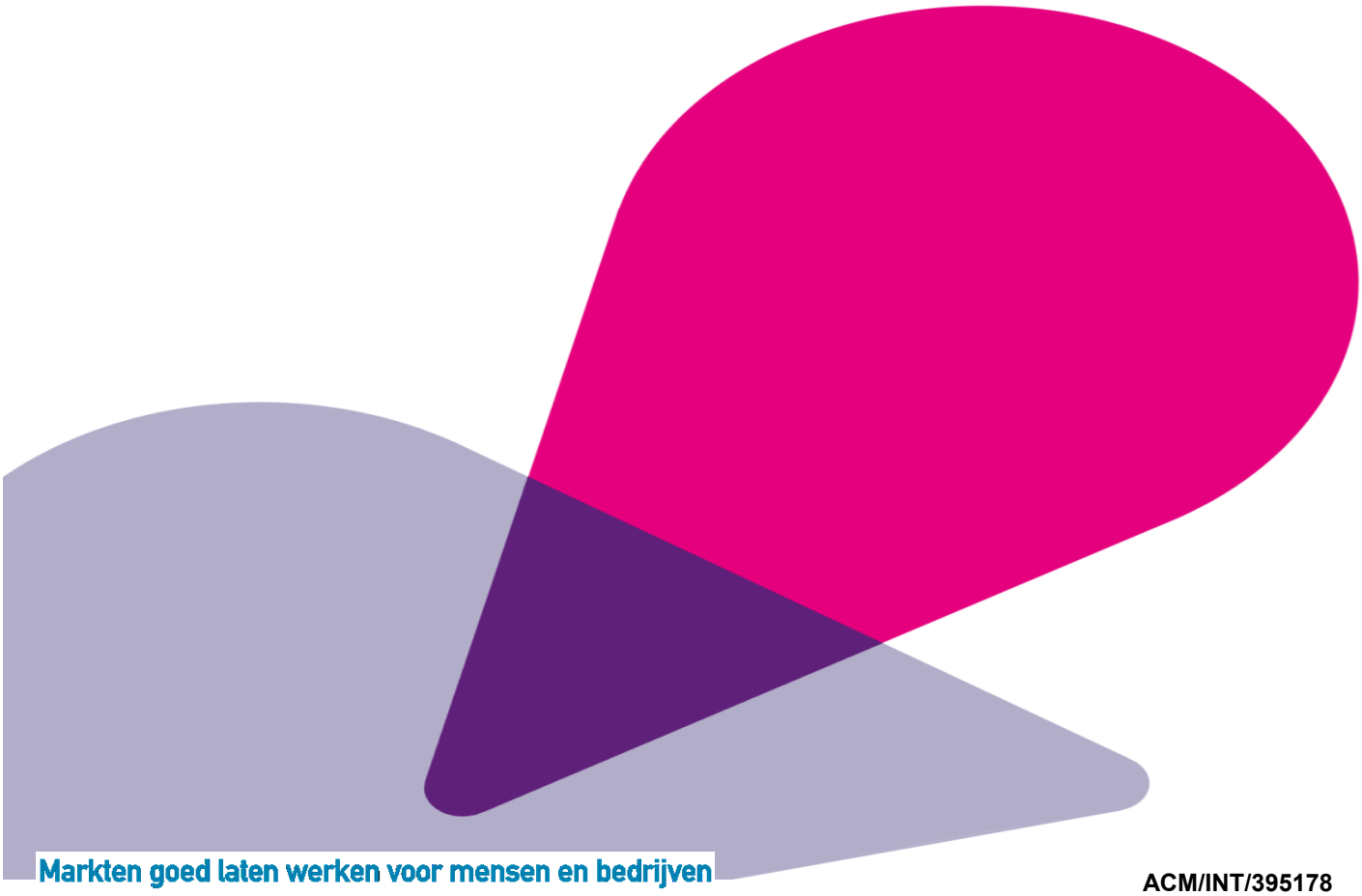
Autoriteit
Consument & Markt

Openbaar

Traffic Management

Voorlichtend document



Markten goed laten werken voor mensen en bedrijven

ACM/INT/395178

Inhoudsopgave

1 Leeswijzer

Traffic Management (hierna: TM) is een verzameling technieken die ingezet wordt om het internetverkeer op telecomnetwerken in goede banen te leiden. Het gebruik van deze technieken kan sommige soorten verkeer prioriteit geven en andere vertragen.

Op basis van de Open Internet Verordening (Verordening 2015/2120[1], hierna: OI Verordening) moet de ACM toezicht houden op de gelijke en niet-discriminatoire behandeling van verkeer bij het aanbieden van internettoegangsdienst. TM maatregelen die aanbieders van internettoegangsdiensten (hierna: ISP) nemen, kunnen hier inbreuk op maken. Om de kennis over TM maatregelen binnen de ACM te versterken en te controleren of Nederlandse ISPs zich aan de wet- en regelgeving houden, is het project *Verkenning Traffic Management* uitgevoerd. Door middel van desk research, informatieverzoeken en gesprekken met ISPs is de benodigde informatie verzameld. Dit rapport vat de bevindingen van dit project samen.

In dit rapport wordt eerst in een algemeen hoofdstuk ingegaan op de kenmerken van TM, de scenario's waarbij TM nodig is en de voorbeelden van TM technieken. Vervolgens wordt in een juridisch hoofdstuk een wegwijzer OI Verordening opgeschreven en worden de stappen voor TM maatregel beoordeling belicht. Dit hoofdstuk wordt afgerond met BEREC Opinie en de resulterende aanpassingen in de BEREC Guidelines. In hoofdstuk 4 worden veel voorkomende TM toepassingen toegelicht met groene en rode vlaggen om aan te geven welke punten tot zorgen over compliantie met de OI Verordening kunnen leiden, en wat voor omstandigheden deze zouden kunnen wegnemen. Gezien veel TM toepassingen door commerciële leveranciers als kant-en-klaar producten worden aangeboden, biedt hoofdstuk 5 een overzicht over deze TM mogelijkheden. De ACM heeft ook onderzocht welke TM maatregelen worden toegepast door Nederlandse ISP's en hoe zij zorgen dat deze voldoen aan de Verordening. De ACM concludeert dat de benodigde interne processen zijn ingericht. Dit wordt besproken in hoofdstuk 6. Het laatste hoofdstuk van dit rapport, hoofdstuk 7, biedt een korte handleiding aan toezichthouders die TM toepassingen moeten beoordelen. Dat betekent dat een belangrijke basis van onderzoeksvragen die nodig is voor het beoordelen TM praktijken hierin te vinden is.

De ACM maakt deze bevindingen openbaar om stakeholders meer duidelijkheid te geven over Traffic Management en wat er op dit gebied is toegestaan en wat niet. Zowel de ACM als andere Europese toezichthouders beoordelen namelijk regelmatig maatregelen van ISP's. De ACM nodigt ISP's en andere stakeholders uit om contact op te nemen wanneer zij vragen hebben over TM.

[1] http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32015R2120&rid=1. Deze verordening werd eerder de Netneutraliteitsverordening genoemd.

2 Wat is Traffic Management?

Traffic Management (TM) is een verzameling technieken die ingezet wordt om het verkeer op telecomnetwerken in goede banen te leiden. Het gebruik van deze technieken heeft als resultaat dat (simpel gezegd) sommige soorten verkeer prioriteit krijgen en andere vertraagd worden.

TM kun je zien als het in goede banen leiden van het verkeer, net zoals op de snelweg[2]. Vrachtwagens houden rechts aan, in de VS is er een gereserveerde rijbaan voor carpoolers, en politie en ambulance mogen desnoods over de vluchtstrook. Het internetverkeer kan worden gezien als de vrachtwagen en de carpoolers. Verkeer met speciale voorrang zijn dan politie en ambulance, zij komen overal het snelst.

2.1 Waar is TM voor nodig?

De verschillende soorten diensten die geleverd worden over telecomnetwerken, hebben verschillende eisen om goed te werken. Internetbellen bijvoorbeeld, heeft niet veel bandbreedte nodig maar stelt wel andere eisen:

- lage latency (vertraging) omdat het lastig praten is als wat je zegt vertraagd aankomt;
- niet te veel jitter (dat een later verzonden pakketje toch eerder aankomt) omdat je zin niet door elkaar mag raken.

Bij het downloaden van grote bestanden waar je later pas mee aan de slag gaat (bijvoorbeeld met een film van een streaming service opslaan op je tablet) zijn latency en jitter minder belangrijk, maar bandbreedte juist wel. Je wil de hele film wel snel binnen hebben.

Een belangrijk begrip in het kader van TM is congestie. Congestie ontstaat wanneer er meer verkeer bij een knooppunt op het netwerk aankomt dan het netwerk aankan. Buffers[3] op knooppunten helpen om hiermee om te gaan, maar het kan nog steeds te veel worden. Op zo'n moment worden datapakketjes weggegooid (of vertraagd). Dan merk je dat de dienst die je gebruikt even hapert. Een site wil bijvoorbeeld niet zo snel volledig laden als normaal. De verzender merkt wel dat de pakketjes niet aankomen en verstuurt ze iets later opnieuw[4]. Korte congestiemomentjes worden zo bijna vanzelf opgelost.

Elke router waar je datapakket langs komt, kan besluiten het voorrang te geven, te vertragen of weg te gooien. Dat kan bijvoorbeeld op basis van de eigenschappen van het pakket. Op elk datapakket zijn bepaalde dingen standaard zichtbaar in de *header* (een soort adreslabel): het IP-adres en poortnummer van de afzender, IP-adres en poortnummer van de ontvanger, en een beschrijving van de inhoud van het pakket. Een router kan die informatie gebruiken wanneer hij beslist wat hij met een pakket gaat doen. Dieper in het pakket kijken, dus naar de inhoud, kan technisch gezien wel (Deep

[2] https://www.ofcom.org.uk/__data/assets/pdf_file/0012/6042/traffic.pdf

[3] Een buffer kun je zien als een soort wachtkamer waar datapakketten even worden neergezet voordat ze worden doorgestuurd. Dat is handig, want als er even te veel pakketten tegelijk aankomen om meteen te verwerken, kunnen ze even wachten in de buffer voordat ze doorgestuurd worden en hoeven ze niet weggegooid te worden.

[4] Pakketjes opnieuw sturen wordt gedaan bij gebruik van het TCP protocol. Dat is handig als je per se alle informatie moet ontvangen (bijvoorbeeldalle delen van een bestand) en het niet zo veel uitmaakt als pakketjes op een iets andere volgorde aankomen. Realtime diensten zoals VoIP werken met UDP, waarbij pakketjes niet opnieuw verstuurd worden. Bij een verloren pakketje hoor je een tikje of wat ruis. Dat is minder storend dan het eerder verloren stukje geluid later alsnog opnieuw horen. https://wand.net.nz/pubs/19/html/node6.html

Packet Inspection) maar dat mag in de EU niet. En in de praktijk is het onhandig omdat het veel rekenkracht kost.[5]

Congestie kan ook langer duren, bijvoorbeeld wanneer mensen stranden op een station op Koningsdag en tegelijkertijd mobiele internetdiensten gebruiken. De netwerkpunten worden dan een tijd lang bestookt met zo veel data dat niemand meer goede mobiele internettoegang heeft. Een groot deel van iedereen zijn pakketjes moet namelijk weggegooid worden omdat ze niet verwerkt kunnen worden. Dat betekent trouwens niet dat de bewoners van de flat naast het station niet meer kunnen internetbellen, of geen IPTV meer kunnen kijken. Mogelijk blijven *specialised services (zie hoofdstuk 3.2.1)* die het mobiele netwerk gebruiken ook werken. Het zijn andere soorten diensten die gescheiden zijn van het internetverkeer: ze hebben hun eigen rijbaan. Dit soort dingen regelen op het netwerk is een voorbeeld van TM.

TM kan ook gebruikt worden om de impact van internetaanvallen te minimaliseren. Bij DDoS (Distributed Denial of Service) aanvallen bijvoorbeeld, worden (bijvoorbeeld geïnfecteerde) apparaten ingezet om heel veel aanvragen op een bepaalde dienst af te sturen. Ook Nederlandse organisaties overkomt dit zo nu en dan[6]. Daardoor raakt de dienst overbelast en kunnen klanten deze niet meer gebruiken. Een DDoS aanval opzetten is eenvoudig: ze zijn voor weinig geld in te kopen[7]. Met TM maatregelen kan het aanvallende verkeer worden omgeleid zodat de dienst weer beschikbaar is.

2.2 Voorbeelden van TM technieken

Traffic shaping: dit wordt gebruikt om binnenkomend verkeer op een netwerkpunt opnieuw te sorteren zodat de datapakketten het knooppunt in een gunstigere volgorde verlaten. Er wordt altijd gebruik gemaakt van een buffer.[8] Dit gebeurt in twee stappen:

- Stap 1: eerst komen alle pakketten binnen in de buffer. Of niet, als de buffer vol is. In het laatste geval worden alle aankomende datapaketten weggegooid. Maar dat is niet zo handig, omdat dan ook pakketten met hoge prioriteit verdwijnen. Deze *overflow*[9] kan ook ongeshaped[10] doorgestuurd worden. Een andere optie is om door middel van Active Queue Management (AQM) de buffer altijd een klein stukje leeg te houden zodat de mogelijkheid blijft bestaan om inkomende pakketten te bekijken. Voor AQM kunnen verschillende algoritmes gebruikt worden. Ze laten ofwel steeds minder pakketten binnen als de buffer steeds voller wordt, of gooien pakketten die al in de buffer zitten er weer uit om plek te maken. [11]
- Stap 2: nu zitten er dus datapakketten in de buffer. De *network scheduler* gaat bepalen in welke volgorde de pakketten het netwerk op gaan. Hier zijn allerlei verschillende algoritmes voor.[12] Het belangrijkste onderscheid is dat de *network scheduler* het óf simpel kan houden, óf verkeersclassificatie kan inzetten (zie hieronder). De *network scheduler* kan dus, als er bijvoorbeeld vijf pakketten in de buffer staan, ervoor kiezen eerst het pakket dat als derde

[5] https://www.antagonist.nl/blog/2016/04/netneutraliteit/

[6] https://nos.nl/artikel/2214537-nieuwe-ddos-aanval-op-abn-amro-ing-rabo-en-belastingdienst.html

[7] https://nos.nl/artikel/2215507-18-jarige-brabander-opgepakt-voor-recente-ddos-aanvallen.html *"De verdachte heeft naar eigen zeggen voor 40 euro aan capaciteit ingekocht bij een 'stresser', een onlinedienst die door bedrijven gebruikt kan worden om hun DDoS-bestendigheid te testen, maar net zo goed ingezet kan worden voor een daadwerkelijke DDoS."*

[8] https://en.wikipedia.org/wiki/Traffic_shaping

[9] Met *overflow* worden pakketten bedoeld die aankomen nadat de buffer al is volgelopen: als een emmer die overstroomd.

[10] Ongeshaped: de pakketten worden doorgestuurd in dezelfde volgorde als die waarop ze zijn aangekomen.

[11] https://en.wikipedia.org/wiki/Active_queue_management

[12] https://en.wikipedia.org/wiki/Network_scheduler

aankwam, daarna 2, 4 en 5 en als laatste pas pakket 1 door te sturen het netwerk op. En misschien is pakket 1 ondertussen weer uit de buffer verwijderd door het AQM. AQM wordt door de Internet Engineering Task Force aanbevolen als best practice voor het voorkomen van netwerkcongestie. [13]

In randnummer 54 van de BEREC Guidelines (hierna: Guidelines) staat dat Endpoint-based congestion control niet in strijd is met artikel 3 (3), eerste alinea omdat dit plaatsvindt in de eindapparatuur en daarmee buiten de scope van de OI Verordening valt. Endpoint-based congestion control wordt toegepast om ervoor te zorgen dat een netwerkkooppunt niet meer dataverkeer verwerkt dan het aan kan. Volgens de BEREC Guidelines moeten netwerk-interne technieken die endpoint-based control mogelijk maken (bijvoorbeeld AQM) wel voldoen aan de verplichtingen uit artikel 3 (3) van de OI Verordening.

Verkeersclassificatie en -prioritering
Op basis van de kenmerken van het aankomende verkeer wordt het ingedeeld in categorieën. Verkeer kan direct worden ingedeeld op basis van de informatie in de *header* van het datapakket, en die informatie kan ook worden aangevuld met kenmerken van de stroom pakketten (zoals hoe vaak ze verstuurd worden en hoe groot ze zijn). Zo kan ingeschat worden wat de inhoud van het pakket is. In dat tweede geval worden vaak *machine learning* algoritmes gebruikt om de categorieën te definiëren.[14]

Door bepaalde informatie mee te geven met een datapakket kan je er dus voor zorgen dat een pakket een grotere kans heeft om (snel) aan te komen op zijn bestemming omdat hij bij elk knooppunt voorrang heeft op veel andere pakketten.

Deep Packet Inspection
Bij Deep Packet Inspection (DPI) wordt in de inhoud van een datapakket gekeken, bijvoorbeeld om aanvullende informatie te verkrijgen op wat wordt gehaald uit de *header* en de kenmerken van de verkeersstroom om het pakket nauwkeuriger te kunnen classificeren. In de inhoud van het pakket zit informatie die privacygevoelig kan zijn. Uit overweging 10 van de OI Verordening is te concluderen dat ISP's geen DPI mogen toepassen.

Verbindingen belemmeren
Zoals hiervoor is uitgelegd, kan bijvoorbeeld verkeersclassificatie ingezet worden om verkeer te prioriteren waardoor de ene soort sneller doorkomt en de andere vertraagd wordt. Daarnaast is het uiteraard mogelijk verbindingen te blokkeren.

Address blocking: met *address blocking* kunnen eenvoudigweg alle binnenkomende pakketjes van een bepaald IP-adres worden genegeerd. Hiermee kunnen applicaties brute force attacks (een account kraken door geautomatiseerd heel snel heel veel wachtwoorden te proberen) afslaan.[15] Dit kan ook de andere kant op: netwerkknooppunten kunnen zo geprogrammeerd worden dat alle pakketjes richting een bepaald IP-adres verdwijnen. Dan kunnen gebruikers de dienst die dat IP-adres gebruikt niet meer bereiken.[16] Dit wordt ook wel blackholing genoemd.

[13] https://tools.ietf.org/html/rfc7567
[14] https://en.wikipedia.org/wiki/Traffic_classification
[15] https://en.wikipedia.org/wiki/IP_address_blocking
[16] https://blog.thousandeyes.com/deconstructing-great-firewall-china/

Een andere optie om een site onbereikbaar te maken is 'DNS poisoning'. Op een DNS server staat welke domeinnaam (website naam) bij welk IP adres hoort. Door op deze server verkeerde informatie te plaatsen, kun je zorgen dat gebruikers die naar een site willen, daar niet kunnen komen. Als je in China bijvoorbeeld naar www.google.cn wil gaan, kom je uit bij Baidu (een Chinese zoekmachine).[17]

Ook is het mogelijk om al gemaakte verbindingen weer te verbreken. In 2007 hinderde Comcast middels 'forged TCP resets' het BitTorrent verkeer. Wanneer Comcast een BitTorrent verbinding tussen twee gebruikers herkende, stuurde het beide gebruikers een 'reset pakket' waardoor beide gebruikers dachten dat de ander de verbinding wilde verbreken. Dit deed Comcast niet helemaal consistent, waardoor gebruikers niet klaagden over complete blokkades, maar slechts over trage werking van het BitTorrent programma.[18]

[17] https://blog.thousandeyes.com/deconstructing-great-firewall-china/

[18] http://www.nbcnews.com/id/21376597/#.WnrMSf6ounI

3 Wegwijzer Open Internet Verordening (deel TM)

In hoofdstuk 2 zijn verschillende TM technieken uitgelegd. Daar is nog niet ingegaan op de vraag of en wanneer deze technieken toegepast mogen worden. Op basis van de OI Verordening kan bepaald worden of TM maatregelen/technieken die toegepast worden door ISP's zijn toegestaan. Met een maatregel bedoelen we de inzet van één of meerdere technieken om een bepaald doel te bereiken. Dit hoofdstuk vat de belangrijkste onderdelen van de OI Verordening op het gebied van TM samen en licht ze toe. Dit hoofdstuk verwijst daarnaast naar de Guidelines waar invulling is gegeven aan de OI Verordening. Momenteel is BEREC bezig met het vernieuwen van de Guidelines, hierbij wordt stilgestaan in paragrafen 4 en 5.

3.1 Internetverkeer op gelijke wijze behandelen

Zoals in het vorige hoofdstuk is beschreven kunnen TM technieken gebruikt worden om bepaald verkeer te prioriteren en ander verkeer te vertragen. In artikel 3 van de OI Verordening wordt echter de verplichting opgelegd aan aanbieders van internettoegangsdiensten om alle verkeer op gelijke wijze, zonder discriminatie, beperking of interferentie te behandelen bij het aanbieden van een internettoegangsdienst. Dit betekent dat het toepassen van TM technieken in strijd kan zijn met artikel 3(3) van de OI Verordening.

In overweging 8 van de OI Verordening staat hier verder het volgende over:

" […] Volgens de algemene beginselen van het Unierecht en de vaste rechtspraak mogen vergelijkbare situaties niet verschillend worden behandeld en mogen verschillende situaties niet op dezelfde wijze worden behandeld, tenzij een dergelijke behandeling objectief gerechtvaardigd is."

Kort gezegd komt dit er op neer dat ISPs bij het aanbieden van internettoegangsdiensten (hierna: IAS) geen verschil mogen maken in de manier waarop zij vergelijkbaar internetverkeer technisch behandelen. Dit verbod op technische discriminatie van internetverkeer houdt bijvoorbeeld[19] in dat een ISP in principe geen hogere kwaliteitsniveau (QoS) mag bieden aan bepaalde applicaties of services. Als een ISP de ene video streaming dienst met een betere kwaliteit doorgeeft dan de andere, dan mag dat niet. Het zijn vergelijkbare diensten en daarom mogen ze niet verschillend worden behandeld.

3.2 Technische discriminatie

In randnummer 55 van de Guidelines worden drie voorbeelden genoemd van TM maatregelen die vallen onder het verbod op technische discriminatie zoals genoemd in artikel 3 (3) van de OI Verordening:

- Een maatregel waarbij een ISP de toegang tot specifieke content, een of meer applicaties (of categorieën daarvan) blokkeert, vertraagt, beperkt, interfereert met, degradeert of discrimineert, behalve in uitzonderingsgevallen zoals genoemd in artikel 3 (3) derde sub paragraaf.

- IAS aanbiedingen waarbij toegang tot het internet beperkt is tot een gelimiteerd aantal applicaties of eindpunten door de ISP (sub-internet diensten aanbod) zijn in strijd met artikel 3(3) eerste sub paragraaf, aangezien zulke aanbiedingen zien op het blokkeren van applicaties en/of discriminatie, beperking of interferentie gerelateerd aan de herkomst of bestemming van de informatie.

[19] Dit is maar één voorbeeld van een TM maatregel die ISPs kunnen inzetten om bepaald verkeer te prioriteren. In zowel de BEREC Guidelines als in hoofdstuk 2 van dit document zijn andere voorbeelden te vinden.

– Een zero rating aanbod[20] waar alle applicaties zijn geblokkeerd (of vertraagd) wanneer de data cap is bereikt behalve voor de zero rated applicatie(s), aangezien dit een overtreding is van artikel 3(3) eerste (en derde) sub paragraaf.

3.2.1 Uitzonderingen op het verbod op technische discriminatie

Zoals in de voorbeelden hierboven is genoemd is het vanuit de OI Verordening verboden om TM maatregelen toe te passen die zien op **blokkeren**, **vertragen**, **wijzigen**, **beperken** of **degraderen** van, **interfereren** met of **discrimineren** tussen specifieke inhoud (bijvoorbeeld video's over katten), toepassingen of diensten (bijvoorbeeld verschillende video streaming apps), of specifieke categorieën daarvan.[21] Voor TM maatregelen gelden extra strenge regels, waardoor die maatregelen slechts in uitzonderlijke omstandigheden zijn toegestaan. Van deze uitzonderlijke omstandigheden kan volgens de OI Verordening alleen sprake zijn in de volgende gevallen[22]:

1) Om te voldoen aan Europese of nationale wetgeving (juridische verplichtingen);

Een voorbeeld hiervan is het bevel van de rechtbank Den Haag aan ISPs om toegang tot de website The Pirate Bay te blokkeren[23].

2) Om de integriteit en de veiligheid van het netwerk, diensten die via het netwerk worden aangeboden en eindapparatuur van eindgebruikers te beschermen (DDoS aanvallen, spoofing, hacking of virussen via het blokkeren van IP adressen)[24] en

3) Om nakende netwerkcongestie te voorkomen en de effecten van uitzonderlijke of tijdelijke netwerkcongestie te voorkomen, op voorwaarde dat gelijkwaardig verkeer alsnog gelijk wordt behandeld. De maatregelen mogen alleen tijdelijk van aard zijn en geen substituut voor structurele oplossingen zoals het vergroten van de netwerkcapaciteit.

Een voorbeeld hiervan is dat een ISP bij netwerkcongestie ervoor kiest om het emailverkeer met een milliseconde te vertragen om zo het voice verkeer zonder onderbreking door te laten komen. Dit is als er sprake is van netwerkcongestie toegestaan op voorwaarde dat dan wel het emailverkeer van alle emaildiensten (zowel Gmail als Hotmail en de eigen dienst, enz.) wordt vertraagd.

Redelijke TM maatregelen

Als er sprake is van een van de bovengenoemde uitzonderingen dan mogen de TM maatregelen alsnog alleen toegepast worden als het gaat om "**redelijke traffic management maatregelen**"[25] in het geval van een internettoegangsdienst.

Om een efficiënt gebruik van netwerkcapaciteit mogelijk te maken, is in de OI Verordening de uitzondering van de redelijke TM maatregelen opgenomen[26]. TM maatregelen zijn als redelijk[27] te

[20] Bij zero rating is een deel van het verkeer 'gratis': dit dataverbruik telt niet mee voor de databundel van het abonnement. Zie ook randnummers 40 – 43 van de Guidelines.

[21] Verordening (EU) 2015/2120, artikel 3(3), derde alinea

[22] Verordening (EU) 2015/2120, artikel 3(3), derde alinea, onder a-c

[23] https://www.telecompaper.com/nieuws/ziggo-xs4all-moeten-the-pirate-bay-weer-blokkeren--1213114

[24] Het monitoren van internetverkeer is dan ook toegestaan om aanvallen op tijd te signaleren en tegen te houden.

[25] Verordening (EU) 2015/2120, artikel 3(3), tweede alinea

[26] Verordening (EU) 2015/2120, overweging 9 preambule

beschouwen wanneer deze[28]:

- Transparant, niet-discriminerend en evenredig zijn;
- Gebaseerd zijn op objectief verschillende technische kwaliteitsvereisten van specifieke categorieën verkeer[29];
- Niet gebaseerd zijn op commerciële overwegingen;
- Niet specifieke content monitoren (o.a. Deep Packet Inspection) en
- Niet langer worden aangehouden dan nodig.

Onder "*niet langer aangehouden dan nodig*" verstaat BEREC het volgende, namelijk dat de TM maatregelen proportioneel zijn. Dit houdt in dat om te bepalen of TM maatregelen niet langer in stand worden gehouden dan nodig er gekeken moet worden naar de uitwerking van de voorliggende TM maatregel. In bepaalde situaties zou het toegestaan kunne zijn onder de OI Verordening dat een ISP TM maatregelen op een continue basis in werking heeft (op de achtergrond). De eindgebruiker merkt hier alleen wat van als het drukker wordt op het netwerk en de TM maatregel effect gaat hebben. Echter, wanneer TM maatregelen permanent en terugkerend actief zijn, dan is BEREC van mening dat de NRA de noodzaak van de maatregelen in twijfel kan trekken en of deze nog wel als redelijk beschouwd kunnen worden.

Specialized services
Specialized services betreft de tweede groep waarvoor de OI Verordening een uitzondering geeft op het technische discriminatieverbod. Specialized services zijn diensten die een specifiek kwaliteitsniveau vereisen dat niet gegarandeerd kan worden binnen het standaard best effort IAS aanbod. Specialized services hebben de volgende kenmerken:

- Diensten anders dan IAS diensten;
- Geoptimaliseerd voor een specifieke aanbieder van inhoud en toepassingen en
- De optimalisatie is objectief gezien nodig om aan de eisen te voldoen voor een specifiek kwaliteitsniveau.

Voorbeelden van mogelijke specialized services zijn: VoLTE (voice over LTE, bellen over 4G), IPTV (live TV kijken over internet) met specifieke QoS (quality of service) eisen, operaties op afstand, M2M (machine-to-machine, bijvoorbeeld sensors verbonden aan een mobiel netwerk) en in specifieke gevallen VPN (virtual private network).

Het aanbod van specialized services is gebonden aan een aantal voorwaarden:
- Er is voldoende netwerkcapaciteit om de specialized services aan te bieden naast de IAS;
- Specialized services zijn niet bruikbaar als of worden aangeboden als vervanger voor IAS;
- Specialized services hebben geen negatief effect op de beschikbaarheid of algemene kwaliteit van IAS voor eindgebruikers en
- Specialized services mogen niet gebruikt worden om de bepalingen inzake traffic management maatregelen te omzeilen. NRAs moeten dus onderzoeken of een bepaalde toepassing niet aangeboden kan worden via IAS.

Providers mogen zelf specialized services bedenken en aanbieden, zolang ze aan de bovenstaande punten voldoen. We zien dat hier in de markt interesse voor is.

[27] Verordening (EU) 2015/2120, artikel 3(3), tweede alinea
[28] Randnummer 57 tot en met 74 van de BEREC Guidelines
[29] Verordening (EU) 2015/2120, artikel 3(3), tweede alinea

3.3 Beoordeling TM maatregel

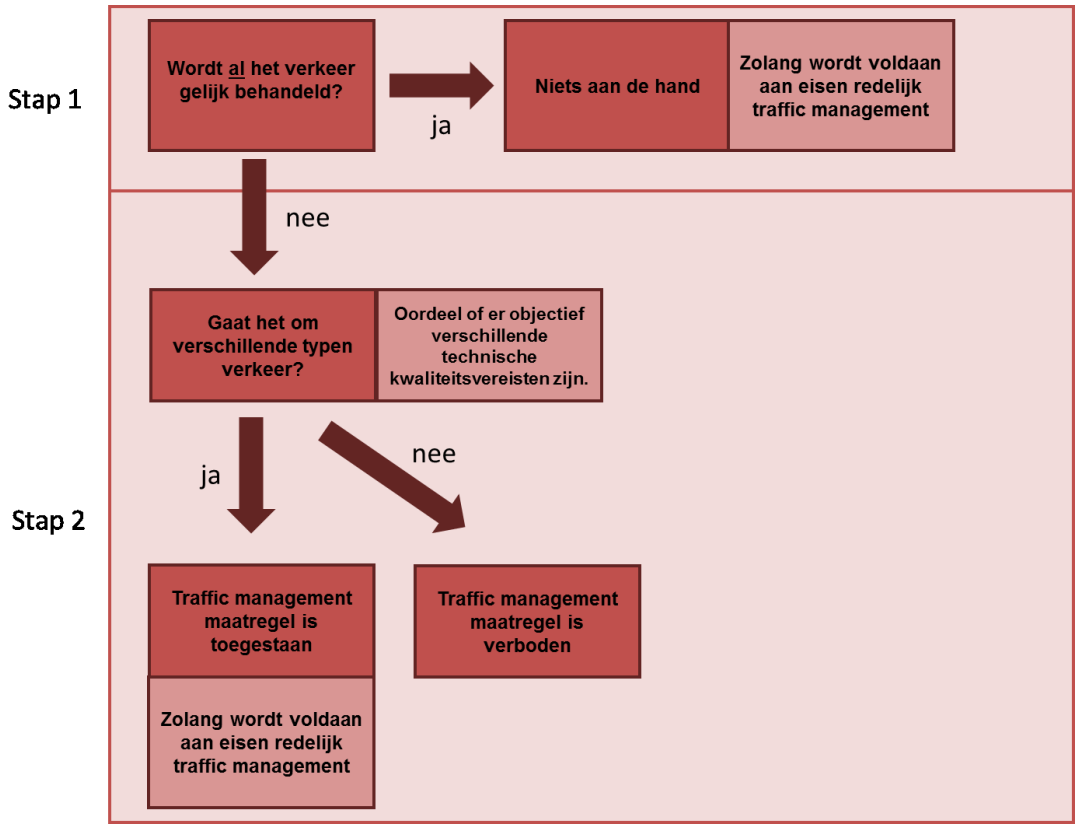
Het is aan de toezichthouder om te bepalen of een TM maatregel onder de OI Verordening is toegestaan of niet. In randnummer 51 van de Guidelines staat dat de toezichthouder hiervoor in twee stappen een beoordeling moet uitvoeren:

Stap 1: beoordelen of al het verkeer gelijk wordt behandeld.

Stap 2: beoordelen of situaties vergelijkbaar zijn of verschillend, en of er objectieve gronden zijn die het verschil in behandeling van het internetverkeer kunnen rechtvaardigen onder artikel 3 (3), tweede alinea van de OI Verordening.

Bij de beoordeling van TM maatregelen die onder bepaalde voorwaarden zijn toegestaan onder de OI Verordening zal de ACM een case by case beoordeling uitvoeren. Aan de hand van beoordeling stelt de ACM vast of de TM maatregel is toegestaan of verboden. In de BEREC NN werkgroep bespreekt de ACM met andere Europese telecomtoezichthouders de cases die ter beoordeling voorliggen om kennis uit te wisselen. De ACM adviseert ISPs die twijfelen over of TM maatregelen zijn toegestaan onder de OI Verordening om in een vroeg stadium met de ACM in gesprek te gaan.

Zie hiervoor ook de onderstaande figuur:



3.4 BEREC Opinie

In de BEREC opinie zijn een aantal onderwerpen op het gebeid van TM opgenomen waarvan BEREC het voornemen heeft om deze te verduidelijken in de Guidelines. Deze vormt een belangrijke basis voor de update van de Guidelines die BEREC in de eerste helft van 2020 gaat publiceren. In deze paragraaf zullen deze onderwerpen besproken worden.

Het aanbieden van IAS met verschillende QoS
Volgens meerdere stakeholders is het niet duidelijk of het is toegestaan om IAS met verschillende QoS[30] aan te bieden. Het aanbieden van IAS met verschillende QoS is volgens BEREC onder de OI Verordening toegestaan zolang eindgebruikersrechten niet worden beperkt. BEREC zal in de Guidelines verder verduidelijken dat het aanbieden van IAS met verschillende QoS klassen kan zolang deze in ieder geval applicatie-onafhankelijk, proportioneel en transparant worden geïmplementeerd.

Data compressie
BEREC vindt het in het belang van alle stakeholders om in de Guidelines verdere verduidelijking te bieden over data compressie en het verbod op "*throttling*" van dataverkeer. De OI Verordening staat het gebruik van niet-discriminerende data compressie technieken die alleen de grootte van een databestand verkleinen zonder dat de inhoud aangepast wordt toe (overweging 11). Volgens BEREC is "*throttling*" door een ISP van de datastream binnen de IAS niet toegestaan onder artikel 3(3) van de OI Verordening en daarmee is het volgens BEREC ook niet toegestaan om applicatie-specifieke throttling te gebruiken om CAPs te dwingen om hun video content in een lagere resolutie aan te leveren. Dit type maatregelen valt volgens BEREC niet onder data compressie zoals bedoeld en toegestaan onder overweging 11 van de OI Verordening.

Blokkeren van content
Door stakeholders is meerdere malen de vraag aan BEREC gesteld of het is toegestaan om bepaalde content, zoals spam, illegale content en content die niet geschikt is voor kinderen te blokkeren. Het voorstel van BEREC is de Guidelines op dit punt te verduidelijken aan de hand van de volgende drie aspecten:

- De reikwijdte van de OI Verordening ziet niet op software die geïnstalleerd is op eindapparatuur, zoals computers en mobiele telefoons. Het installeren van software voor een kinderslot is daarom dan ook niet in strijd met de OI Verordening zolang deze op eindapparatuur is geïnstalleerd.
- De reikwijdte van de OI Verordening ziet op de IAS (network layer) en niet op de content en applicaties die over de IAS worden geleverd. Het filteren van spam kan toegestaan zijn als bijvoorbeeld een emailserver de spam zou filteren. Applicatie servers vallen niet binnen de reikwijdte van de OI Verordening, omdat dit eindpunten betreft die verbonden zijn met het internet.
- Het filteren van web content in het netwerk is niet toegestaan. Dit is bijvoorbeeld wanneer datapakketten die verstuurd worden tussen een webserver en webclient en de *middlebox* in het netwerk van de ISP de datapakketten die langskomen mag controleren en de payload mag manipuleren. Dit is in strijd met de OI Verordening, omdat de payload wordt veranderd gedurende de transmissie tussen de eindpunten van de applicatie (i.e. in het netwerk).

BEREC zal in de Guidelines verder verduidelijken tot welke hoogte het blokkeren van bepaalde content is toegestaan in het geval van *endpoint-based mechanisms* en *application layer mechanisms.*

[30] QoS parameters zijn bijvoorbeeld snelheid, latency, jitter en packet loss.

Legitieme veiligheidsmaatregelen
Vanwege de input van stakeholders en de gesprekken met ENISA vindt BEREC het wenselijk om te verduidelijken in de Guidelines hoe toezichthouders maatregelen die zien op de integriteit en beveiliging van het netwerk, diensten die over het netwerk worden geleverd en eindapparatuur van eindgebruikers kunnen beoordelen. ENISA heeft richtsnoeren ontwikkeld die toezichthouders kunnen gebruiken om verzoeken van ISPs om de internettoegangsdienst te beperken op grond van netwerkveiligheid en integriteit maatregelen te beoordelen. Echter, de beoordeling of een TM maatregel is toegestaan op grond van de legitieme veiligheidszorgen ligt bij de toezichthouder en zal gemaakt worden op basis van specifieke nationale omstandigheden. In de Guidelines zal BEREC proberen verder te verduidelijken wat legitieme veiligheidsmaatregelen zijn en zal hierbij de ENISA [31] richtsnoeren hierin meenemen.

Duur van de traffic management maatregelen
Sommige stakeholders hebben tijdens de consultatie aangegeven dat in de Guidelines randnummer 73 verduidelijkt moet worden en anderen hebben voorgesteld dat het toegestaan moet zijn om redelijke TM maatregelen op een continue basis toe te passen. BEREC heeft het voornemen om in de Guidelines te verduidelijken dat er een verschil is tussen is tussen maatregelen die geen impact hebben op het verkeer (bijvoorbeeld een functionaliteit die op een continue basis op de achtergrond monitort of er veiligheidsrisico's zijn), en maatregelen die wel impact hebben op het verkeer. Alleen voor de laatste geldt dat deze slechts tijdelijk actief mogen zijn.

Specialized services
Vanwege de publieke discussies over de comptabiliteit tussen netneutraliteit en 5G technologieën is de vraag wat een specialized service is en welke criteria meegenomen moet worden bij de beoordeling nog relevanter geworden. BEREC zal daarom bekijken of een verdere verduidelijken van de criteria waaraan voldaan moet worden om een dienst te kunnen kwalificeren als een specialized service op basis van een case-by-case beoordeling in de Guidelines nodig is. Hierbij merkt BEREC al we op dat dat er in de OI Verordening in principe geen verschil bestaat tussen 5G en bestaande of opkomende netwerktechnologieën. De OI Verordening is techniekneutraal. BEREC zal in de Guidelines ook verder verduidelijking bieden over de relatie tussen specialized services en de internettoegangsdienst.

3.5 Vernieuwde BEREC Guidelines

Alle punten uit hoofdstuk 3.4 zijn meegenomen in de vernieuwde BEREC Guidelines. Daarnaast is ook duidelijker gemaakt hoe ISPs om moeten gaan met partijen die willen deelnemen aan hun zero rating programma's. Toezichthouders beslissen hierover per individuele zaak, en in de Guidelines zijn te overwegen punten opgenomen. Ook heeft BEREC in de consultatie vragen gesteld aan stakeholders over het verbod op het monitoren van specifieke content. Om de Guidelines op dit punt te kunnen verduidelijken, heeft BEREC namelijk meer informatie nodig.

Tussen 10 oktober en 28 november 2019 konden stakeholders hun zienswijzen op de Guidelines indienen. BEREC publiceert in het eerste helft van 2020 de definitieve geüpdatete versie van de Guidelines.

[31] https://www.enisa.europa.eu/publications/guideline-on-assessing-security-measures-in-the-context-of-article-3-3-of-the-open-internet-regulation

4 Traffic management voorbeelden

We gebruiken de volgende sectie om de voorbeelden toe te lichten die zijn besproken binnen BEREC. De voorbeelden zijn gegroepeerd op basis van hun gemeenschappelijke kenmerken, zoals technologie of toepassing. Onder elke groep beginnen we met een korte beschrijving van de kenmerken. We vatten de aandachtspunten samen met de rode en groene vlagen en geven aan hoe momenteel tegen dit onderwerp aan wordt gekeken. Een rode vlag betekent dat wanneer dit punt van toepassing is bij een maatregel, dit bij een toezichthouder waarschijnlijk zal leiden tot zorgen over compliantie met de OI Verordening. Wanneer een groene vlag van toepassing is, zal dit bij een toezichthouder waarschijnlijk leiden tot minder zorgen over compliantie met de OI Verordening. Dit kan niet worden gezien als een oordeel van de ACM over concrete zaken, want concrete zaken beoordelen we per stuk op basis van de specifieke informatie over die zaak.

4.1 Zero-rating

Zero-rating is de praktijk om voor het datagebruik van bepaalde internetdiensten een nultarief in rekening te brengen. Meerdere ISPs bieden zero rating diensten aan onder verschillende voorwaarden.

Veel zero-rating diensten bieden tegen een nultarief toegang tot bepaalde applicaties (bijvoorbeeld Facebook, Instagram en Whatsapp) en streaming-services (bijvoorbeeld muziek- of video-diensten). Een variant hierop is dat dergelijke zero-rating diensten via een bepaald platform worden aangeboden. Een deel van de ISPs biedt de zero-rating diensten aan tot het moment dat de klant zijn datalimiet heeft bereikt. Dat betekent dat de klant geen zero-rated diensten meer mag gebruiken als zijn databundel verbruikt is. Er zijn echter ook ISPs die gebruik van zero-rated diensten altijd toestaan, ook wanneer de datalimiet al bereikt is en niet-zero-rated diensten dus niet meer gebruikt kunnen worden.

Dit laatste is in strijd met artikel 3, derde lid, van de NN-verordening.[32] Bij de beoordeling van een zero-rating dienst toetst de toezichthouder of deze niet in strijd is met artikel 3, lid 2 en lid 3 van de OI Verordening.

Het komt ook voor dat ISPs zero-rating in combinatie met andere voorwaarden willen aanbieden, zoals onbeperkt video kijken waarbij verplicht de videoresolutie wordt verlaagd. In de vernieuwde versie van de OI Guidelines licht BEREC toe dat dit niet valt onder de uitzondering op datacompressie die in de OI Verordening wordt beschreven in overweging 11.

Rode vlaggen:
- Wanneer klanten hun datalimiet bereiken, hebben klanten alleen nog toegang tot zero-rated diensten.
- Er zijn voorwaarden (anders dan de al genoemde selectie van diensten) verbonden aan het zero rated aanbod, zoals een beperking op de doorgiftesnelheid of resolutie.

Groene vlaggen:
- Als na het bereiken van de datalimiet het verkeer van de zero-rated diensten technisch op dezelfde manier behandeld wordt. Blokkeert de ISP na het bereik van de datalimiet het overige verkeer, dan moet het verkeer van zero-rated diensten ook geblokkeerd worden. Is het beleid van de ISP om de snelheid te verlagen na het bereiken van de datalimiet, dan moet de snelheid voor

[32] Vonnis, Bestuursrechtbank te Stockholm, zaak nr. 4207-17.

het zero-rated verkeer tot dezelfde snelheid worden verlaagd.

Verder worden zero rating diensten ook beoordeeld onder artikel 3(2), onder andere op de invloed van het zero rating aanbod op de keuze van de eindgebruikers en op de toegankelijkheid voor app-aanbieders.

4.2 Throttling

Throttling is een methode om de snelheid van een internetdienst opzettelijk te verlagen of beperken. Verschillende ISPs passen throttling toe voor klanten die zero-rating diensten hebben voor het video- en muziekverkeer. Er zijn ook klanten die throttling ervaren tijdens roaming binnen de EU. Tot nu toe heeft geen enkele ISP die throttling toepast bij zero rating diensten hiervoor objectieve technische redenen kunnen geven.

Rode vlaggen:
- Objectieve technische redenen om throttling toe te passen zijn tot nu toe nog niet aangedragen door ISPs.
- Het is belangrijk om te checken wie het throttelen toepast: de ISP of de aanbieder van de content? Toepassing van throttling door de ISP moet nader onderzocht worden. heeft extra aandacht nodig.

Groene vlaggen:
- Als de ISP dit toepast wanneer de internetbundel van de klant op is, en deze zonder kosten toch gebruik kan blijven maken van zijn internetverbinding met een beperkte snelheid.

4.3 Websites blokkeren

ISPs blokkeren de toegang tot websites die auteursrechten schenden. Het blokkeren kan een gevolg zijn van zowel een rechtelijke uitspraak als een verzoek van de auteursrechthebbende. De NRA moet onderzoeken of het blokkeren van de website is toegestaan onder OI Verordening.

Rode vlaggen:
- ISP blokkeert toegang tot een website.

Groene vlaggen:
- Mogelijke vrijstelling onder artikel 3, lid 3, onder subparagraaf 3.

4.4 Poorten blokkeren

ISPs blokkeren poorten om veiligheidsredenen. Als gevolg hiervan konden de applicaties die deze poorten gebruiken geen data uitwisselen via de internettoegangsdiensten. Deze praktijk is gerechtvaardigd overeenkomstig artikel 3, lid 3, onder b, op voorwaarde dat het blokkeren de integriteit en veiligheid van het netwerk, de diensten die via het netwerk worden aangeboden of de apparatuur van de eindgebruiker beschermt.

Rode vlaggen:
- In het geval dat de ISP geen legitieme reden heeft om een poort te blokkeren.

Groene vlaggen:
- In het geval dat het blokkeren gerechtvaardigd is op voorwaarde dat dit de integriteit en veiligheid

van het netwerk beschermt.

ENISA heeft richtlijnen gemaakt die helpen bij het beoordelen van veiligheidsmaatregelen.[33]

4.5 Aangepaste gespecialiseerde diensten

De ISP voegt bijvoorbeeld een Video on Demand dienst (VoD-dienst) toe boven op de lineaire tv-dienst en het gecombineerde verkeer (d.w.z. VoD- en TV-diensten) wordt geprioriteerd. De lineaire tv-dienst is een gespecialiseerde dienst[34] maar de VoD-dienst niet. De prioriteitstelling van deze VoD-dienst (via de bundeling met de lineaire TV) beperkt het recht van eindgebruikers om andere VoD-diensten te bekijken omdat andere (standalone) VoD-diensten niet dezelfde geprioriteerde behandeling krijgen.

Rode vlaggen:
- Een aangepaste *specialized service* (bijvoorbeeld een standaard gespecialiseerd dienst met een add-on-dienst) voldoet niet automatisch aan de criteria van een gespecialiseerde service. Er moet daarom ook gekeken worden naar de standalone alternatieven van dergelijke add-on-diensten.

Groene vlaggen:
- Geen

4.6 Verbreken van de internetverbindingen

De internetverbinding van de eindgebruiker wordt elke 24 uur door de ISP verbroken. Dit beperkt het recht van de eindgebruiker om informatie te verspreiden en om applicaties en services aan te bieden. In dit geval belemmert de ISP het internetverkeer dat wordt aangeboden door de eindgebruiker. In dit geval heeft de NRA de ISP bevolen om te stoppen met het verbreken van de internetverbinding en minstens 31 dagen een ononderbroken internetverbinding aan te bieden.

Rode vlaggen:
- ISP beperkt de gebruikersrechten (artikel 3(1))
- ISP interfereert met het verkeer (artikel 3(3))

Groene vlaggen:
- Geen

[33] https://www.enisa.europa.eu/publications/guideline-on-assessing-security-measures-in-the-context-of-article-3-3-of-the-open-internet-regulation

[34] Para 113, NN BEREC guideline.

5 Door commerciële partijen aangeboden TM mogelijkheden

TM producten zijn bij meerdere aanbieders uit verschillende landen verkrijgbaar. De ACM heeft het aanbod onderzocht van een aantal leveranciers. De onderzochte partijen zijn F5 [35], NEC [36], Allot [37], Infradata [38], A10 Networks [39], en Dyn [40]. Deze partijen kwamen hoog in de zoekresultaten voor bij algemene zoekopdrachten zoals “traffic management solution”. Zij bieden zowel producten aan die door ISPs kunnen worden gebruikt, als producten die door aanbieders van content en diensten kunnen worden gebruikt. De volgende paragrafen leggen de belangrijkste termen uit die aanbieders gebruiken om hun producten te beschrijven.

Verkeersclassificatie
Dit is de basis van TM, en is uitgelegd in hoofdstuk 2. Veel aanbieders bieden producten aan die dit kunnen, zodat providers bijvoorbeeld VoIP, peer-to-peer (torrents)[41], en webverkeer van elkaar kunnen onderscheiden en indien gewenst anders kunnen behandelen. Soms beschrijven aanbieders dat content wordt geïnspecteerd of dat DPI wordt ingezet om het verkeer te classificeren.

Beheer van Quality of Experience en Quality of Service
Meestal is dit het doel van traffic management producten. Hiermee bedoelen aanbieders het zo efficiënt mogelijk bieden van een zo goed mogelijke internetervaring. Hiervoor zetten zij verschillende technische mogelijkheden in. Welk deel van het verkeer door welk onderdeel (bijvoorbeeld een virusscanner) wordt ‘behandeld’ kan statisch (op basis van regels over het type verkeer) of dynamisch (op basis van regels over het type verkeer én het type gebruiker) worden bepaald. Zo hoeft niet al het verkeer overal langs en wordt op capaciteit bespaard.

Bandbreedtecontrole
Dit is het bepalen van hoe veel bandbreedte een gebruiker op een bepaald moment mag gebruiken, en dit handhaven. De toegestane bandbreedte kan bepaald worden op basis van bijvoorbeeld de abonnementskenmerken van de gebruiker (snelheid die bij het abonnement hoort, of de datalimiet al bereikt is) of de hoeveelheid verkeer op het netwerk.

Abonneebewustzijn
Abonneebewustzijn (subscriber awareness): informatie over de eindgebruiker wordt gebruikt om het verkeer te managen. Het gaat om informatie zoals IP adres, IMSI (een nummer in de SIM kaart), of informatie over de mobiele zendmast.

Analyse van gebruikersgedrag
Dezelfde informatie die wordt gebruikt voor het managen van het verkeer, kan ook worden gebruikt om gebruikersgedrag te analyseren. Op basis van deze informatie kunnen beslissingen worden gebaseerd over netwerkmanagement en producten zoals nieuwe soorten abonnementen en hun voorwaarden.

---

[35] https://f5.com/about-us

[36] http://www.nec.com/en/press/201502/global_20150224_03.html

[37] https://www.allot.com/service-providers/traffic-management/

[38] https://www.infradata.eu/nl/technologieen/network-services/traffic-management

[39] A10 Solution Brief, Intelligent Traffic Steering in Mobile Networks, Oct 2017, blz 1.

[40] https://dyn.com/dns/traffic-steering/

[41] Gebruikers bieden via een programma bestanden aan die op hun computer staan, die andere gebruikers kunnen downloaden.

Transparent caching
Content die vaak opgevraagd wordt, kan in een cache server dichter bij de gebruiker worden opgeslagen. Wanneer een gebruiker content opvraagt, wordt eerst gekeken of deze content al *gecached* is. Zo ja, dan krijgt de gebruiker de content aangeleverd vanuit de cache server want dat is sneller. Zo nee, dan wordt de content opgehaald vanaf de normale server.

DNS sturing
Deze manier van verkeerssturing gebruikt het Domain Name System (DNS). Dit systeem wordt gebruikt om namen van computers te vertalen naar IP-adressen en andersom. Dit werkt met opzoektabellen. Met DNS verkeerssturing kan bijvoorbeeld gezorgd worden dat eindgebruikers contact maken met de dichtstbijzijnde beschikbare server voor de dienst die zij willen gebruiken. Daardoor werkt de dienst sneller. DNS verkeerssturing lijkt vooral gebruikt te worden door aanbieders van content en diensten. Op deze manier heeft deze dienst niet direct invloed op de internettoegangsdienst, maar wel op de internetervaring.

DoS verdediging
Tijdens een DoS (Denial of Service) aanval wordt zo veel verkeer naar een site, dienst of server gestuurd, dat deze voor normale klanten moeilijk of niet meer bereikbaar is. Deze aanvallen zijn te herkennen doordat opeens ongewoon grote hoeveelheden verkeer aankomen bij de site, dienst of server, vanaf één of een aantal bronnen. ISPs kunnen deze verkeersstromen herkennen en bijvoorbeeld *blackholen:* doorsturen naar een niet bestaande bestemming. Hierdoor verdwijnt het verkeer en is de site, dienst of server weer beschikbaar voor normale klanten.

Conclusie
Meerdere partijen bieden verschillende producten op het gebied van traffic management aan. Een deel van de aangeboden producten (of onderdelen daarvan), zoals inspectie van content, is in strijd met de OI Verordening. De ACM heeft daarom Nederlandse ISPs gevraagd of zij gebruikmaken van externe leveranciers voor TM, en zo ja, hoe zij ervoor zorgen dat alleen oplossingen worden geïmplementeerd die voldoen aan de OI Verordening. Dit is namelijk hun verantwoordelijkheid. ISPs lichtten toe dat zij kunnen kiezen hoe producten worden geïmplementeerd. Zo kunnen zij ervoor zorgen dat de TM producten die zij gebruiken, voldoen aan de OI Verordening. Zie hoofdstuk 6 voor een meer uitgebreide toelichting hierop.

6 Wat doen providers aan Traffic Management

In 2017 en 2018 heeft de ACM de algemene voorwaarden van verschillende ISPs onderzocht om mogelijke overtredingen van de OI verordening op te sporen, waaronder die op de bepalingen over traffic management. De ACM heeft ook gesprekken gevoerd met vier ISPs die eigen netwerk hebben en daarna brieven gestuurd naar de twaalf grootste ISPs op de Nederlandse markt. Het doel was om te achterhalen welke maatregelen zij toepassen en eventueel passages uit de algemene voorwaarden te verduidelijken. Ook heeft de ACM hen gevraagd hoe zij zorgen dat zij alleen traffic management maatregelen toepassen die in overeenstemming zijn met de OI Verordening. In paragraaf 6.1 wordt besproken welke soorten maatregelen ISPs over het algemeen toepassen, en paragraaf 6.2 bespreekt de interne processen die zij gebruiken om te zorgen dat zij voldoen aan de OI Verordening.

6.1 Toegepaste traffic management praktijken

Uit het onderzoek van de ACM, blijkt dat alle bevraagde ISPs verkeersbeheersmaatregelen nemen. De onderstaande paragrafen bespreken de verschillende types maatregelen.

Filteren op spam, virussen, malware
Alle bevraagde ISPs die zelf traffic management uitvoeren, filteren op spam, virussen, en malware. Dit houdt in dat gedetecteerde spam, virussen en malware tegengehouden worden, en kan ook betekenen dat gebruikers die dit verspreiden in quarantaine gezet worden. Gebruikers in quarantaine kunnen tijdelijk geen gebruik maken van hun internetverbinding totdat zij de verspreiding vanaf hun verbinding hebben opgelost. ISPs assisteren gebruikers hierbij. Artikel 3(3), onder b van de Verordening staat maatregelen toe om de veiligheid van het netwerk, de diensten op het netwerk en de eindapparatuur van de eindgebruikers te beschermen.

Poorten blokkeren
Poorten die vaak gebruikt worden om computers te besmetten, of die gemakkelijk te misbruiken zijn worden dicht gezet of alleen voor specifieke diensten open gelaten. De meeste providers hebben bijvoorbeeld poort 25 voor het meeste verkeer gesloten omdat deze lange tijd gebruikt werd om spam te versturen. Consumenten kunnen via deze poort daarom alleen de e-mail dienst van hun provider gebruiken.

Controle op basis van verkeersstromen
Door Nederlandse ISPs wordt ook controle op basis van verkeersstromen toegepast. In hoofdstuk 5 is uitgelegd hoe dit wordt ingezet om (D)DoS aanvallen te herkennen. Naast (D)DoS aanvallen is het ook mogelijk hiermee andere problemen te herkennen die een verandering in de verkeersvolumes teweeg brengen, bijvoorbeeld een geïnfecteerde computer die virussen gaat verspreiden.

Tijdkritisch verkeer voor laten bij congestie
VoIP kan bijvoorbeeld voorrang krijgen wanneer het erg druk is op het netwerk. Dit is een standaard praktijk en gerechtvaardigd omdat VoIP een specifiek kwaliteitsniveau vereist om bruikbaar te zijn.

Traffic management voor partijen die ruimte inkopen
Wanneer partijen netwerkcapaciteit inkopen bij een provider, kunnen zij ervoor kiezen het traffic management daar zelf te doen, of er een dienst voor in te kopen bij de netwerkeigenaar. Dit geldt voor zowel de mobiele als de vaste netwerken.

6.2 Interne processen traffic management

Dit hoofdstuk beschrijft de interne processen die de Nederlandse ISPs met eigen netwerken hanteren om te zorgen dat de TM maatregelen die zij toepassen compliant zijn met de Open Internet Verordening.

Proces voor nieuwe diensten
Alle ISPs hebben interne processen die worden doorlopen wanneer nieuwe producten worden ontwikkeld. Senior medewerkers van de juridische afdeling worden standaard bij het ontwikkelproces betrokken en ze geven advies over compliantie van het product met de Open Internet Verordening. Een deel van de ISPs heeft in het ontwikkelproces vaste momenten opgenomen waar de juridische afdeling advies geeft over het nieuwe product. De andere ISPs kiezen die momenten per project.

Vetorecht juridische afdeling
Bij een deel van de ISPs kan de juridische afdeling een veto uitspreken over een product dat zij niet compliant vinden met de OI Verordening. Bij de andere ISPs neemt de directie een besluit op basis van het advies van de juridische afdeling.

OI Verordening training van medewerkers
Alle ISPs zorgen voor trainingen op het gebied van netneutraliteit, voor zowel medewerkers van de juridische afdelingen als bredere groepen medewerkers. Dit zijn zowel trainingen van externen aan medewerkers van ISPs, als presentaties en trainingen die intern worden georganiseerd.

Gesprekken met de ACM
Een deel van de ISPs heeft als beleid om actief met de ACM in gesprek te gaan wanneer er twijfel is over voorliggende cases. Dit is ook al gebeurd. De andere ISPs hebben dit beleid niet. De ACM wil alle ISPs graag aanmoedigen om bij twijfel over nieuwe producten of maatregelen contact te zoeken.

Apparatuur en software ingekocht van derden
Wanneer ISPs producten kopen van aanbieders die ook buiten de EU opereren, bestaat de zorg dat deze niet voldoen aan de OI Verordening. Alle ISPs geven aan dat wanneer zij apparatuur of software inkopen voor verkeersmanagement zij zeer nauw betrokken zijn bij de implementatie daarvan. Er zijn altijd mogelijkheden om bepaalde functies wel of niet te activeren. Zo zorgen ISPs dat wordt voldaan aan de OI Verordening, ook wanneer zij werken met een product dat dingen kan die hieronder niet zijn toegestaan.

Wholesale afnemers en verkeersmanagement
Wholesale afnemers hebben bij alle ISPs de keuze of zij verkeersmanagement zelf willen doen, of dit als dienst willen afnemen bij de netwerkeigenaar. De netwerkeigenaar doet wel controles aan de randen van het netwerk, omdat de netwerkeigenaar verantwoordelijk wordt gehouden wanneer verkeer met veiligheidsrisico's zijn netwerk verlaat.

7 Vragen om te stellen bij beoordelen van TM praktijken

In hoofdstukken 2 tot en met 6 is besproken wat TM is, wat er op dit gebied wel en niet mag volgens de Open Internet Verordening, welke voorbeelden er bekend zijn bij de ACM en BEREC en hoe deze worden beoordeeld op basis van de Verordening. Dit hoofdstuk brengt al deze informatie bij elkaar in een lijst onderzoeksvragen die gebruikt kan worden bij de beoordeling van een traffic management maatregel. Dat kan zowel zijn wanneer een ISP met de ACM in gesprek gaat over een maatregel, als wanneer een maatregel formeel beoordeeld wordt. De Verordening en de Guidelines blijven leidend, en deze lijst is een overzichtelijke set vragen om de beoordeling mee te starten.

1. Wordt er verkeer anders behandeld, en hoe? Denk aan:
    - Een hoger kwaliteitsniveau geven, bijvoorbeeld door prioritering/voorrang;
    - Blokkeren of vertragen;
    - Onderweg aanpassen, bijvoorbeeld de resolutie verlagen (lossless compressie hoeft geen probleem te zijn);
    - Andere tarieven, zoals zero rating.

In de eerste drie gevallen kan het om technische discriminatie gaan. Dat kan in bepaalde gevallen gerechtvaardigd worden. Om dit te beoordelen, gebruik je vragen 2 t/m 5. Vragen 5 en 6 zijn om zero rating aanbiedingen te beoordelen.

2. Welk verkeer wordt beïnvloed?
    - Al het verkeer van één gebruiker. Als de bundel van een gebruiker op is, mag zijn snelheid verlaagd worden of de internettoegang afgesloten. Als een provider premium abonnementen aanbiedt die voorrang hebben op normale abonnementen hoeft dit geen probleem te zijn, zolang het in ieder geval om ál het verkeer binnen dat abonnement gaat.
    - Een deel van het verkeer van één gebruiker. Ga verder met de volgende vragen om dit te beoordelen.

3. Waar wordt de verkeersstroom beïnvloed?

End point based congestion control, die in de eindapparatuur van de gebruiker plaatsvindt, is niet in strijd met de Verordening. Dit staat in randnummer 54 van de Guidelines.

4. Waarom beïnvloedt de ISP dit verkeer? Voor de volgende situaties zijn er uitzonderingen:
    - Om te voldoen aan wetgeving of gerechtelijke uitspraken.
    - Om de integriteit en veiligheid van het netwerk, de diensten erop en de eindapparatuur van gebruikers te beschermen.
    - Om met uitzonderlijke of tijdelijke netwerkcongestie om te gaan;
    - Om te garanderen dat een specifieke dienst die speciale technische vereisten heeft blijft/kan werken (specialized service).

Past de reden waarom het verkeer wordt beïnvloed niet in een van de categorieën onder vraag 4? Dan is er geen uitzondering op het verbod op technische discriminatie, en mag het dus niet. Als het wel om een van deze redenen gaat, moet nog beoordeeld worden of de maatregel wel redelijk is. Kijk daarvoor in hoofdstuk 3.2.1 van dit document, en gebruik de OI Verordening en de BEREC Guidelines.

5. Hoe wordt het relevante verkeer herkend?

Het is belangrijk om dit heel duidelijk te krijgen. De Verordening schrijft voor dat er geen specifieke content gemonitord mag worden. Er mag dus in ieder geval geen deep packet inspection plaatsvinden. Als informatie van het pakketje zelf wordt gebruikt, mag alleen de *header* daarvoor ingezet worden, er

mag niet dieper worden gekeken. Het IP adres mag bijvoorbeeld wel, de (volledige) URL niet. Er worden regelmatig nieuwe manieren bedacht om verkeer te kunnen herkennen. De ACM deelt kennis hierover actief binnen BEREC.

6. Wat doet de tarifering met de keuzevrijheid van de gebruiker?
    - Hoe wordt bepaald welke apps onder het speciale tarief vallen? Als app-eigenaren zich kunnen aanmelden en er geen hoge drempel bestaat, is de drempel lager dan wanneer de ISP zelf selecteert.
    - Hoe veel ruimte heeft de gebruiker om gebruik te maken van apps die niet onder het speciale tarief vallen? Als de algemene bundel groot is, is er minder snel een probleem op dit gebied dan wanneer de algemene bundel klein is.
    - Wat gebeurt er met de toegang tot het zero rated verkeer als de algemene bundel op is? Als de algemene bundel op is, mag toegang tot het speciaal geprijsde verkeer niet doorlopen.
    - Zijn er nog andere voorwaarden verbonden aan het speciaal geprijsde verkeer? Een Fair Use Policy met een maximale hoeveelheid totaal verbruik hoeft geen probleem te zijn, maar bijvoorbeeld onbeperkt video kijken op voorwaarde dat de ISP de resolutie mag verlagen, of beperkingen op het gebied van tethering zijn niet toegestaan.
    - Hoe wordt aan de gebruiker duidelijk gemaakt wat wél binnen het speciale tarief valt en wat niet? Dit moet transparant zijn.

Kijk ook in de Annex van de vernieuwde Guidelines om dit goed te beoordelen.