen over netneutraliteit en zij zijn zeker niet te beroerd om dit te laten horen. Op talloze fora geven zij aan of en wanneer zij problemen ervaren hiermee. Het is dan ook zaak om dit regelmatig te monitoren op signalen over problemen. Het eventuele gebrek aan betrouwbaarheid van de individuele metingen wordt gecompenseerd door de grote massa van het aantal controleurs en het aantal meetpunten en meetmomenten. De monitoringkosten van het Ministerie van Economische Zaken (zie paragraaf 4.5) kunnen zo aanzienlijk dalen. Mogelijk kan het Ministerie van Economische Zaken ook een loketfunctie vervullen waar consumenten die problemen ervaren zich kunnen melden. Door middel van een specifiek e-mailadres kan dit op een zeer laagdrempelige wijze.

5.4 Conclusie

In hoofdstuk 5 stond het onderzoeksdoel centraal, betreffende de toekomstige marktsituatie en het monitoren van de situatie. Deze paragraaf presenteert de conclusies van dit hoofdstuk.

Hoe zal netneutraliteit zich in de Nederlandse markt naar verwachting ontwikkelen?

We concluderen dat er verschillende krachten zijn, die een positieve of negatieve impact hebben op de kans dat netwerkexploitanten verkeer verschillend behandelen. De krachten verschillen in de termijn waarop ze optreden en in de mate van waarschijnlijkheid (of omvang). De krachten met een positieve impact (zie tabel 6) spelen vooral op de langere termijn en hebben een middelgrote impact. Een aantal negatieve krachten - waaronder toename capaciteitsvraag bij mobiel internet en de opkomst van diensten die het business model van (vaste en mobiele) ISP's ondermijnen - speelt al op de korte termijn en heeft een middelgrote of grote impact. Op basis hiervan moet de overheid serieus rekening houden met het scenario dat het verschillend behandelen van verkeer in de komende jaren in Nederland toeneemt. De waarschijnlijkheid van dit scenario werd ook in de meeste interviews bevestigd.

Op de langere termijn gaan de positieve krachten – waaronder nieuwe technieken die het capaciteitsplafond van vaste en mobiele netwerken substantieel verhogen – een belangrijkere rol spelen. Voor zover discriminerend gedrag van netwerkexploitanten was ingegeven voor capaciteitsvraagstukken, zal het risico op het verschillend behandelen van verkeer daarmee afnemen.

Hoe kan het Ministerie van Economische Zaken deze ontwikkeling het best monitoren?

Monitoring van de situatie is van groot belang. Het laat onder andere zien in hoeverre de ingevoerde transparantie (zoals beoogd in het vorige hoofdstuk) inderdaad leidt tot een situatie die als wenselijk wordt beschouwd. Monitoring kan uit verschillende componenten bestaan:

- Het monitoren van een aantal marktontwikkelingen (krachten) die in dit rapport worden beschreven, zoals de capaciteitsvraag en de beschikbaarheid en het gebruik van diensten. Dit kan onder meer door op gezette tijden marktonderzoeken te consulteren, en gericht onderzoek uit te voeren.
- Een vinger aan de pols te houden door goed naar signalen van de eindgebruiker te luisteren. De internetgemeenschap is behoorlijk mondig en de overheid kan daar gebruik van maken. Het is belangrijk om steeds te weten in welke mate het verschillend behandelen van verkeer valt binnen de verkeerspolicies zoals bekend gemaakt door de ISP's. Inzicht in beide situaties (bekendgemaakte discriminatie en niet bekendgemaakte discriminatie) is van belang om na te gaan of de ingeslagen weg als succesvol moet worden beschouwd.
- Goed bijhouden of er steeds aan de voorwaarden voor transparantie wordt voldaan (voldoende mededinging, ontbreken van belemmerende overstapdrempels).

6 Besluit

Dit rapport kent drie centrale doelstellingen, te weten (1) het schetsen van de huidige marktsituatie, (2) het vergroten van transparantie en (3) het monitoren van de toekomstige marktsituatie. Deze doelstellingen, en de achterliggende onderzoeksvragen, zijn uitgewerkt in de hoofdstukken 3 tot en met 5. Die hoofdstukken sluiten elk met een concluderende paragraaf af. In dit laatste hoofdstuk gaan we in op de beleidsopties van het Ministerie van Economische Zaken aangaande netwerkneutraliteit, bezien vanuit de bevindingen uit deze studie.

De belangstelling voor het vraagstuk van netwerkneutraliteit – of het verschillend behandelen van internetverkeer – is groeiende. Hoewel het aantrekkelijk lijkt het verschillend behandelen van internetverkeer simpelweg te verbieden, is dat niet zonder meer de optimale oplossing. Achter de bedoelde gedragingen gaan verschillende motieven schuil, waarvan sommige vanuit een publiek perspectief meer toelaatbaar worden geacht dan anderen. De consequentie van een hard verbod zijn complex van karakter, omdat het ook consequenties kan hebben voor het aanbod, de productvariëteit, het prijspeil, en de mate van investeringen en innovaties, zowel in de netwerken zelf als in de periferie. Welke effecten het sterkste zijn is niet goed te voorspellen. Niet-economische argumenten (zoals vrijheid van meningsuiting en een recht om informatie te benaderen) zijn nog moeilijker mee te wegen. Daar komt bij dat het zeer moeilijk is een juiste grens te stellen. Dat komt onder meer omdat er verschillende motieven voor het verschillend behandelen bestaan, er verschillende inzichten bestaan welke motieven daarvan legitiem zijn of niet, en omdat uit een bepaalde handeling niet eenduidig opgemaakt kan worden wat het achterliggende motief voor die handeling is (‘Was er een technische noodzaak?’ ‘Is er bewust ondergeïnverteerd?’ ‘Probeert men eigen diensten te beschermen?’). Zelfs als er consensus zou bestaan over een bepaalde grens dan kan die grens door technologische ontwikkelingen of door ontwikkelingen in de markt achterhaald raken.

Het bovenstaande maakt de keuze voor een dergelijk verbod, en de keuze waar precies de lijn wordt getrokken, een lastige normatieve en dus politieke keuze. De consequenties zijn lastig te overzien en daarmee is het niet duidelijk of deze aanpak proportioneel is met de omvang van het probleem. In de Verenigde Staten is enkele jaren geleden geprobeerd om een volledig verbod af te kondigen, maar dat voorstel wist het politiek niet te halen. Ook de op handen zijnde revisie van het Europese New Regulatory Framework (NRF) voor telecommunicatie lijkt niet af te stevenen op een hard verbod (hoewel men wel de mogelijkheid voor een minimumniveau van dienstverlening wil vastleggen, als mogelijke maatregel indien blijkt dat de markt niet goed werkt).

Harde grenzen lijken dan misschien niet verstandig, we moeten tegelijkertijd concluderen dat het geen kwestie is die zichzelf oplost. Uit de analyses in dit rapport blijkt dat ook in Nederland behoorlijk wat consumenten te maken hebben met een aanbieder (ISP) die het verkeer op de een of andere manier verschillend behandeld. Ongeveer eenderde van de Nederlandse abonnees voor vaste diensten wordt hiermee geconfronteerd, en nagenoeg alle mobiele ISP’s doen aan vormen van verschillend behandelen (hoewel het af kan hangen van het gekozen abonnement). De consument kan niet altijd makkelijk nagaan of er sprake is van verschillend behandelen of niet.

Een beleid met als doel om alle aanbieders duidelijke informatie te laten verstrekken over hun verkeersbehandeling is daarom een aantrekkelijke keuze. Ze stoelt op een vorm van marktwerking: consumenten kunnen dit element mee laten wegen bij de keuze voor een

aanbieder. Daarmee ontstaat concurrentiedruk om ook op het gebied van netwerkneutraliteit een aantrekkelijk consumentenaanbod te doen. Anderzijds blijft er een zekere keuzevrijheid bij aanbieders. Om technische, strategisch/commerciële of andere redenen kan de aanbieder er voor kiezen een of meerdere producten aan te bieden die wel zekere beperkingen kennen (zoals snelheidsbeperkingen of blokkeringen bij bepaalde toepassingen of diensten). Hoewel de invoering van transparantie wel enige kosten en neveneffecten met zich meeneemt (zoals dat bij iedere interventie het geval is), zijn deze relatief gering. Een ander voordeel van een transparantiebeleid is de regelgever niet voor de taak staat om achterliggende motieven bij verschillend behandelen te achterhalen en te beoordelen. Ten slotte ligt de invoering van transparantie in lijn met de voorstellen voor de eerder genoemde revisie van het Europese New Regulatory Framework (NRF) voor telecommunicatie – de kans lijkt groot dat Europa een vorm van transparantie op dit gebied sowieso verplicht gaat stellen voor alle ISP's in Europa.

Transparantie is een middel om marktwerking te verbeteren. Voor dat laatste moet ook aan andere voorwaarden worden voldaan, zoals voldoende keuzevrijheid (lees: voldoende mededinging) en het ontbreken van belemmerende overstapdrempels. We concluderen dat aan de randvoorwaarde van mededinging wordt voldaan. De situatie betreffende overstapdrempels wordt door de overheid reeds geadresseerd.

Een belangrijk aspect bij transparantie is de vormgeving van dat instrument. Wie moet er transparant zijn, waarover moeten ze transparant zijn, voor wie en hoe moet de informatie beschikbaar zijn? Dit rapport bevat een aantal aanbevelingen hierover. De grootste uitdaging zit in het precieze format: welke informatie moet precies gecommuniceerd worden? Enerzijds is er de wens dat de informatie begrijpelijk is voor consumenten, zodat ze hun gedrag kunnen laten afhangen van de informatie die ze krijgen. We noemen dit *directe transparantie*. Anderzijds is er de wens dat de informatie feitelijk en controleerbaar is, alleen dan is controle en naleving mogelijk. De manier waarop het verschillend behandelen van verkeer plaatsvindt, is en blijft uiteindelijk een technische aangelegenheid. Er ligt hier ook nog een ander, aantrekkelijk aspect voor de overheid: deze gedetailleerde, feitelijke informatie *empowered* de internet community. Deze gemeenschap omvat technisch ervaren en sterk betrokken leden, die een belangrijke rol spelen bij het signaleren van gedragingen en misstanden, de vertaling van informatie voor de eindgebruiker, en het mobiliseren van de pers en soms zelfs de politiek. We noemen dit *indirecte transparantie.* Deze vorm van transparantie is vermoedelijk nog effectiever dan directe transparantie. Aanbieders blijken op de voet te volgen wat er in de internet community gebeurt, en passen hun gedrag aan op het moment dat er ophef of reputatieschade dreigt. Feitelijke, technische gedetailleerde transparantie helpt de internet community in grote mate haar werk te doen. Zeker als iets politieke aandacht krijgt kan dat effect hebben. Daar zijn diverse voorbeelden van, één waarvan zich voordeed ten tijde van het afsluiten van dit onderzoek. Bij de introductie van Skype voor de iPhone ontstond er een intense discussie over het feit dat bij sommige Nederlandse abonnementen voor mobiele telefonie Skype niet was toegestaan. Kort daarna kwamen diverse mobiele aanbieders met de toezegging hun beleid ten aanzien van Skype te (gaan) veranderen.[78]

Op basis van het bovenstaande adviseren we een transparantiemodel te kiezen waarin beide vormen worden gecombineerd: aanbieders moeten feitelijke, technisch verifieerbare informatie leveren over het eventuele verkeer dat ze verschillend behandelen; tegelijkertijd

[78] Voor de volledigheid moeten we melden dat het betreffende Skype programma geen gebruik kan maken van de mobiele telefoonverbinding van de iPhone; Skypen kan alleen via de WiFi verbinding. Naar verluidt heeft Skype hier van af gezien onder druk van Apple en de grote (Amerikaanse) mobiele telefoonaanbieders.

moeten ze voor de consument begrijpelijke informatie bieden welke consequenties een en ander heeft in termen van vaakgebruikte content, diensten en applicaties. Het is van belang om de stakeholders voldoende te betrekken bij het ontwerp van het format: dat helpt draagvlak te creëren. Aanbieders zijn (begrijpelijk) weinig enthousiast over een nieuwe verplichting, maar ze lijken niet geheel onwillig – indien ingevoerd op een manier die recht doet aan legitieme belangen.

Hoe netwerkneutraliteit zich de komende jaren zal ontwikkelen is afhankelijk van verschillende krachten. Sommige hebben een positieve impact op de kans dat netwerkexploitanten verkeer verschillend behandelen, andere een negatieve. De krachten verschillen in de termijn waarop ze optreden en in de mate van waarschijnlijkheid of omvang. Belangrijk is dat de overheid serieus rekening moet houden met het scenario dat het verschillend behandelen van verkeer in de komende jaren in Nederland toeneemt. Het is daarom van belang dat de situatie rondom netwerkneutraliteit goed wordt gemonitord. Dit rapport doet daartoe een aantal voorstellen, waarbij het opvangen van signalen uit de markt van consumenten en de internet community een belangrijke is.

Zoals eerder betoogt is de invoering van transparantie op dit moment verreweg de meest aantrekkelijke beleidsoptie. Uit de monitoring zal moeten blijken of de ingevoerde transparantie inderdaad leidt tot een situatie die (door de politiek) als wenselijk wordt beschouwd. Als dat niet het geval is, kunnen andere maatregelen – waaronder direct ingrijpen, met mogelijk meer vergaande neveneffecten tot gevolg – worden overwogen. Maar die zijn nu vooralsnog niet op zijn plaats.

Bijlage A: geraadpleegde literatuur

Atkinson & Weiser (2006).
A "third way" on network neutrality.
http://www.itif.org/files/netneutrality.pdf

Beverly et al (2007).
The internet is not a big truck, towards quantifying net neutrality.
http://www.rbeverly.net/research/papers/truck-pam07.pdf

Bleich & Mulder (2008).
Bewuste paniekzaaierij?
C'T - Magazine voor Computertechniek

Brennenraedts et al. (2008).
Go with the dataflow! Analysing the Internet as a Datasource (IaD).
http://www.ez.nl/dsresource?objectid=157262&type=PDF

Carter et al. (2008).
Network neutrality: implications for Europe.
http://www.wik.org/content/diskus/Diskus_314.pdf

Chirico et al (2007).
Network neutrality in the EU.
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1018326

Cooper & Scott (2006).
Importance of the internet and public support for net neutrality: national survey results.
http://www.consumerfed.org/pdfs/net_neutrality_poll.pdf

Crowcroft (2007).
Net neutrality: the technical side of the debate.
http://portal.acm.org/citation.cfm?id=1198263

Dischinger et al. (2008).
Detecting bittorrent blocking.
http://doi.acm.org/10.1145/1452520.1452523 & http://broadband.mpi-sws.org/transparency/results/

Eckersley et al. (2007).
Packet Forgery By ISPs: A Report On The Comcast Affair.
http://www.eff.org/files/eff_comcast_report2.pdf

Federal Trade Commision (2007).
Broadband connectivity, competition policy.
http://s158729929.onlinehome.us/images/uploads/Broadband_Report.pdf

Felten (2006).
Nuts and bolts of net neutrality.
http://itpolicy.princeton.edu/pub/neutrality.pdf

Ganley & Allgrove (2006).
Net neutrality: a user's guide.
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=925693

Gilroy (2006).
Net neutrality: background and issues.
http://www.fas.org/sgp/crs/misc/RS22444.pdf

Hermalin & Katz (2007).
The economics of product-line restrictions with an application to the network neutrality debate.
http://repositories.cdlib.org/cgi/viewcontent.cgi?article=1059&context=iber/cpc

Kocsis & De Bijl (2007).
Network neutrality and the nature of competition between network operators.
http://www.cpb.nl/nl/org/homepages/vks/kocsis-de-bijl_network_neutrality_2007.pdf

Kruse (2008).
Network neutrality and quality of service.
http://www.springerlink.com/content/u3p060p126355275/

Ministerie van Economische Zaken (2008).
Beleidsbrief convergentie.
http://www.ez.nl/dsresource?objectid=158451&type=PDF

Ministerie van Economische Zaken (2002).
Glashelder: meer inzicht in transparantie.
Intern document Ministerie van Economische Zaken

Moore (2006).
Staying in neutral: European implications of the net neutrality debate.
http://www.stockholm-network.org/downloads/publications/d41d8cd9-Network%20Neutrality%20Paper%20Final.pdf

Odlyzko (2008).
Net Neutrality and the never-ending confilct between efficiency and fairness.
http://www.dtc.umn.edu/~odlyzko/doc/net.neutrality.pdf

Odlyzko (2009).
Network neutrality, search neutrality, and the never-ending conflict between efficiency and fairness in markets.
http://www.rnejournal.com/artman2/uploads/1/odlyzko_RNE_mar09.pdf

OECD (2007).
Internet traffic prioritisation: an overview.
http://www.oecd.org/dataoecd/43/63/38405781.pdf

Peha (2006).
The benefits and risks of mandating net neutrality and the quest for a balanced policy.
http://web.si.umich.edu/tprc/papers/2006/574/Peha_balanced_net_neutrality_policy.pdf

Pouwelse et al. (2008).
Pirates and samaritans: measurements on peer production and implications for net neutrality.
http://www.tribler.org/trac/raw-attachment/wiki/PiratesSamaritans/pirates_and_samaritans.pdf

Renda (2008).
I own the pipes, you call the tune. The net neutrality debate and its (ir)relevance for Europe.

http://se1.isn.ch/serviceengine/FileContent?serviceID=ISN&fileid=68CBA6C9-BF97-0C80-D03B-9863380EA611&lng=en

Senster & De Kort (2007).
Consumentenbehoeften Mobiele communicatie.
http://www.ez.nl/dsresource?objectid=154504&type=PDF

Valcke et al. (2008).
Legal analysis of network neutrality under EU competition rules and the regulatory framework for electronic communications.
http://ssrn.com/abstract=1246642

Van der Berg (2008).
How the net works.
http://arstechnica.com/guides/other/peering-and-transit.ars

Van Schewick (2007).
Towards an economic framework for net neutrality regulation.
http://ssrn.com/abstract=812991

Weinstein (2007).
Ma Bell's revenge: the battle for net neutrality.
http://cacm.acm.org/magazines/2007/1/5742-ma-bells-revenge/pdf?dl=no

Yoo (2004).
Would mandating net neutrality help or hurt competition.
http://ssrn.com/abstract=495502

Bijlage B: interviewees

Naam	Organisatie
Aanbieders van diensten en content	
Machiel Bolhuis	Google
Stef van der Ziel	Jetstream
Hans Bos & Evert Romeyn	Microsoft
Egon Verharen	NPO
Marcel Flipse	Notubiz/Mybit
Rob Curver	VoIPro
Aanbieders van ISP-diensten	
Inez Jolink & Martijn de Jonge	Bbned
Jos Huigen & Ad Bresser	KPN
Walter Kroeze	Vodafone
Edwin Evenhuis	UPC
Niels Huijbregts	XS4ALL
Gerard Lieverse, Klaas Mantje & Leon Lemmens	Ziggo
Vertegenwoordigers van consumenten	
Maurice Wessling	Consumentenbond
Paul Brackel	Open Mobiel Internet
(Technisch) experts	
Driek van Dijk	AMS-IX
Klaus Mochalski & Hendrik Schulze	Ipoque
Erwin Bleumink	Surfnet
Johan Pouwelse	Technische Universiteit Delft
Erik Huizer	Universiteit Utrecht
Toezichthouder	
Robert Stil	OPTA

Bijlage C: aanwezigen workshop

Naam	Organisatie
Driek van Dijk	AMS-IX
Edwin Bogert	Bird & Bird
Feyo Sickinghe	Bird & Bird
Bart Schermer	ECP.NL
Patrick Blankers	Ericsson
Machiel Bolhuis	Google
Ad Bresser	KPN
Joost van der Vleuten	Ministerie van Economische Zaken
Marloes van Caspel	Ministerie van Economische Zaken
Norbert van den Hove	Ministerie van Economische Zaken
Roman Volf	Ministerie van Economische Zaken
Ronald van der Luit	Ministerie van Economische Zaken
Mathieu Andriessen	NL Kabel
Egon Verharen	NPO
Paul Brackel	Open Mobiel Internet
Erik Huizer	TNO-ICT
Jasper van Sluijs	Universiteit Tilburg
Edwin Evenhuis	UPC
Rob Rosendaal	Verizon
Walter Kroeze	Vodafone
Niels Huijbregts	XS4ALL
Gerard Lieverse	Ziggo
Joepke van der Linden	Ziggo

Contact:
Dialogic
Hooghiemstraplein 33-36
3514 AX Utrecht
Tel. +31 (0)30 215 05 80
Fax +31 (0)30 215 05 95
www.dialogic.nl