ANCOM
Autoritatea Naţională pentru Administrare şi Reglementare în Comunicaţii

Str. Delea Nouă nr.2, Sector 3, 030925 Bucureşti, România
Telefon: 0372 845 400 / 0372 845 454. Fax: 0372 845 402
E-mail: ancom@ancom.org.ro. Website: www.ancom.org.ro

Raport privind neutralitatea reţelelor

1. Aspecte generale şi cadrul de reglementare

Neutralitatea rețelelor este un subiect care a stârnit reacții și dezbateri aprinse în întreaga lume, mai ales în ultimii ani. Deși nu există o definiție universal valabilă a **neutralității rețelelor,** în documentele întocmite de BEREC[1] acest concept se bazează pe principiul conform căruia toate comunicațiile electronice transmise prin intermediul unei rețele trebuie tratate în mod egal, indiferent de conținut, aplicații, tehnologie, serviciu, echipament (dispozitiv), expeditor sau destinatar. Expeditorul și destinatarul se referă la furnizorul de serviciu/conținut/aplicație și la utilizatorul final.

Esența neutralității rețelelor și aspectele care stau la baza dezbaterii vizează în principal modalitățile optime de a păstra caracterul deschis al rețelei internet, de a asigura în continuare furnizarea serviciilor de înaltă calitate pentru toți și de a asigura dezvoltarea inovațiilor, contribuind în același timp la respectarea și fructificarea drepturilor fundamentale, precum libertatea de exprimare și libertatea de a desfășura o activitate comercială.

BEREC definește **internetul** ca fiind rețeaua publică de comunicații electronice, formată din rețele care utilizează protocolul IP[2] pentru a comunica cu punctele terminale accesibile folosind o adresă globală unică în internet.

Multe dintre dezbaterile[3] pe tema neutralității rețelelor sunt centrate pe *gestionarea traficului*[4] și pe ce anume constituie un management rezonabil al traficului. Este unanim acceptat faptul că operatorii de rețea trebuie și pot să adopte unele practici de gestionare a traficului în scopul de a asigura o utilizare eficientă a rețelei și că anumite servicii furnizate pe suport IP, cum ar fi, de exemplu, serviciul IPTV[5] și serviciul de video conferință, pentru a asigura o calitate predefinită a serviciului, pot necesita o gestionare mai restrictivă a traficului – servicii specializate sau gestionate[6]. Pe de altă parte, unii operatori practică managementul traficului pentru blocarea sau degradarea anumitor servicii (de ex. VoIP) care concurează cu propriile servicii. Această practică poate fi considerată în contradicție cu caracterul deschis al internetului. Transparența este, de asemenea, o parte esențială în dezbaterea privind neutralitatea rețelelor. Dispunând de informații adecvate asupra unor posibile limitări sau informații privind managementul traficului practicat de furnizori, consumatorii pot face alegeri în cunoștință de cauză. Una dintre concluziile extrase de BEREC, în urma dezbaterilor pe tema neutralității rețelelor este că transparența este primul pas pentru asigurarea neutralității rețelelor, având drept scop stimularea competiției prin educarea utilizatorului final. Acest pas trebuie efectuat înainte de a avea în vedere alte forme de intervenție cu caracter de reglementare. Cu toate acestea, în Ghidul său privind Transparența în domeniul neutralității internetului[7], BEREC a observat că efectele unei politici de

[1] Organismul autorităţilor europene de reglementare în domeniul comunicaţiilor electronice
[2] Internet Protocol
[3] ANCOM are o participare activă în cadrul întregului grup de experți în cadrul BEREC, inclusiv în grupul de lucru privind neutralitatea rețelelor.
[4] Managementul traficului (Traffic Management)
[5] Internet Protocol television
[6] Specialized services/managed services
[7] http://berec.europa.eu/doc/berec/bor/bor11_67_transparencyguide.pdf

transparență pot fi insuficiente, mai ales în cazurile în care concurența dintre furnizori nu este eficientă și unde schimbarea furnizorului de servicii este îngreunată. De asemenea, chiar dacă ar exista concurență eficientă și furnizorul ar putea fi schimbat ușor, BEREC a arătat că tot rămâne o posibilitate ca nivelul calității serviciului de acces la internet oferit utilizatorilor finali să fie necorespunzător.

Astfel, pentru a avea o imagine completă asupra conceptului de neutralitate, trebuie analizate aspecte precum: transparența, calitatea serviciilor și gestionarea traficului (inclusiv blocarea și degradarea traficului).

La nivel legislativ, dezbaterile pe tema neutralității rețelelor purtate în ultimii ani au condus la modificări[8] importante în ceea ce privește cadrul de reglementare din domeniul comunicațiilor electronice în Uniunea Europeană. Astfel, modificarea pachetului telecom din anul 2009 urmărește promovarea concurenței și stabilirea neutralității rețelelor ca obiectiv de strategie generală a autorităților de reglementare (prin îmbunătățirea condițiilor în care utilizatorii pot schimba furnizorul de servicii, respectiv prin impunerea în sarcina furnizorilor de servicii de comunicații electronice destinate publicului a anumitor obligații de transparență în ce privește tehnicile de gestionare a traficului și calitatea serviciului de acces la internet).

În cele ce urmează, vor fi evidențiate principalele prevederi ale Directivelor revizuite în anul 2009 (*Framework Directive*[9] și *Universal Service Directive*[10]), care reglementează domeniul comunicațiilor electronice și care stau la baza documentelor, studiilor și a ghidurilor elaborate de BEREC în scopul atingerii obiectivului neutralității rețelelor.

Directiva revizuită privind serviciul universal si drepturile utilizatorilor cu privire la rețelele și serviciile de comunicatii electronice cuprinde prevederi referitoare la niveluri minime ale calității serviciilor, precum și obligații concrete de transparență în ceea ce privește limitările accesului și/sau ale utilizării serviciilor și aplicațiilor. Astfel:

- **Art. 20 alin. (1) lit. (b)** stabilește **obligația furnizorilor de servicii de comunicații electronice destinate publicului de a include în contractele încheiate cu utilizatorii finali** anumite categorii de informații, precum:
  - ✓ Informații referitoare la orice condiții care limitează accesul și/sau utilizarea serviciilor și aplicațiilor;
  - ✓ Nivelurile minime de calitate oferite de furnizorii de acces la internet;
  - ✓ Orice proceduri stabilite de furnizorii de acces la internet în scopul măsurării și modelării traficului în așa fel încât să se evite utilizarea conexiunii la capacitate maximă sau aglomerarea acesteia, precum și informații cu privire la modul în care aceste proceduri ar putea influența calitatea serviciilor;
  - ✓ Orice restricții impuse de furnizor privind utilizarea echipamentului terminal utilizat.
- Paragraful 2 al aceluiași articol acordă abonaților dreptul de a renunța la contract fără penalități, în cazul în care furnizorul serviciului de acces la internet notifică schimbări privind condițiile contractuale referitoare la categoriile de informații menționate mai sus.
- **Art. 21 alin. (3) și art. 22 alin. (3)** prevăd, printre altele, o serie de **obligații pe care autoritățile naționale de reglementare le pot impune în sarcina furnizorilor de servicii de comunicații electronice destinate publicului**, cum ar fi:

---

[8] **Directiva 2009/136/CE** a Parlamentului European și a Consiliului din 25 noiembrie 2009 de modificare a Directivei 2002/22/CE privind serviciul universal și drepturile utilizatorilor cu privire la rețelele și serviciile de comunicații electronice, a Directivei 2002/58/CE privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice și a Regulamentului (CE) nr. 2006/2004 privind cooperarea dintre autoritățile naționale însărcinate să asigure aplicarea legislației în materie de protecție a consumatorului şi **Directiva 2009/140/CE** a Parlamentului European și a Consiliului din 25 noiembrie 2009 de modificare a Directivelor 2002/21/CE privind un cadru de reglementare comun pentru rețelele și serviciile de comunicații electronice, 2002/19/CE privind accesul la rețelele de comunicații electronice și la infrastructura asociată, precum și interconectarea acestora și 2002/20/CE privind autorizarea rețelelor și serviciilor de comunicații electronice ;

[9] **Directiva 2002/21/CE (FD)**: http://www.ancom.org.ro/uploads/links_files/32002L0021_EN.pdf

[10] **Directiva 2002/22/CE (USD)** : http://www.ancom.org.ro/uploads/links_files/32002L0022_EN.pdf

- ✓ Obligația de a informa abonații cu privire la orice schimbare a condițiilor care limitează accesul la servicii și aplicații și/sau utilizarea acestora, atunci când aceste condiții sunt permise de legislația națională;
- ✓ Obligația de a furniza informații cu privire la orice proceduri aplicate de furnizor pentru măsurarea și modelarea traficului în așa fel încât să se evite utilizarea conexiunii la capacitate maximă sau aglomerarea acesteia, precum și la modul în care aceste proceduri ar putea influența calitatea serviciului;
- ✓ Obligația de a respecta anumiți parametri de calitate.

- **Art. 22** se referă la **calitatea serviciului** și conform acestui articol:
  - ✓ Autoritățile naționale de reglementare pot solicita furnizorilor de servicii de comunicații electronice destinate publicului să publice pentru utilizatorii finali, informații comparabile, adecvate și actualizate privind calitatea serviciilor acestora;
  - ✓ Autoritățile naționale de reglementare pot specifica, *inter alia*, indicatorii care trebuie măsurați cu privire la calitatea serviciilor, precum și conținutul, forma și metoda de publicare a informațiilor.

Directiva cadru revizuită stabilește obligația autorităților de reglementare de a promova capacitatea utilizatorilor finali de a accesa și distribui orice informații sau utiliza aplicații și servicii la alegerea acestora (Art. 8 alin. (4) lit. g). De asemenea autoritățile de reglementare au și alte obiective, care ar trebui avute în vedere, precum:

- promovarea concurenței în furnizarea rețelelor și a serviciilor de comunicații electronice (Art. 8 alin. (2));
- promovarea investițiilor eficiente și a inovațiilor în infrastructuri noi și consolidate (Art. 8 alin. (5)).

Directivele Europene au fost transpuse în legislația românească prin **Ordonanța de Urgență a Guvernului nr. 111/2012**, privind comunicațiile electronice, aprobată, cu modificări și completări, prin Legea nr. 140/2012, care reglementează, printre altele, drepturile și obligațiile furnizorilor de rețele și de servicii de comunicații electronice, precum și drepturile utilizatorilor finali, după cum urmează:

- **Art. 12 alin. (1)** prevede dreptul oricărui operator al unei rețele publice de comunicații electronice de a negocia cu un altul un acord de interconectare (lit. a)), dar și obligația de negociere a unui astfel de acord, la solicitarea unui terț (lit. b));
- **Conform art. 51 alin. (2),** contractele încheiate cu utilizatorii trebuie să conțină *într-o formă clară, inteligibilă și ușor accesibilă*, cel puțin clauze minime privind orice alte condiții care limitează accesul sau utilizarea anumitor servicii și aplicații (lit. b), informații privind *nivelurile minime de calitate a serviciilor oferite* (lit.c) și informații privind *procedurile de măsurare și gestionare a traficului în scopul de a evita congestionarea segmentelor de rețea sau utilizarea acestora la capacitate maximă, precum și privind impactul acestor proceduri asupra calității serviciului* (lit.d)*;*
- **Conform art. 60 alin. (1)** *Furnizorii de rețele publice de comunicații electronice și furnizorii de servicii de comunicații electronice destinate publicului au obligația de a pune la dispoziția publicului* ***informații transparente, comparabile, adecvate și actualizate privind prețurile și tarifele aplicabile****, sumele percepute la momentul încetării contractului, dacă este cazul, precum și celelalte condiții privind accesul la serviciile oferite și utilizarea acestora, pentru a asigura posibilitatea utilizatorilor finali de a decide în cunoștință de cauză.*
- **Conform art. 61 alin. (4)**, *pentru a preveni degradarea serviciului și obstrucționarea sau încetinirea traficului în rețele,* ***ANCOM poate impune*** *furnizorilor de rețele publice de comunicații electronice și furnizorilor de servicii de comunicații electronice destinate publicului* ***un set minim de cerințe privind calitatea serviciului.***

De asemenea, **Decizia președintelui ANCOM nr. 1201/2011** privind stabilirea indicatorilor de calitate pentru furnizarea serviciului de acces la internet și publicarea parametrilor aferenți cuprinde prevederi referitoare la asigurarea transparenței în ceea ce privește calitatea serviciilor oferite, prin impunerea în sarcina furnizorilor de comunicații electronice care oferă servicii de acces la internet a

obligației de a publica pe paginile proprii de internet valorile parametrilor aferenți indicatorilor de calitate administrativi (art. 2 lit.a)).

Prin art. 5 al aceleiași decizii, ANCOM poate să realizeze, să administreze și să pună la dispoziția publicului o aplicație interactivă prin intermediul căreia se pot măsura indicatorii tehnici de calitate, urmând ca valorile măsurate să fie publicate pe pagina de internet ANCOM.

După mai mulți ani de activitate desfășurată în scopul atingerii obiectivului care vizează neutralitatea rețelelor, BEREC a publicat o serie de documente, inclusiv concluzii ce privesc piața comunicațiilor electronice și ghiduri având mai multe subiecte-cheie legate de neutralitatea rețelelor, astfel[11]:

- Răspunsul BEREC la consultarea publică lansată de Comisia Europeană referitoare la neutralitatea internetului *(BEREC's Response to the European Commission's consultation on the open Internet and net neutrality in Europe*[12] *-September 2010*);

    - Acest document este prima prezentare a subiectelor legate de neutralitate. BEREC conclude că actualul cadru de reglementare (inclusiv noile prevederi care consolidează transparența și care permit impunerea unor cerințe minime de calitate a serviciului) este probabil suficient pentru a aborda multe din preocupările exprimate în contextul neutralității rețelelor.

- Ghidul BEREC privind transparența și neutralitatea rețelelor – "Transparența & NN" *(Guidelines on Transparency in the scope of Net Neutrality: best practices and recommended approaches*[13] - December 2011)

    - Transparența față de practicile de gestionare a traficului este elementul cheie în atingerea obiectivului de neutralitate a internetului stabilit de Directivele revizuite în anul 2009, împreună cu existența unei concurențe eficiente și capacitatea utilizatorilor finali de a schimba furnizorul de servicii de comunicații electronice. De asemenea, transparența poate stimula și concurența dintre furnizori, îmbunătățind în același timp gradul de informare a utilizatorilor finali. Ghidul analizează modul în care noile obligații de transparență ar trebui să fie puse în practică de autoritățile naționale de reglementare și de furnizorii de servicii de comunicaţii electronice destinate publicului. Sunt stabilite tipurile de informații care trebuie puse la dispoziția publicului, modul în care ar trebui transmise și ce organisme ar trebui implicate. De asemenea, sunt descrise cerințele necesare pentru ca politica de transparență să fie eficientă.

- Raportul BEREC privind cadrul pentru calitatea serviciilor în contextul neutralității rețelelor *(A framework for Quality of Service in the scope of Net Neutrality*[14] -December 2011)

    - Acest document stabilește bazele definirii de către autoritățile naționale de reglementare a calității serviciului în raport cu neutralitatea rețelelor, elaborând concepte legate de calitate, relevante pentru rețelele IP și metode de evaluare a calității în internet.

---

[11] *Summary of BEREC positions on net neutrality*
http://berec.europa.eu/files/document_register_store/2012/12/BoR_(12)_146_Summary_of_BEREC_positions_on_net_neutrality2.pdf

[12] Versiunea integrală a documentului este disponibilă la următoarea adresă:
http://www.irg.eu/streaming/BoR%20(10)%2042%20BEREC%20response_ECconsultation_Net%20neutrality_final.pdf?contentId=546969&field=ATTACHED_FILE

[13] Versiunea integrală a documentului este disponibilă la următoarea adresă:
http://berec.europa.eu/doc/berec/bor/bor11_67_transparencyguide.pdf

[14] Versiunea integrală a documentului este disponibilă la următoarea adresă:
http://berec.europa.eu/doc/berec/bor/bor11_53_qualityservice.pdf

- Investigația asupra managementului traficului în Uniunea Europeană lansată la invitația Comisiei Europene *(BEREC findings on Traffic management and other practices resulting in restrictions to the open Internet in Europe*[15] -May 2012)

    - La invitația Comisiei Europene, BEREC a inițiat o investigație în privința practicilor de gestionare a traficului aplicate în prezent în Uniunea Europeană. Potrivit rezultatelor acestei investigații, majoritatea ISPs (Internet Service Providers- furnizori de serviciu de internet) nu oferă serviciu de acces la internet cu restricții, în funcție de tipul aplicațiilor. Dar anumite practici, cum ar fi blocarea sau limitarea traficului peer-to peer sau VoIP, pot crea probleme pentru utilizatorii finali. Din investigație a rezultat că acestea apar mai des în rețelele mobile decât în cele fixe. Mai mult decât atât, datele colectate arată diferențe semnificative între practicile aplicate în diferite state.

- Raportul BEREC denumit în continuare "Aspecte privind concurența în contextul neutralității rețelelor" *(Report on differentiation practices and related competition issues in the context of Net Neutrality*[16] -December 2012)

    - Raportul privind practicile diferențiate și aspecte legate de concurență în contextul neutralității rețelelor furnizează un cadru de analiză al efectelor pe care practicile diferențiate (ca blocarea sau prioritizarea traficului) le pot avea asupra concurenței și inovației. Sunt analizate diverse practici de diferențiere aplicate serviciului de acces la internet și se examinează măsura în care acestea pot aduce prejudicii intereselor utilizatorilor finali și pot avea un efect negativ atât asupra pieței de comunicații electronice, cât și asupra pieței de conținut și aplicații.

- Documentul privind analiza interconectării IP în contextul neutralității internetului *(An assessment of IP interconnection in the context of Net Neutrality*[17] -December 2012)

    - Raportul oferă o imagine despre piața interconectării IP și relațiile economice dintre ISPs și alți intermediari în lanțul de valori al internetului. Se analizează dacă abaterile de la principiul neutralității rețelelor pot sau nu să fie reflectate la nivel de interconectare și sunt amintite aspecte legate de reglementare.

- Ghidul BEREC privind calitatea serviciilor în contextul neutralității internetului *(Guidelines for Quality of Service in the scope of Net Neutrality*[18] -December 2012)

    - Ghidul privind calitatea serviciului în scopul neutralității rețelelor oferă o direcție pentru autoritățile naționale de reglementare (NRA[19]) în scopul exercitării puterii de a impune operatorilor cerințe minime a calității serviciului pentru a preveni degradarea serviciului.

---

[15] Versiunea integrală a documentului este disponibilă la următoarea adresă: http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/45-berec-findings-on-traffic-management-practices-in-europe

[16] Versiunea integrală a documentului este disponibilă la următoarea adresă: http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/?doc=1094

[17] Versiunea integrală a documentului este disponibilă la următoarea adresă: http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/1130-an-assessment-of-ip-interconnection-in-the-context-of-net-neutrality

[18] Versiunea integrală a documentului este disponibilă la următoarea adresă: http://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/1101-berec-guidelines-for-quality-of-service-in-the-scope-of-net-neutrality

[19] National Regulatory Authority

În cadrul activității privind neutralitatea rețelelor, BEREC a identificat mai multe direcții de acțiune, care au fost dezvoltate de-a lungul anilor în documentele mai sus amintite și care se referă la:

- Practici de gestionare a traficului
- Calitatea serviciului
- Transparență
- Aspecte privind competiția și
- Interconectarea IP

1. Practici de management al traficului

Având în vedere importanța pe care o are managementul traficului în cadrul neutralității rețelelor, vom prezenta în continuare o descriere a principalelor aspecte legate de acest subiect.

În cadrul răspunsului BEREC la chestionarul Comisiei Europene privind anumite aspecte care țin de transparență, gestionarea traficului și schimbarea furnizorului de serviciu (documentului BoR[20](12)145, publicat în decembrie 2012), este abordat subiectul managementului traficului, fiind prezentate, printre altele, aspecte legate de **tehnicile de management al traficului precum și cazurile în care aplicarea acestora este necesară, potrivită sau problematică**. Acest capitol își propune tocmai clarificarea aspectelor mai sus amintite. De asemenea, în tratarea acestor subiecte, am ținut cont și de investigația realizată de BEREC în 2012 (*BEREC findings on Traffic management and other practices resulting in restrictions to the open Internet in Europe*), la cererea Comisiei Europene, în scopul de a obține cât mai multe informații de pe piață cu privire la blocarea aplicațiilor, limitarea și degradarea traficului. Acest chestionar a urmărit identificarea practicilor de management al traficului, care includ atât măsurile care țin cont de tipul de trafic sau identitatea transmițătorului sau destinatarului (*application-specific TM*), cât și măsurile care nu depind de tipul aplicației (*application-agnostic TM*).

În cadrul documentațiilor studiate (vezi Bibliografie), există mai multe definiții pentru conceptul de management al traficului, anume:

- *Managementul traficului este termenul folosit pentru a descrie o serie de practici tehnice întreprinse în scopul de a gestiona traficul în rețea. Aceste practici sunt folosite ulterior pentru a furniza și pentru a menține o anumită experiență pentru utilizatori. Odată cu creșterea volumelor de trafic, tehnicile de management al traficului ajută la utilizarea eficientă a rețelelor și îmbunătățirea experienței utilizatorului.* (*Voluntary industry code of practice on traffic management transparency for broadband services*-OFCOM)
- *Managementul traficului se aplică pentru a implementa o varietate de funcții, la mai multe nivele, de către mai mulți actori, în numeroase moduri pentru mai multe scopuri. Pentru a delimita aceste componente, se definește termenul de tehnici de management ca fiind o anumită funcție aplicată la un anumit nivel. De asemenea, se definește noțiunea de practici de management al traficului ca fiind o serie de tehnici de management al traficului utilizate de un anumit tip de actor, într-un mod specific, pentru un anumit scop.*(*How to determine whether a traffic management practice is reasonable*- Scott Jordan)
- *Managementul traficului este procesul de prioritizare, shaping și rutare a traficului în rețea în scopul de a asigura funcționalitatea aplicațiilor critice. O abordare completă a managementului traficului cuprinde o încărcare echilibrată, adaptarea vitezei și alte măsuri pentru a asigura calitatea serviciului și disponibilitatea rețelei.* (http://www.f5.com/glossary/traffic-management/)

[20] Versiunea integrală a documentului este disponibilă la următoarea adresă: http://berec.europa.eu/eng/document_register/subject_matter/berec/opinions/1145-berec-response-to-ec-questionnaire-on-specific-aspects-of-transparency-traffic-management-and-switching-in-an-open-internet

- *Termenul de trafic management se referă la o serie de diferite tehnici pe care operatorii de rețea și ISPs le utilizează fie pentru a restricționa traficul, fie pentru a da prioritate unui anumit tip de trafic în detrimentul altuia.* (AGCOM)
- *Managementul traficului într-o rețea reprezintă o serie de tehnici care pot fi folosite de furnizorii de servicii de internet în scopul de a atinge performanțe optime pentru diverse clase de utilizatori. Aceste tehnici includ utilizarea unor măsuri de performanță pentru a defini nivelurile de servicii adaptate la diferitele cerințe ale utilizatorilor și pentru a asigura calitatea serviciului.(Network traffic management and the evolving internet- IEEE[21] 2010)*

Având în vedere multitudinea de elemente care se regăsesc sub conceptul de management al traficului vom porni de la o definiție simplă: **Managementul traficului este termenul folosit pentru a descrie o serie de practici tehnice[22] întreprinse în scopul de a gestiona traficul în rețea**, urmând ca în continuarea capitolului să detaliem aceste practici tehnice în funcție de locul unde se pot aplica, tipurile de practici și scopul în care sunt aplicate.

2.1 Tehnici de gestionare a traficului

Conform BEREC, tehnicile de managementul traficului pot fi clasificate în funcție de nivelul, respectiv nodul de rețea la care sunt aplicate, variind de la nodurile interne de rețea la cele externe și de la nivelul rețea la cel de aplicație. De precizat că în acest caz ne referim la cele două nivele (rețea, respectiv aplicație), ca făcând parte din sistemul de referință propus de BEREC în cadrul documentului *A framework for Quality of Service in the scope of Net Neutrality*[23]. Acest document prevede simplificarea modelului de referință TCP/IP format din 4 nivele în modelul format din cele două nivele. Astfel, nivelul aplicație/conținut include în acest model simplificat nivelele superioare de aplicație și transport ale modelului TCP/IP, iar nivelul rețea din cadrul modelului simplificat include nivelele internet și conexiune (care de asemenea se poate împărți în subnivelele legătură de date și fizic) corespunzătoare modelului TCP/IP.

Astfel că sunt amintite trei categorii de management al traficului:

1) Tehnici executate la nivelul rețea,
2) Tehnici executate la nivelul aplicație, în punctele terminale (de exemplu: echipamentele terminale ale utilizatorului și servere),
3) Tehnici executate la nivelul aplicație în nodurile interne ale rețelei.

Acestea sunt ilustrate în figura de mai jos, conform documentului BEREC, menționat anterior.

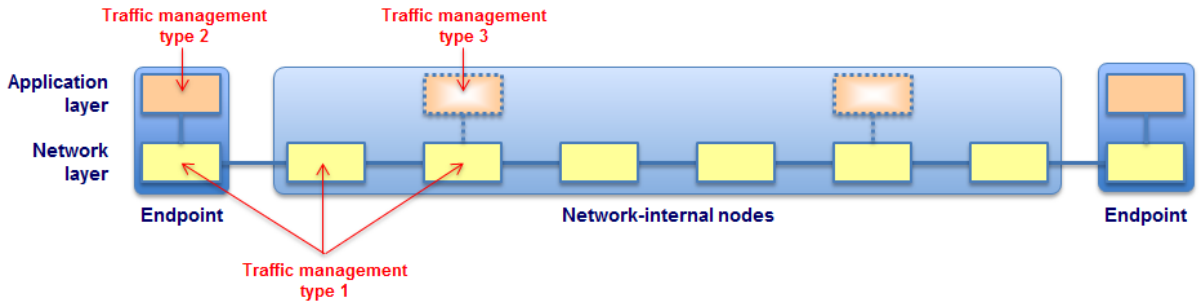

Fig.1 Ilustrarea categoriilor de tehnici de management al traficului

1) Primul tip de management al traficului (type 1) se efectuează la nivelul rețea și include funcții care realizează rutarea și retransmiterea (forwarding) pachetelor IP individuale prin intermediul

[21] Institute of Electrical and Electronics Engineers
[22] în cursul documentului se va folosi si termenul de tehnici de management al traficului având acelaşi înţeles
[23] http://berec.europa.eu/doc/berec/bor/bor11_53_qualityservice.pdf

diferitelor legături disponibile în rețea folosind adresa de destinație sau alte informații similare existente în header-ul pachetului IP.

Rutarea este procesul de selectare a celei mai bune căi pe care poate fi transportat un pachet IP într-o rețea. **Retransmiterea** pachetelor (fowarding) reprezintă procesul de transmitere a pachetelor spre destinație pe baza informației de rutare. Protocolul folosit pentru rutare în cadrul unei rețele este OSPF (Open Shortest Path First), protocol bazat pe calea cea mai scurtă. Pentru rutarea pachetelor între rețele se folosește protocolul BGP (Border Gateway Protocol). În procesul de rutare, pachetele care sunt transmise mai departe traversează noduri intermediare. Acestea constau în echipamente de rețea, precum routere, punți (bridges), porți (gateways), firewalls sau switch-uri. De obicei, alegerea căii optime pe care va fi transmis pachetul, se face ținând cont de tabelele de rutare, care sunt stocate în memoria routerelor și care conțin căile posibile către diferite destinații în rețea.

În cadrul procesului de rutare a traficului în rețea, furnizorii de servicii de internet pot utiliza și mecanisme MPLS (Multi Protocol Label Switching). Prin intermediul acestui protocol, pachetele sunt direcționate în rețea în funcție de o etichetă atribuită, care este asociată cu o cale predeterminată în rețea. Rutarea bazată pe MPLS permite ca anumitor fluxuri de date să le fie atribuite diferite caracteristici QoS și priorități. Practic, pachetele sunt mai întâi examinate, clasificate, după care li se atribuie o etichetă corespunzătoare și sunt transmise mai departe, iar pe măsură ce parcurg calea, fiecare router întâlnit folosește această etichetă (și nu altă informație, cum ar fi header-ul IP) pentru a lua decizia de transmitere mai departe.

În plus, acest tip de management al traficului (type 1) poate să conțină și **funcții de management al congestiei** care nu depind de tipul aplicației (application agnostic) și care vin în scopul susținerii controlului congestiei în punctele terminale.

Funcțiile de managementul congestiei permit controlul congestiei prin stabilirea ordinii în care sunt transmise pachetele mai departe, în funcție de gradul lor de prioritate. Managementul congestiei implică crearea cozilor de așteptare, introducerea (adăugarea) pachetelor în aceste cozi și programarea pachetelor în vederea transmiterii lor mai departe. Atunci când nu există congestie, pachetele sunt transmise pe măsură ce sosesc. În cazul în care există congestie, pachetele sosesc mai repede decât pot fi preluate pentru a fi transmise mai departe, însă, folosind funcțiile de managementul congestiei, pachetele sunt puse într-o coadă de așteptare până când pot fi transmise, fiind programate în funcție de gradul de prioritate care le este atribuit.

Există patru tipuri de cozi de așteptare:

- FIFO (first-in, first-out), care nu implică conceptul de prioritizare sau de clase de trafic, pachetele fiind transmise mai departe pe măsură ce sosesc;
- WFQ (Weighted fair queueing)- distribuirea pachetelor în cozi de așteptare este făcută în funcție de mai mulți parametri (de exemplu, pachetele cu aceeași adresă sursă și destinație, și același port sursă și destinație);
- CQ (Custom queueing), caz în care capacitatea de transmisie este alocată proporțional pentru fiecare clasă de trafic. Practic, în cazul CQ, este specificat numărul de pachete sau de octeți care pot deservi fiecare clasă de trafic;
- PQ (priority queueing)- pachetele care aparțin unei clase prioritare de trafic sunt transmise înaintea traficului cu prioritate mai mică, în scopul de a asigura livrarea la timp a acestor pachete.

2) Al doilea tip de management al traficului (type 2) se aplică în punctele terminale, la nivelul aplicație (așa cum a fost definit în schema de mai sus) și cuprinde măsuri de **control al congestiei și codare dinamică adaptivă (dynamic adaptive coding).**

Controlul congestiei se poate realiza utilizând funcționalitățile protocolului TCP (Transport Control Protocol), care constau, printre altele, în ajustarea automată a vitezei cu care datele sunt transmise într-o rețea. Ideea care stă la baza conceptului de control al congestiei este de a controla nivelul de încărcare din rețea prin ajustarea la nivelul surselor, conform cu nivelul congestiei în rețea, a vitezei cu care sunt transmise pachetele IP. Mai exact, sursele detectează sau observă pierderi de pachete și scad rata de transmitere a pachetelor pentru a evita alte pierderi de pachete sau congestia. Dacă o sursă observă că

toate pachetele au fost transmise, va crește viteza de transmitere, pentru a folosi la maxim capacitatea rețelei. În acest fel, TCP va minimiza pierderea de pachete, folosind în mod eficient capacitatea rețelei.

În cadrul controlului congestiei, TCP folosește patru algoritmi (*slow start, congestion avoidance-evitarea congestiei, fast retransmit* și *fast recovery*) și toți acești algoritmi iau în considerare pierderea de pachete în detectarea congestiei.

- Algoritmul *slow start* asigură faptul că noile pachete de date sunt transmise în rețea cu aceeași viteză cu care sunt returnate confirmările.
- Tehnicile de evitare a congestiei (*congestion avoidance*) monitorizează încărcarea traficului în rețea în scopul de a anticipa și evita congestia. Evitarea congestiei este realizată prin eliminarea de pachete. Un astfel de mecanism de evitare a congestiei este Random Early Detection (RED), care previne încărcarea la capacitate maximă a cozilor de așteptare, prin eliminarea în mod aleator a pachetelor. RED nu deține mecanism de diferențiere între fluxurile de trafic, astfel că a devenit o metodă de control a congestiei depășită. În schimb, WRED (Weighted Random Early Detection), reprezintă un alt mecanism de evitare a congestiei, care ține cont de anumiți parametri înainte de a selecta pachetele care vor fi eliminate. În cazul WRED este mai puțin probabil ca pachetele cu prioritate mare să fie eliminate, în detrimentul celor cu prioritate mică. Altfel spus, cu cât pachetul are o prioritate mai mare, cu atât este mai probabil să fie transmis.
- Algoritmul *fast retransmit* scurtează timpul de așteptare înainte ca sursa să retransmită un segment de date pierdut. Semnalizarea pierderii de pachete se face folosind un număr prestabilit de confirmări duplicate. Cu alte cuvinte, dacă sursa primește (de exemplu) trei duplicate ale confirmării pentru aceeași secvență de date (pachetul 2, în figura de mai jos), înseamnă că în mod cert secvența imediat următoare (pachetul 3) a fost pierdută, iar sursa îl va retransmite, fără a mai aștepta expirarea timpului alocat primirii confirmării.

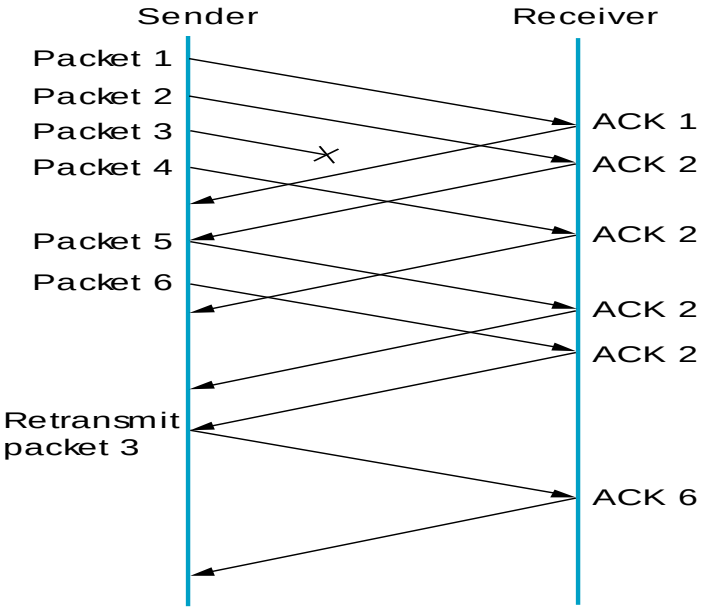

Fig.2 ***Fast Retransmit- În cazul în care numărul prestabilit de confirmări duplicate este 3***

(sursa: TCP Congestion Control- "Computer Networks A Systems Approach", Third Ed., Peterson and Davie, Morgan Kaufmann, 2003)

- Algoritmul *fast recovery* constă în activarea *congestion avoidance*, imediat ce algoritmul *fast retransmit* trimite segmentul pierdut. Motivul pentru care nu este activat *slow start*

și este preferat *congestion avoidance* este că din moment ce există un schimb de pachete între cele două părți, nu se dorește încetinirea fluxului, care s-ar produce în cazul activării *slow start*.

Codarea dinamică adaptivă este o tehnică folosită din ce în ce mai des în cazul aplicațiilor de tip media. Această tehnică permite ajustarea ratei de compresie a fluxului de date în concordanță cu capacitatea disponibilă pe legătura dintre sursă și destinație. Practic, aplicând această tehnică, pe un server sunt disponibile mai multe variante de reprezentare ale aceluiași conținut (variantele sunt caracterizate de o anumită rezoluție și viteză), utilizatorii aplicațiilor media având posibilitatea să schimbe (comute) între codările disponibile pe server, în funcție de gradul de încărcare a rețelei.

3) Cel de-al treilea tip de management al traficului (type 3) constă în tehnici executate în nodurile interne ale unei rețele, în cadrul nivelului aplicație (așa cum a fost definit în schema de mai sus). Aceste tehnici sunt implementate în noduri speciale de rețea, în echipamente precum firewalls sau gateways și presupun funcționalități superioare celor existente într-un router obișnuit. Astfel, pe baza unei politici predefinite, anumite pachete pot fi retransmise, întârziate sau aruncate/distruse.

În continuare sunt prezentate câteva dintre tehnicile de management al traficului de tip trei:

Traffic policing reprezintă un mecanism de reglare a traficului folosit pentru a limita viteza fluxurilor de trafic. Această tehnică permite controlul vitezei maxime cu care traficul este transmis sau recepționat pe o interfață. Traficul care se încadrează în parametri (respectă viteza maximă configurată) este transmis, iar cel care depășește acești parametri este distrus sau transmis cu o prioritate diferită.

Traffic shaping reprezintă o practică de modelare a transferului datelor în rețea, aplicată în scopul de a asigura un anumit nivel de performanță sau calitate a serviciului. Această tehnică constă în întârzierea fluxurilor de pachete în scopul de a controla viteza de transmisie a datelor și de a evita astfel apariția congestiei. Traffic shaping este o metodă de a modela traficul astfel încât acesta să respecte anumite reguli/politici prestabilite. De obicei, această practică se aplică traficului la ieșirea dintr-un port.

Diagrama de mai jos ilustrează elementul cheie care diferențiază cele două tipuri de practici. În cazul traffic policing, atunci când traficul atinge maximul vitezei configurate, excesul de trafic este ignorat. Spre deosebire de această practică, traffic shaping păstrează pachetele în exces într-o coadă de așteptare, urmând ca acestea să fie transmise mai târziu. În urma acestei practici viteza pachetelor va fi una atenuată.

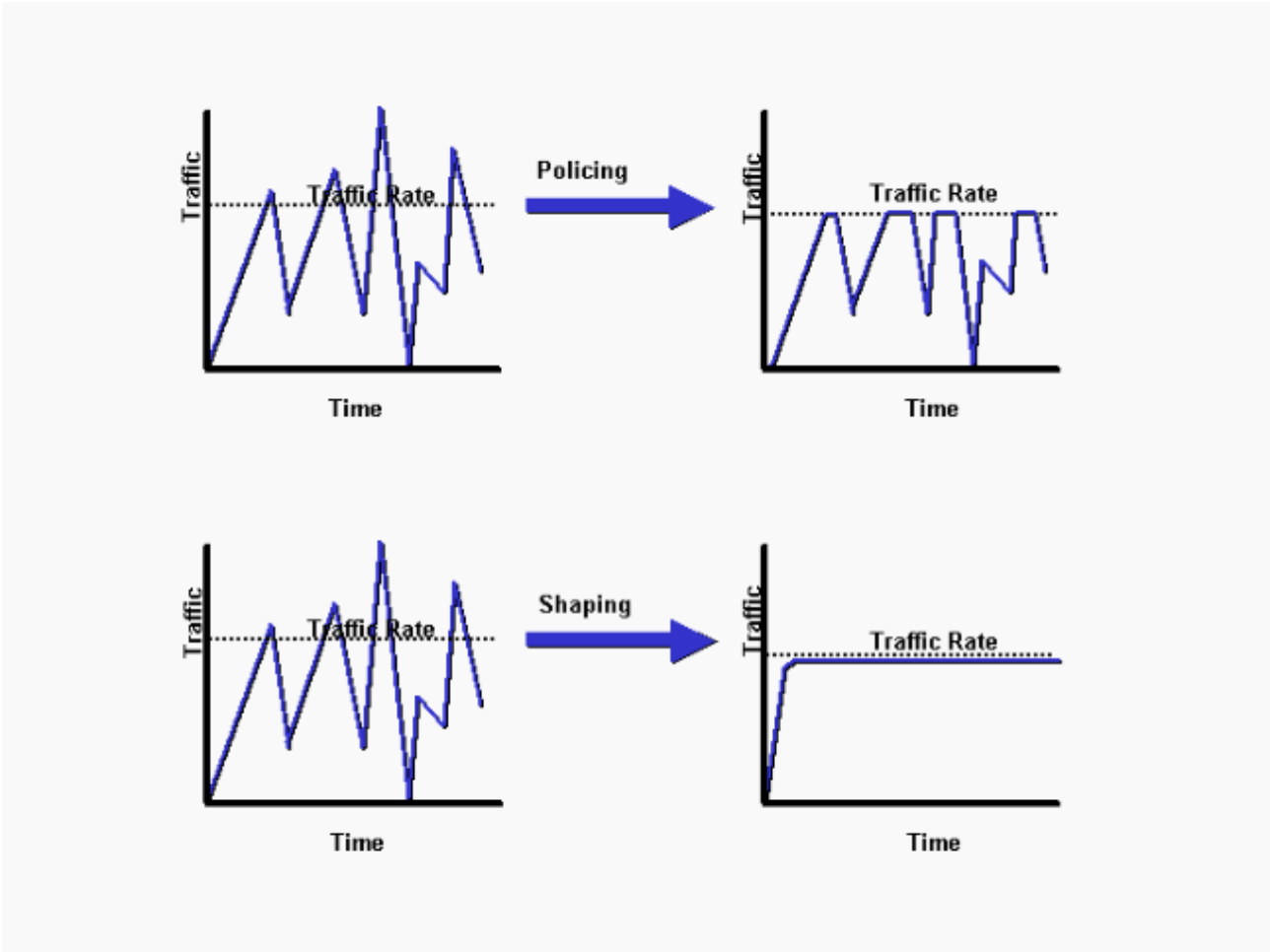

Fig.3 Comparație între practicile de traffic policing și traffic shaping

Spre deosebire de policing, noțiunea de shaping implică existența unei cozi de așteptare și memorie suficientă pentru a păstra pachetele întârziate. Pachetele care părăsesc o interfață sunt puse într-o coadă de așteptare și li se poate aplica practica de shaping. Traficul de intrare într-o interfață poate fi supus doar practicii de policing.

Clasificarea traficului (Traffic classifying) reprezintă primul pas în identificarea diferitelor aplicații și protocoale care există într-o rețea. Altfel spus, clasificarea traficului permite organizarea pachetelor IP în clase de trafic sau categorii în funcție de modul în care traficul îndeplinește anumite criterii.

Există două tipuri de abordări în clasificarea traficului:

- Clasificarea bazată pe metoda statistică
- Clasificarea în funcție de capacitatea utilă (payload based).

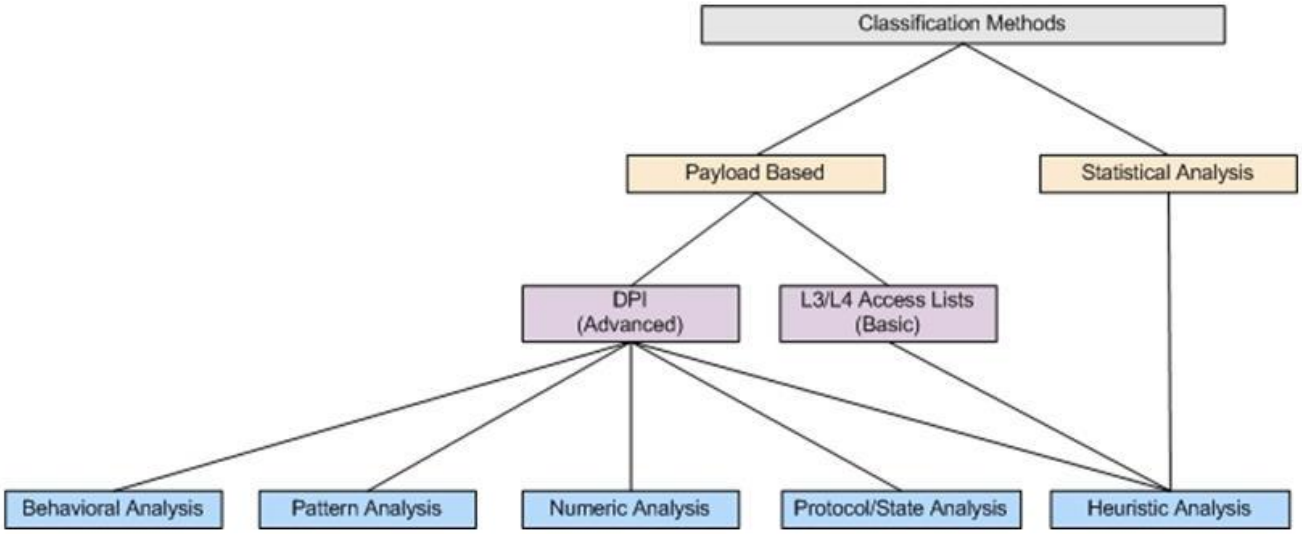

Fig.4 Metode de clasificare a traficului

Clasificarea bazată pe metoda statistică folosește analiza statistică a comportamentului traficului (cum ar fi inter-packet arrival, session time).

Clasificarea traficului, făcută în funcție de capacitatea utilă este mai des întâlnită și poate fi realizată în două moduri:

- fie printr-o analiză de bază (care utilizează informațiile din header-ul pachetului IP) – această tehnică este considerată foarte rudimentară și nu furnizează o clasificare pentru cele mai multe dintre aplicații.
- fie prin tehnici mai avansate, bazate pe DPI (Deep Packet Inspection). Pentru o clasificare corectă a traficului este necesară aplicarea acestui tip de tehnici. Inițial, aplicațiile sunt studiate din punct de vedere al caracteristicilor unice (numite Semnături), care sunt trecute într-o bază de date de referință. Pentru a identifica în mod exact o aplicație, traficul este comparat cu această referință (Analiza Semnăturilor). Acest lucru implică necesitatea actualizării bazei de date, pentru a fi la curent cu noile aplicații și cu noile dezvoltări în cadrul protocoalelor existente. Există mai multe metode de Analiză a Semnăturilor:
    - Analiza unui tipar (Pattern Analysis)- unele aplicații includ anumite tipare (octeți, caractere) în încărcătura utilă a pachetelor, care pot folosi în etapa de clasificare. Pentru aplicațiile care nu includ astfel de tipare, această metodă nu este aplicabilă.
    - Analiza numerică (Numerical analysis)- constă în căutarea în caracteristicile numerice a pachetelor (de ex. payload size, numărul de pachete de răspuns). Aplicând această metodă, decizia de clasificare poate dura un timp mai îndelungat.
    - Behavioral & Heuristic analysis- analiza comportamentului traficului poate fi concludentă în etapa de clasificare a traficului. Similar, prin realizarea unei analize euristice (heuristic analysis) a pachetelor inspectate, se poate face o clasificare a protocoalelor. Aceste tipuri de analiză merg mână în mână cu multe dintre programele anti-virus, care folosesc aceste tehnici pentru a identifica viruși și viermi.
    - Protocol/state analysis- în cazul unor aplicații, protocolul urmează o anumită secvență de pași sau acțiuni. O astfel de conformitate a protocolului poate fi folosită în clasificarea traficului.

O clasificare acceptabilă a tuturor aplicațiilor nu se poate realiza aplicând o singură metodă (oricare din cele mai sus amintite). Prin urmare, în clasificarea traficului se folosește o combinație a acestor metode. În principiu, odată ce pachetele au fost clasificate (identificate) ca aparținând unei anumite aplicații sau protocol, acestea sunt marcate.

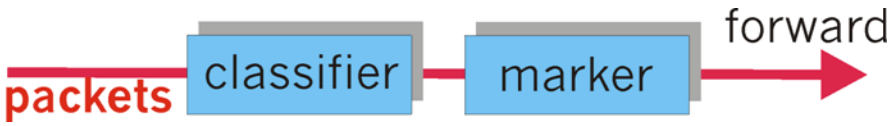

Fig.5 Succedarea etapelor de clasificare și marcare a traficului

Marcajele respective vor folosi pentru determinarea politicilor adecvate de tratare a acestor fluxuri în cadrul routerelor. Marcarea poate fi făcută în mai multe feluri, dintre care cel mai des utilizat este folosind DSCP (Differentiated Services Code Point). DSCP reprezintă un câmp în cadrul pachetului IP, care permite împărțirea traficului pe nivele diferite de calitate a serviciului. Modul în care un pachet IP este tratat depinde de valoarea reprezentată în câmpul DSCP. Facem precizarea că marcarea traficului poate fi făcută și în cadrul echipamentelor terminale ale utilizatorului final. De exemplu terminalele VoIP setează automat câmpul DSCP, astfel încât traficul să fie tratat prioritar.

Filtrarea/Blocarea se realizează prin configurarea listelor de acces (Access List), care au rolul de a preveni intrarea sau ieșirea unui anumit trafic în/din rețea. Astfel, routerul examinează fiecare pachet și în funcție de criteriile (de ex. adresa sursă sau destinație a traficului, valoarea reprezentată în câmpul DSCP) stabilite în cadrul listei de acces, se ia decizia dacă pachetele sunt transmise mai departe sau distruse.

Bandwidth throttling (conform IEEE) reprezintă o practică a ISP de a limita viteza cu care un utilizator poate uploada/downloada informații, indiferent de capacitatea resurselor disponibile în rețea (în special lățimea de bandă disponibilă).

Conform documentului BEREC privind Investigația asupra managementului traficului în Uniunea Europeană (*BEREC findings on Traffic management and other practices resulting in restrictions to the open Internet in Europe),* cele mai frecvente tehnici de management al traficului aplicate de furnizori sunt blocarea și/sau limitarea (throttling) traficului P2P în rețelele fixe și mobile și blocarea traficului VoIP, în rețelele mobile.

Atunci când rețelele IP furnizează mai multe clase de trafic sau nivele de prioritate, tipurile de management al traficului 1 și 3 sunt implicate. Mai întâi pachetele sunt repartizate în clase de trafic prin intermediul unor tehnici de management al traficului de tip 3. Apoi pachetele pot fi eliminate sau transmise în rețea folosind cozi separate de așteptare în funcție de clasele de trafic din care fac parte.

2.2 Motive pentru aplicarea tehnicilor de management al traficului

Managementul traficului poate fi efectuat din mai multe motive și poate servi unor obiective diferite. Această secțiune va descrie unele din motivele pentru care furnizorii de rețele și servicii de comunicații electronice aplică tehnicile de management al traficului.

Congestia

Evitarea congestiei este cel mai important obiectiv al managementului traficului. Congestia poate apărea din două motive: situații imprevizibile, ce au loc în mod neregulat (ca de exemplu fluctuații ale fluxului de trafic, sau în cazul unei avarii în rețea) sau situații previzibile, ce au loc în mod regulat (cum ar fi neadaptarea capacității rețelei la volumul de trafic). Efectele congestiei constau în latență crescută, pierderea de pachete sau blocarea de noi conexiuni, cu posibil impact asupra disponibilității serviciului și experienței utilizatorului.

Prin managementul traficului, un furnizor poate bloca sau limita selectiv lățimea de bandă sau volumul de trafic generat de anumite tipuri de aplicații, în scopul de a reduce congestia. În principal sunt vizate aplicațiile care consumă multă bandă, precum VoD[24] sau P2P[25]. De asemenea, furnizorul poate prioritiza un anumit tip de trafic pentru a asigura nivelul de calitate cerut pentru funcționarea

[24] Video on Demand
[25] Peer to Peer

adecvată a aplicației sau serviciului respectiv în caz de congestie. Această diferențiere poate fi aplicată (i) astfel încât să producă efecte doar în cazul în care se înregistrează congestie sau (ii) indiferent dacă există sau nu congestie.

Trebuie menționat, de asemenea, că furnizorii au opțiunea de a efectua managementul congestiei fără a viza un anumit tip de trafic sau o anumită aplicație. În acest caz managementul traficului este de tip „application agnostic".

În general, aceste tipuri de diferențiere au ca obiectiv asigurarea unui anumit nivel de performanță a rețelei și pot conduce la o utilizare mai eficientă a capacității existente a rețelei.

Diferențierea serviciilor destinate utilizatorilor

Tratarea diferită a traficului poate fi aplicată de furnizori pentru a oferi clienților pachete speciale în funcție de performanță, aplicând în consecință și prețuri diferențiate. Aceste practici pot include:

- limitări ale vitezei pentru accesul la internet în funcție de anumite condiții (permanent, după ce este atins un nivel fix de transfer, în timpul orelor de vârf etc.);
- diferite nivele de calitate (normal, premium etc.) luând în considerare diferiți indicatori de performanță;
- livrarea prioritară pentru un anumit tip de trafic selectat (ex. aplicații în timp real, ca VoIP sau video streaming);
- furnizarea de servicii care oferă protecție împotriva primirii de conținut nesolicitat(spam) sau restricționează accesul la un anumit conținut precum site-urile pentru adulți sau cele care difuzează violență;
- furnizarea serviciilor specializate precum IPTV (ce oferă o calitate cap la cap) în paralel cu serviciul de acces la internet (de tip best effort).

Diferențierea serviciilor destinate CAPs[26]

Acest tip de management al traficului se referă la diferențierea condițiilor în care CAP obțin acces la utilizatorii finali, conectați printr-un anumit ISP. Anumiți CAPs sau un anumit serviciu de conținut sau aplicație pot primi o prioritate/calitate mai mare în schimbul unei plăți sau a unui contract cu furnizorul de servicii de acces la internet. Astfel, traficul poate fi transmis având o calitate mai bună (din punct de vedere al indicatorilor de performanță a rețelei) în rețeaua ISP, în comparație cu calitatea de tip best effort. În acest caz tratarea diferențiată a traficului este limitată la rețeaua furnizorului respectiv.

De reținut că aceste practici de diferențiere pot fi aplicate în moduri diferite. Pot fi aplicate unui anumit tip de trafic (ex: trafic video), unor anumite tipuri de aplicații (ex: VoIP) sau anumitor furnizori de conținut și aplicații. Mai mult, această diferențiere poate fi oferită ca fiind o caracteristică a serviciului de acces la internet sau poate fi oferită ca un serviciu suplimentar oferit în paralel cu serviciul de acces la internet de bază.

Pe de o parte, diferențierea serviciilor e utilă în scopul de a satisface cererea pentru servicii de calitate superioară. Pe de altă parte, acestea pot afecta calitatea disponibilă pentru alți CAPs, care nu doresc să plătească pentru o calitate mai mare și pot avea un impact negativ asupra întregii piețe de conținut și aplicații.

Protejarea afacerilor existente

Servicii precum VoD, aplicațiile VoIP sau mesagerie IP pot fi percepute ca un substitut pentru serviciile tradiționale de voce, date sau video, putând astfel amenința serviciile tradiționale oferite deja de furnizorul de servicii de comunicații electronice. În cazul unui astfel de furnizor care oferă atât servicii tradiționale precum voce sau televiziune cât și serviciul de acces la internet (prin intermediul căruia se pot accesa servicii peste IP) exista un potențial stimulent de a bloca sau încetini serviciile accesibile prin intermediul protocolului IP. Astfel, accesul la anumite aplicații și servicii este limitat în cazul „serviciului standard de acces la internet" și este permis/disponibil pentru un tarif suplimentar, într-un plan de tarifare separat.

[26] Content and Application Providers

Blocarea, deprioritizarea sau tarifele suplimentare aplicate pentru furnizarea serviciilor mai sus amintite pot duce la practici anticoncurențiale sau la costuri excesive.

Motive legale

Tratarea diferențiată a traficului poate fi aplicată pentru respectarea anumitor prevederi legale, de exemplu, în cazul situațiilor de urgență pentru a permite realizarea comunicațiilor dintre autoritățile publice cărora le revine responsabilitatea privind organizarea apărării împotriva dezastrelor.

De asemenea, există cazuri în care aplicarea unor restricții este impusă în baza ordinelor judecătorești. Astfel de cauze, care pot conduce la aplicarea unor tehnici de gestionare a traficului includ:

- Blocarea accesului la folosirea ilegală a conținutului (în unele cazuri conținutul disponibil pe internet poate fi considerat ilegal și interzis pentru accesul public);
- Protejarea drepturilor de autor (în funcție de politica de protejare a drepturilor de autor, disponibilitatea anumitor conținuturi poate fi restricționată);
- Situații de urgență (reglementarea națională poate impune folosirea prioritară a rețelei și serviciilor de comunicațiile electronice pentru forțele de securitate, personal medical, etc.)
- Interceptarea legală a comunicațiilor electronice.

Securitatea și integritatea rețelei

Managementul traficului poate fi esențial în obținerea și menținerea securității și integrității rețelei, astfel că, în anumite condiții, se impune aplicarea anumitor tehnici de management al traficului:

- în cazul defectării unei linii de transmisiune sau a unui router sunt aplicate tehnici de management al traficului pentru redirecționarea traficului și management al congestiei pentru a restabili performanța rețelei la un nivel de calitate acceptabil și pentru a echilibra traficul între diferite elemente de rețea;
- în cazul atacurilor de tip DoS/DDoS managementul traficului este utilizat pentru depistarea și blocarea pachetelor ce provin de la surse suspecte;
- blocarea anumitor porturi.

2.3 Necesitatea măsurilor de management al traficului

Aplicarea tehnicilor de TM poate fi considerată necesară, adecvată sau problematică, în funcție de motivația și implementarea practicii, trebuind evaluate atât practica în sine, cât și situația în contextul pieței.

BEREC subliniază faptul că nu ar fi nici adecvat, nici relevant să fie definite practicile rezonabile și nerezonabile de gestionare a traficului. În plus, este dificil de apreciat dacă anumite forme de tratare diferențiată a traficului sunt rezonabile sau nu, dacă afectează competiția și inovația, sau afectează utilizatorii. Decizia în această privință depinde de obiectivele și efectele (intenționate sau nu) acestei diferențieri asupra părților implicate. Așadar, evaluarea acestui aspect trebuie făcută în funcție de caz.
BEREC propune evaluarea condițiilor în care restricțiile contractuale și practicile de TM sunt rezonabile, ținând cont de următoarele criterii:

I. **Nediscriminarea între participanți**- aceasta înseamnă că practicile sunt aplicate într-un mod nediscriminatoriu pentru toți furnizorii de conținut și aplicații,
II. **Controlul utilizatorului final**- faptul că practicile de gestionare a traficului pot fi aplicate (respectiv, dezactivate) la cererea utilizatorului, reprezintă un indicator important în scopul acestei evaluări,
III. **Eficiența și proporționalitatea**- măsurile ar trebui limitate la ce este necesar în atingerea obiectivului, pentru a minimiza posibile efecte adverse,
IV. **Practici care nu țin cont de tipul de aplicații –** întrucât acest tip de practici pot avea același efect, BEREC exprimă preferința pentru practicile care nu depind de conținut și aplicații.

Atunci când autoritatea de reglementare evaluează practicile de management al traficului, respectiv restricțiile în general, procesul de reglementare constă în două faze: prima se referă la evaluarea ofertelor diferitelor servicii ținând cont de criteriile mai sus amintite, urmată de cea de-a doua, în cadrul

căreia situația este evaluată în contextul pieței, ținând cont de disponibilitatea ofertelor de servicii de acces la internet la o calitate suficientă și/sau de ofertele de servicii de acces la internet nerestricționate.

3. Calitatea serviciului (QoS-quality of service)

Pornind de la prevederile Art. 22 (3)USD, potrivit căruia: *în vederea prevenirii degradării serviciului și a blocării sau încetinirii traficului în rețea, autoritatea de reglementare poate stabili cerințe minime de calitate a serviciului pentru unul sau mai mulți furnizori de rețele publice de comunicații,* acest capitol își propune clarificarea unor aspecte privind **definirea termenului de „calitate”**, **clasificarea tipurilor de servicii** precum și expunerea **etapelor implicate în identificarea situațiilor care impun stabilirea unor cerințe minime de calitate**.

3.1 Calitatea serviciului

Calitatea serviciului[27] reprezintă totalitatea caracteristicilor serviciului de telecomunicații, care se bazează pe capacitatea sa de a îndeplini nevoile stabilite și implicite ale utilizatorului serviciului.

Ținând cont de complexitatea dată de multitudinea caracteristicilor și a componentelor unui sistem de comunicații, conceptul de *calitate* poate fi privit din mai multe puncte de vedere. Astfel că:

- În scop pur tehnic se folosește termenul *performanța rețelei* (pentru a măsura performanța rețelei pe porțiuni aflate sub controlul furnizorului, parametrii relevanți fiind: întârzierea pachetelor, variația întârzierii, pierderea de pachete, viteza de transfer);
- Interacțiunea utilizatorului cu serviciul la interfața om-mașină este evaluată de conceptul QoS - *calitatea serviciului*; măsurătorile QoS se fac folosind parametrii cantitativi (sunt măsurabili și au atribuită o valoare a perfomanței) și calitativi (exprimați folosind înțelegerea și judecata umană);
- Modul în care utilizatorul final percepe un serviciu reprezintă calitatea experienței (QoE), care poate fi influențată de așteptările utilizatorului dar și de contex.

Așadar, *calitatea serviciului* cuprinde atât parametrii ce țin de *performanța rețelei (Network Performance)*, aflați sub controlul ISP, cât și parametrii care scapă de sub controlul furnizorilor (*Non-network performance*), de exemplu echipamentul terminal, iar ilustrarea legăturii dintre aceste concepte, se regăsește mai jos, în Fig.6:

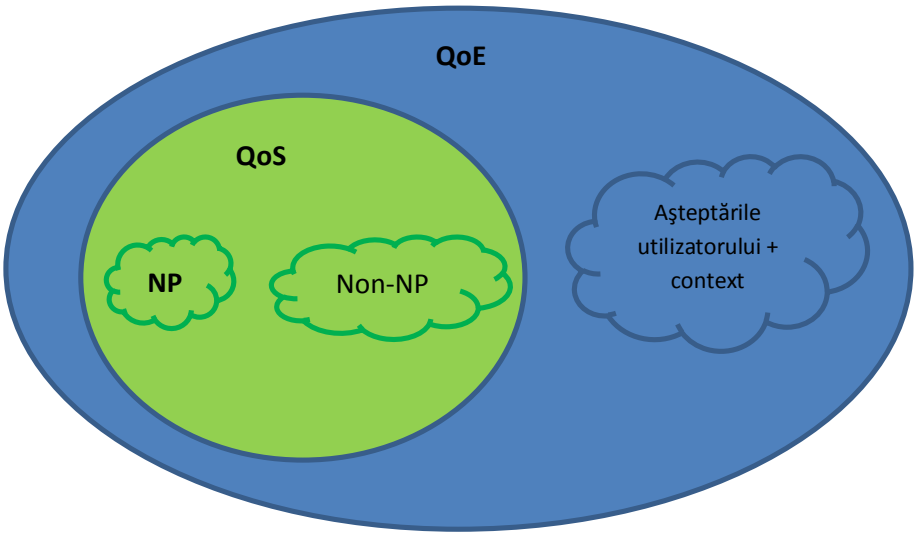

Fig.6 QoS, QoE și Performanța rețelei

[27] ITU-T Rec. E.800

În concluzie, dat fiind faptul că în cazul conceptelor QoS și QoE nu toți parametrii sunt controlabili, interpretarea noilor prevederi ale Art. 22 (3) USD ar trebui să facă referire la conceptul de *performanță a rețelei*, întrucât acesta este conceptul folosit pentru măsurarea performanței porțiunilor de rețea aflate sub controlul fiecărui operator.

Prin Decizia 1201/2012 ANCOM a stabilit un set relevant de parametri tehnici de calitate pentru furnizarea serviciului de acces la internet, și anume: viteza de transfer a datelor, întârzierea de transfer a pachetelor de date, variația întârzierii de transfer a pachetelor de date și rata pierderii de pachete de date. De asemenea, prin aceeași Decizie, este prevăzută dezvoltarea de către ANCOM a unei aplicații interactive, prin care se pot măsura parametrii mai sus amintiți. Aplicația va măsura performanța între echipamentul terminal al utilizatorului și un nod de tip internet interexchange. Măsurătorile vor indica o valoare a parametrilor mai aproape de experiența utilizatorilor finali în accesarea serviciilor de acces la internet, deoarece calea măsurată va include toată rețeaua furnizorului, precum și, în cazul furnizorilor de talie mică, alte rețele interconectate cu rețeaua proprie.

3.2 Tipuri de servicii

În ceea ce privește utilizarea capacității de transmisie într-o conexiune de acces la internet, au fost identificate două tipuri de servicii oferite:

- *Serviciul de acces la internet* (IAS - Internet Access Service) reprezintă serviciul de comunicații electronice destinat publicului care oferă conexiune la rețeaua Internet; serviciul de acces la internet poate fi **nerestricționat** (atunci când serviciul oferă acces la toate punctele terminale și la toate aplicațiile în internet, deși pot fi aplicate și restricționări rezonabile), sau **restricționat** (atunci când sunt aplicate restricționări nerezonabile, prin limitarea accesului către anumite puncte terminale și/sau aplicații).

Conform BEREC, un acces nerestricționat poate implica restricții *rezonabile*, deși termenul în sine poate presupune aplicarea unor practici care să contravină principiului neutralității.

- *Servicii specializate* (ex. IPTV, VPN) reprezintă servicii de comunicații electronice, care prevăd caracteristici garantate, stabilite în clauzele contractuale. Acest tip de servicii se bazează pe restricții de acces și tehnici extinse de gestionare a traficului, în scopul de a asigura caracteristici adecvate ale serviciului.

Întrucât cea de-a doua categorie de servicii oferă termeni contractuali care asigură calitatea serviciului, BEREC nu consideră necesară aplicarea Art. 22 USD (referitor la impunerea unui set minim de cerințe QoS *în scopul prevenirii degradării serviciului și a blocării sau încetinirii traficului în rețea*) în cazul serviciilor specializate.

Astfel, noțiunea de **degradare a serviciului** are în vedere două categorii principale:

- *Degradarea serviciului de acces la internet ca un întreg* ca de exemplu:
  - ✓ ISP prioritizează serviciile specializate în detrimentul serviciului de acces la internet;
  - ✓ Volumul traficului în internet crește mai repede decât capacitatea disponibilă (congestie);
  - ✓ Furnizarea serviciilor de acces la internet la o calitate suficientă este disponibilă doar pentru un număr restrâns de utilizatori.
- *Degradarea anumitor aplicații disponibile prin internet* ca de exemplu:
  - ✓ Blocarea VoIP în cazul serviciului de acces la internet mobil;
  - ✓ Blocarea sau limitarea P2P în cazul serviciilor de acces la internet fix sau mobil;
  - ✓ Tratarea diferențiată a traficului provenit de la furnizorii de conținut și de aplicații.

Degradarea performanței rețelei

O diminuare a performanței rețelei poate fi cauzată de o degradare generală în rețea, de exemplu din cauza unei **congestii** pe o anumită legătură (caz în care este necesară aplicarea practicilor de gestionare a traficului sau mărire a capacității legăturii) sau din cauza prioritizării unui anumit tip de trafic în detrimentul altuia (managementul traficului).

Congestia este situația care poate apărea când numărul pachetelor transmise în rețea este aproape de capacitatea de manipulare a rețelei și se poate datora unei situații neprevăzute sau neadaptării capacității rețelei la nivelul de încărcare.

Managementul traficului reprezintă mecanisme de gestionare a traficului pentru a optimiza fluxul de trafic în cadrul rețelelor proprii și pentru a atenua nivelul congestiei. Managementul traficului poate fi folosit pentru a implementa atât măsuri restrictive (blocare și restricționare), cât și măsuri de rutare și redirecționare.

Managementul traficului poate fi aplicat neținând cont de tipul de aplicații, în acest caz, pachetele IP de la toate aplicațiile fiind puse în aceeași coadă de așteptare, sau poate fi aplicat ținând cont de tipul de aplicații, caz în care aplicațiile sunt tratate diferit (de exemplu VoIP este blocat, P2P limitat, în timp ce alte aplicații sunt tratate normal).

3.3 Identificarea situațiilor în care se impune stabilirea unor cerințe minime de calitate

Procesul de identificare a situațiilor și modul în care autoritățile naționale de reglementare ar trebui să intervină prin măsuri de impunere a unui set de cerințe privind calitatea serviciului cuprinde mai mulți pași:

a) **Monitorizarea calității serviciului** este prima etapă și în cadrul acesteia se pot distinge două tipuri de abordări:
   - ✓ *Abordarea proactivă*, în cadrul căreia se recurge la verificarea termenilor și condițiilor ofertelor de servicii de acces la internet disponibile pe piață. Aceasta se poate face pe baza informațiilor publicate de ISP sau a instrumentelor de măsurare, care furnizează statistici privind performanța rețelelelor furnizorilor de servicii de internet. Publicarea datelor în mod regulat contribuie la o mai mare transparență în ce privește calitatea IAS iar dacă monitorizarea include date de la mai mulți ISP, aceasta poate constitui un instrument de comparare în vederea promovării competiției și creșterea conștientizării utilizatorilor în privința situației de pe piață.
   - ✓ *Abordarea reactivă*, adoptată în urma plângerilor din partea utilizatorilor finali, inclusiv a furnizorilor de conținut și aplicații.

În ambele situații este important ca autoritatea de reglementare să identifice și să monitorizeze indicatori ai practicilor ce încalcă principiul neutralității, în scopul de a trasa o linie de referință. Astfel, monitorizarea pieței de-a lungul unei perioade de timp poate permite observarea indicatorilor care au o traiectorie neobișnuită, ceea ce indică o schimbare.

b) **Evaluarea situației**: este necesară intervenția autorității de reglementare?

În cadrul acestei etape, autoritatea de reglementare analizează dacă incidentele raportate sau detectate constituie o degradare a serviciului, sau prezintă un risc în acest sens, și apreciază dacă este necesar să intervină în anumite cazuri. Prevederile legale stabilesc doar faptul că NRA sunt împuternicite să intervină în scopul de a *preveni degradarea serviciului, obstrucționarea sau limitarea traficului în rețea* (Art. 22 alin. 3 USD), dar nu specifică și criteriile pe care un reglementator trebuie să le aibă în vedere când analizează necesitatea impunerii unui set minim de cerințe privind calitatea serviciului.

BEREC oferă câteva sugestii în acest sens, astfel că:

- Degradarea performanței serviciului de acces la internet poate fi analizată:
  - ✓ Comparând-o cu performanța serviciilor specializate
  - ✓ Făcând comparații între ofertele ISPs
  - ✓ Comparând viteza reală cu cea comercializată de furnizori
- Degradarea aplicațiilor poate fi analizată având în vedere următoarele:
  - ✓ Disponibilitatea și gradul de penetrare al ofertelor de acces nerestricționat la internet în comparație cu cele restricționate
  - ✓ Blocarea/limitarea uneia sau mai multor aplicații
  - ✓ Limitări aplicate în funcție de sursă și/sau destinație

Intervenția autorității de reglementare nu este necesară atunci când există o disponibilitate apreciabilă a ofertelor serviciului de acces la internet, la o calitate satisfăcătoare și la un preț

rezonabil, precum și posibilitatea de a schimba ușor furnizorul (de a migra ușor către diferite pachete de servicii).

c) **Alegerea remediului** reprezintă următorul pas, în cazul în care se consideră că o intervenție din partea autorității de reglementare ar fi justificată.

Opțiunile de reglementare includ, acolo unde se impun, remedii de promovare a concurenței și impunerea unor cerințe (mai clare sau detaliate) de transparență. Dacă aceste măsuri se dovedesc a fi ineficiente în eliminarea degradării serviciului, autoritatea de reglementare poate impune un set minim de cerințe privind calitatea serviciului.

d) Relevanța etapei de **stabilire a cerințelor de calitate** trebuie să fie evaluată din perspectiva principiilor care se referă la *eficiență* (implică faptul că cerințele QoS pot fi implementate în mod rezonabil și pot preveni, reduce sau elimina degradarea), *necesitate* (implică faptul că degradarea s-a materializat, iar alte instrumente de reglementare s-au dovedit, sau au fost considerate insuficiente în scopul remedierii situației) și *proporționalitate* (implică limitarea cerințelor la domeniul de aplicare corespunzător, iar obligația impusă este proporțională cu scopul propus).

4. Transparența

Transparența cu privire la restricționările în accesarea conținutului și aplicațiilor este unul dintre elementele-cheie invocate în cadrul Directivelor Europene în scopul atingerii obiectivului de neutralitate a rețelelor. Așa cum am menționat în capitolul 1, transparența reprezintă o condiție prealabilă esențială pentru capacitatea utilizatorului final de a alege calitatea serviciului care se potrivește cel mai bine nevoilor sale, ceea ce contribuie la sporirea concurenței pe piață.

Un alt beneficiu al transparenței este acela că reduce asimetria de informație existentă între furnizori și utilizatorii finali, încurajând astfel un comportament orientat spre utilizatorul final din partea furnizorilor de servicii de acces la internet.

În atingerea obiectivului neutralității, transparența nu este totuși suficientă, factorii complementari care, împreună cu transparența ar putea conduce la atingerea lui fiind: concurența pe piață și reducerea barierelor existente la schimbarea furnizorului de servicii de acces la internet.

Ținând cont de Ghidul BEREC privind transparența în domeniul neutralității internetului, în cadrul acestui capitol se vor clarifica aspectele ce țin de **conținutul** și **caracteristicile relevante ale unei politici privind transparența** în materie de neutralitate a rețelelor, precum și **metodele prin care informația poate fi pusă la dispoziția utilizatorului final**.

Conform BEREC, **politica de transparență** reprezintă ansamblul tuturor măsurilor adoptate (de către furnizori, instituții publice sau terțe părți) în scopul de a susține sau de a furniza informații transparente către utilizatorii serviciilor de comunicații electronice.

4.1 Caracteristicile relevante ale unei politici privind transparența

Conform Art. 20 din USD, informațiile relevante (despre managementul traficului) trebuie specificate în cadrul contractelor, într-o formă clară, completă și ușor accesibilă. Pentru a satisface această cerință, BEREC a identificat anumite criterii care ar trebui îndeplinite.

De asemenea, BEREC a identificat faptul că o politică de transparență pe deplin eficientă ar trebui să îndeplinească următoarele caracteristici:

- **Accesibilitate**: informațiile referitoare la serviciul de acces la internet și în special managementul traficului și alte restricții trebuie să fie accesibile. Printre altele, accesibilitatea se referă la faptul că informațiile pot fi ușor găsite și identificate.
- **Inteligibilitate**: o altă cerință importantă pentru transparența informației este ca informația să fie inteligibilă pentru utilizatorii finali. Informația care este prea tehnică pentru utilizatori nu va fi înțeleasă de către aceștia și prin urmare, nu vor face alegeri informate. Pentru a fi inteligibilă, informația trebuie de asemenea prezentată într-o formă prietenoasă.

- **Pertinență**: transparența presupune și ca informația să fie pertinentă. Utilizatorii finali nu pot face alegeri informate dacă informațiile sunt ambigue, irelevante, sau sunt prezentate într-un mod nefolositor pentru aceștia.
- **Comparabilitate**: informația este suficient de comparabilă pentru utilizatorii finali atunci când aceeași informație este prezentată într-un mod destul de similar de către diferiți furnizori sau pentru diferite oferte, astfel încât utilizatorii finali să poată identifica cu ușurință asemănările sau deosebirile dintre diferitele oferte.
- **Acuratețe**: informația trebuie să fie corectă și actualizată.

Metodele prin care informația poate fi pusă la dispoziția utilizatorului final

O politică de transparență implică utilizarea a două metode prin care informația poate fi pusă la dispoziția utilizatorilor finali, în contextul neutralității, și anume: *directă* și *indirectă*.

Metoda directă reprezintă metoda prin care furnizorii sunt cei care pun în mod direct informațiile la dispoziția utilizatorilor finali. În acest caz, autoritățile de reglementare au obligația să se asigure că operatorii pun la dispoziția publicului informații care îndeplinesc cele 5 caracteristici amintite mai sus. Tot autoritățile naționale sunt cele care decid nivelul de detaliu al informației pe care furnizorii trebuie să o pună la dispoziția utilizatorilor finali. Întrucât prezentarea unei cantități prea mari de informație foarte tehnică nu ar fi de folos utilizatorului în alegerea ofertelor, autoritățile de reglementare ar putea decide ce tip de informații sunt relevante pentru aceștia precum și modalitatea în care aceste informații vor fi puse la dispoziția utilizatorilor.

Exemple de întrebări la care ISP pot furniza informații relevante:

- Serviciul de internet este restricționat sau nu?
- Dacă este restricționat,
  - Ce aplicații primesc un tratament special din punctul de vedere al managementului traficului?
  - Care este efectul măsurilor de management al traficului asupra aplicațiilor, așa cum este el resimțit de utilizatorii finali?
  - Când poate fi observat acest efect?

Avantajul acestei metodei constă în faptul că furnizorii sunt sau pot fi obligați, prin intermediul cadrului legislativ, să pună anumite informații la dispoziția utilizatorilor finali în mod direct, prin intermediul propriului site, de exemplu, sau prin alte mijloace de comunicare. Principalul dezavantaj ar consta însă faptul că furnizorii nu pot fi obligați la punerea la dispoziția publicului a unei cantități mari de informații.

În cadrul *metodei indirecte,* rolul principal îl au părțile terțe, care pot interpreta (adapta) informațiile tehnice, în scopul de a fi puse la dispoziția utilizatorilor finali într-o formă inteligibilă și adecvată pentru aceștia.

Părțile terțe pot fi reprezentate, printre altele, de experți tehnici, site-uri ce compară tarife, valori ale anumitor parametri, precum și autorități de reglementare, etc. Pentru ca această metodă să funcționeze, este necesar ca părțile terțe să fie bine informate și să aibă acces la toate informațiile actualizate de care au nevoie, iar utilizatorii finali să fie conștienți de existența acestor părți terțe și de rolul lor de a asigura caracterul de comparabilitate, inteligibilitate și pertinență a informațiilor tehnice.

În acest caz, furnizorii de servicii de internet pot furniza informații relevante pentru părțile terțe răspunzând la aceleași întrebări ca și în cazul anterior.

Principalul avantaj al acestei metode îl reprezintă faptul că terțele părți pot pune la dispoziția publicului o cantitate mai mare de informație, inclusiv informație tehnică referitoare la tehnicile de management al traficului. Dezavantajul constă însă în faptul că furnizorii nu sunt obligați să pună la dispoziția terților părți toate informațiile de care aceștia au nevoie pentru a le furniza mai departe utilizatorilor finali.

Prin urmare, având în vedere avantajele fiecărei metode, este necesar ca ambele să fie utilizate de autoritățile de reglementare atunci când stabilesc politica de transparență în ceea ce privește neutralitatea internetului.

4.2 Conținutul unei politici de transparență în ceea ce privește neutralitatea internetului

BEREC consideră că este esențială perceperea transparenței ca un instrument care să permită utilizatorilor să facă alegeri informate.

În vederea îmbunătățirii transparenței cu privire la informațiile oferite utilizatorilor finali, BEREC a identificat acele elemente minime care ar trebui să caracterizeze ofertele ISP, astfel încât să fie îndeplinită o politică de transparență corectă. Acestea sunt detaliate în continuare.

4.2.1 <u>Domeniul de aplicare și conținutul ofertei</u>

Această secțiune cuprinde principalele elemente pe care ar trebui să le conțină oferta furnizorilor din punct de vedere al neutralității internetului.

a) ***Disponibilitatea serviciilor*** - această informație se referă la descrierea serviciilor furnizate, inclusiv la opțiunile disponibile, precum și la diferitele tarife și condiții aplicabile. De asemenea, în contextul asigurării transparenței, este importantă evidențierea ofertelor nerestricționate (restricționările ar însemna, de exemplu, restricții privind utilizarea unor aplicații sau conexiune limitată către anumite destinații în rețea).

b) ***Terminologia*** - în general furnizorii folosesc pentru oferte terminologii diferite sau aceiași termeni cu înțelesuri diferite, fapt ce generează confuzie în rândul utilizatorilor. De exemplu, atunci când își promovează ofertele, furnizorii folosesc termeni ca: „acces la date", „internet", „surf", „web" pentru a-și descrie ofertele. Un utilizator obișnuit nu știe ce presupun aceste servicii, iar pentru a preîntâmpina acest lucru, pentru a garanta caracterul inteligibil și comparabil al ofertelor, este foarte important să existe o formă de înțelegere comună din partea utilizatorilor, cel puțin pentru cele mai utilizate concepte.

c) ***Viteza anunțată (promovată)***[28] - în general, viteza anunțată de furnizori reprezintă viteza de download, însă utilizatorii trebuie să fie informați și în privința vitezei de upload, care în mod normal nu este evidențiată (se poate regăsi ascunsă în clauzele contractuale).

d) ***Viteza reală*** - în practică, vitezele reale (download și upload) sunt semnificativ mai mici decât cele anunțate. Acest lucru constituie și o cauză frecventă a plângerilor utilizatorilor, adresate autorităților de reglementare. ISP ar trebui să fie mai transparenți în privința condițiilor care influențează viteza reală de transfer, experimentată de utilizatorii finali.

e) ***Calitatea minimă a serviciului ofertat și alți parametri de calitate*** - furnizarea informațiilor cu privire la parametrii minimi de calitate a serviciilor implică informarea utilizatorilor despre condițiile de aplicare a acestora (dacă parametrii respectivi se aplică în general, sau sunt valabili doar pentru anumite servicii/aplicații). În contextul neutralității rețelei, din punct de vedere tehnic aceste informații se pot referi la viteză (minimă, medie, etc.), întârzierea de pachete, jitter, sau pierderile de pachete. Având în vedere specificul tehnic al acestui tip de informații, pentru utilizator ar fi mai util să fie informat în legătură cu implicațiile pe care le pot avea diversele limitări asupra experienței sale în utilizarea serviciului.

f) ***Alte considerații asupra domeniului de aplicare a ofertei*** - în contextul transparenței, informațiile furnizate trebuie să fie simple și nu în exces. În orice caz, necesitatea furnizării informațiilor într-o formă simplă, inteligibilă nu ar trebui să servească drept scuză pentru operatori de a nu oferi mai multe informații specifice și detaliate. BEREC admite faptul că reprezintă o provocare încercarea de a stabili un echilibru între simplitate și complexitate.

[28] Viteza nominală/maximă (conform Deciziei 1201 *privind stabilirea indicatorilor de calitate pentru furnizarea serviciului de acces la internet*)

4.2.2 Limitări generale ale ofertei

Aceste limitări se referă la situațiile în care conexiunilor utilizatorilor le sunt aplicate limitări, cum ar fi de exemplu, cazul limitării volumului de date, dincolo de care viteza de acces la internet scade.

a) Transparența privind politicile de utilizare a serviciului de acces la internet

Furnizorii pot folosi de cele mai multe ori politici de utilizare a serviciului de acces la internet, însă acestea sunt uneori enunțate în termeni vagi, insuficient de clari pentru utilizator.

BEREC este de părere că abonatul trebuie să fie informat în mod clar în legătură cu ce se consideră a fi o utilizare corectă sau abuzivă a rețelei/serviciului operatorului respectiv. Astfel, termenii utilizați în descrierea acestor politici nu trebuie să fie confuzi, ci să descrie în mod clar atât drepturile și obligațiile furnizorului, cât și pe cele ale utilizatorului final.

b) Limitări aplicate conform cu volumul de date contractat (download limit)/(data caps)

Utilizatorii trebuie să fie informați în cazul în care există anumite praguri stabilite de furnizori, dincolo de care viteza de transfer a datelor scade (*data caps*) sau abonatul trebuie să plătească în plus pentru a beneficia de serviciul de acces la internet în aceleași condiții (*download limits*). Furnizorul trebuie să menționeze în mod explicit faptul că aceste limitări există, în ce constau și mai ales, care sunt consecințele depășirii acestor praguri. De asemenea, ar trebui ca utilizatorii să aibă posibilitatea de a verifica cât au consumat, precum și volumul de trafic rămas disponibil până la atingerea pragului.

4.2.3 Limitări specifice ale ofertei

a) Aplicarea tehnicilor de gestionare a traficului

Transparența în ceea ce privește tehnicile de management al traficului presupune furnizarea unor diverse tipuri de informații. Furnizorii ar trebui să includă în cadrul ofertelor, răspunsuri la următoarele întrebări:

- Cum se realizează ***managementul congestiei***? Se aplică principiul FIFO (primul venit, primul servit)? Sau sunt aplicate tehnici mai avansate? Modul în care se aplică tehnicile de management al congestiei țin cont de tipul de aplicație sau toate sunt tratate în mod egal?
- Este aplicată politica de limitare a traficului (***bandwidth throttling***)? Dacă da, când este aplicată această formă de gestionare a traficului? Este aplicată în general, sau în funcție de tipul de aplicație?
- Este traficul ***prioritizat***? Dacă da, care tipuri de trafic sunt prioritizate - cel al anumitor clienți, sau anumitor aplicații, protocoale sau conținut? Când este traficul prioritizat - în general, sau în anumite circumstanțe, cum ar fi în orele de vârf?
- Este un anumit trafic ***blocat***? Dacă da, ce anume este blocat (de exemplu accesul la anumite pagini de internet sau anumite aplicații sunt blocate în mod selectiv) și când este traficul blocat?
- Pentru toate aceste tehnici de management al traficului, utilizatorii trebuie să fie informați despre modul în care ele **afectează experiența utilizatorului.**
- Transparența implică de asemenea punerea la dispoziție a informațiilor privitoare la motivele aplicării anumitor tehnici de management al traficului.

b) Punerea la dispoziția utilizatorilor a unor metode care să le permită monitorizarea serviciului de acces la internet

În cazul în care se aplică limitări ale serviciului de acces la internet, abonații au nevoie de instrumente care să le permită monitorizarea serviciului de care beneficiază, putând astfel să analizeze dacă au ales pachetul de servicii care se potrivește cel mai bine nevoilor lor.

5. Aspecte privind competiția

Competiția joacă un rol fundamental (bazat pe calitatea ridicată a produselor) în asigurarea neutralității rețelelor: cu cât este mai puternică presiunea creată prin competiție, cu atât ISP vor fi

încurajați în sensul creșterii calității serviciilor oferite. Acest subiect este abordat în cadrul raportului privind *Practicile diferențiate și aspecte privind competiția în scopul neutralității rețelelor* întocmit de BEREC, în care se face o evaluare a consecințelor pe termen lung și scurt a practicilor diferențiate de gestionare a traficului asupra utilizatorilor. De asemenea, este furnizat un cadru de analiză a acestor practici, fiind examinate trei situații: blocarea VoIP, limitarea traficului P2P și ofertele diferențiate pentru CAPs.

În cadrul raportului BEREC, **practicile diferențiate** sunt definite ca orice decizie a ISP, sau orice tip de acord între ISPs și CAPs, sau între ISPs și utilizatorii finali, care au ca rezultat faptul că traficul dinspre sau înspre anumiți CAPs sau utilizatori finali, sau care se referă la anumite aplicații sau protocoale este tratat diferențiat față de traficul altor CAPs sau utilizatori finali sau alte aplicații ori protocoale. Tratarea diferențiată poate să rezide în limitarea, prioritizarea sau blocarea traficului.

Acest capitol își propune clarificarea unor aspecte dezbătute și în cadrul raportului mai sus amintit și care vizează: **entitățile active** și relația dintre acestea, precum și **efectele** aplicării practicilor de management al traficului.

5.1 Entități active pe piață

Termenul de "*livrare de tip best-effort*" descrie un serviciu de comunicații electronice în care rețeaua nu furnizează nicio garanție că datele sunt livrate și utilizatorului nu-i este garantat nivelul de calitate a serviciului sau o anumită clasă de prioritate. Într-un scenariu de tip best-effort toți utilizatorii obțin o viteză și un timp de transfer în funcție de încărcarea traficului. Astfel că toate cererile de serviciu ale utilizatorilor se tratează în mod egal, indiferent de natura acestuia sau conținut.

În prezent, tehnicile de gestionare a traficului permit ISP să gestioneze mai extensiv și mai precis și să diferențieze pachetele, în funcție de conținut, aplicații, servicii de transport/acces și utilizatori. Așa cum a fost menționat deja în cadrul capitolului 2 din prezentul raport, gestionarea traficului permite o gamă largă de operațiuni cum ar fi, printre altele, construirea unor căi rapide (de ex. clasele de trafic) pentru un anumit tip de date (prioritizare); furnizarea unei capacități garantate de transfer pentru anumiți utilizatori; prevenirea accesului la conținutul ilegal; autentificarea clienților; blocarea de viruși sau abilitatea de blocare sau degradare unui anumit conținut. Așadar, managementul traficului oferă potențiale beneficii (de exemplu gestionarea/reducerea congestiei), dar, pe de altă parte, gestionarea traficului poate fi folosită pentru implementarea unor practici care folosesc tehnici restrictive și care sunt în beneficiul operatorului, dar în detrimentul utilizatorilor.

Tendința este ca diversitatea aplicațiilor să devină tot mai mare, acestea având cerințe specifice, în funcție de caracteristicile lor. Parametrii relevanți pentru calitatea serviciului sunt, printre altele, viteza de transfer (bitrate sau volumul de date transmis în unitatea de timp), întârzierea, variația întârzierii și rata pierderii de pachete. În funcție de tipul de aplicație, unii dintre acești parametri sunt relevanți în furnizarea serviciului. De exemplu, în general, calitatea P2P depinde în principal de viteza de transfer disponibilă, în timp ce întârzierea pachetelor poate fi tolerată având efecte minore asupra calitatății P2P. În cazul VoIP, furnizarea serviciului nu depinde foarte mult de viteză, în schimb întârzierea joacă un rol critic.

Inovațiile tehnologice și evoluțiile pieței au dus la modificarea relațiilor comerciale dintre anumiți actori; în cadrul acestui document au fost identificate ca fiind active trei entități majore:

- *Furnizorii de servicii de internet* (ISPs-Internet Service Providers) sau furnizorii de acces la internet (IAPs-Internet Access Providers). Aceștia pot furniza servicii fie prin intermediul propriei rețele fixe sau mobile fie prin intermediul rețelei altui operator(de ex. distribuitorii și operatorii de rețele virtuale mobile);
- *Furnizorii de conținut și aplicații* (CAPs- Content and Applications Providers) - oferă o gamă largă de activități cum ar fi agregarea de conținut și motoare de căutare, aplicații de tip messenger, divertisment și tranzacții. Aceștia sunt plătiți de către utilizatorii proprii și/sau de advertiseri. Exemple de astfel de furnizori sunt: platforme care permit tranzacții (Amazon, eBay), platforme de socializare (Facebook), motoare de căutare (Google, Bing), servicii de entertainment (Youtube), furnizori de aplicații (Skype), Video on Demand (Netflix);

— *Utilizatorii* care achiziționează acces la internet de la IAPs și folosesc (cu sau fără plată) conținutul și aplicațiile furnizate de CAPs. Utilizatorul poate fi persoană fizică sau juridică. Interacțiunea dintre aceste entități (Fig.7, conform raportului BEREC, *Differentiation practicies and related competition issues in the scope of net neutrality*) are ca rezultat furnizarea serviciilor către utilizatori, care obțin acces la internet prin intermediul ISP și folosesc (gratis sau contra cost) conținutul și aplicațiile furnizate de CAPs.

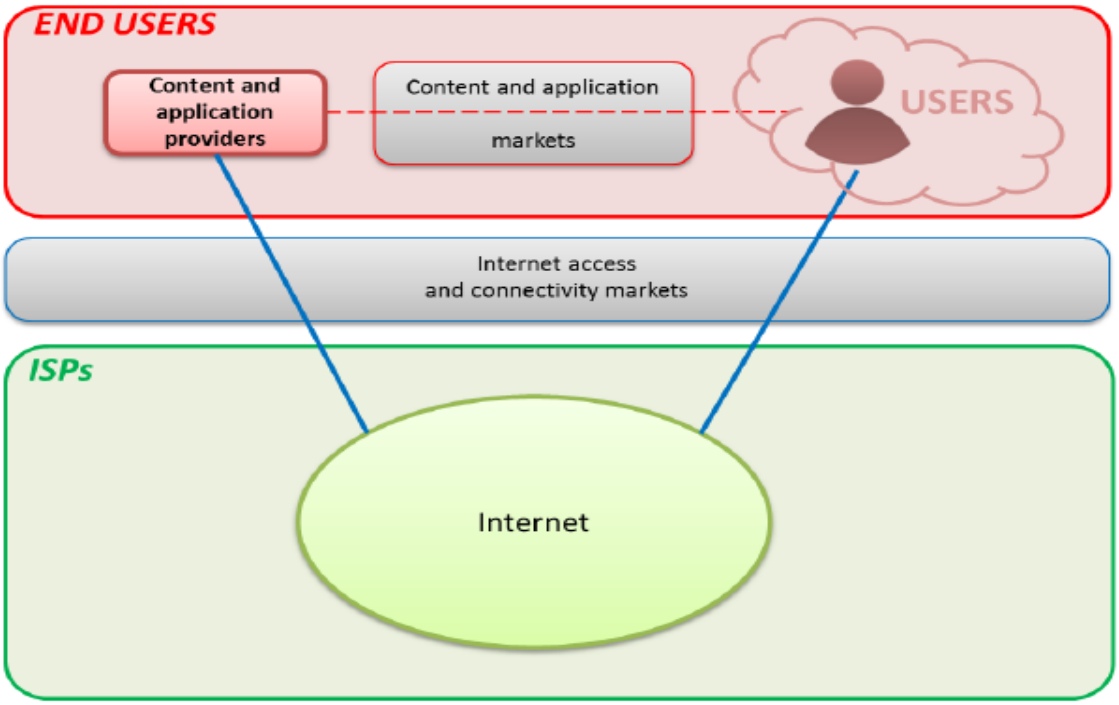

Fig.7 Identificarea entităților

ISP are un rol special, comportându-se ca un intermediar. Pe de o parte, ISP furnizează acces la servicii de comunicații electronice pentru utilizatori, pe de altă parte permit interacțiunea dintre CAPs și utilizatori.
De subliniat este faptul că furnizorii de aplicații și conținut interacționează cu utilizatorii prin așa numitele piețe de aplicații și conținut, dar de obicei acestea nu implică neapărat o legătură directă. Legătura fizică directă între CAPs și utilizatori trece prin piața de servicii de comunicații electronice, cu ISP acționând ca un intermediar.

Pentru a clarifica mai bine poziția și rolul fiecărei entități mai sus amintite, este necesară o descriere mai detaliată a serviciilor de comunicații electronice din perspectiva lanțului de valori a internetului. Figura 7 identifică succint actorii și tipurile de piețe existente. Figura 8 ilustrează faptul că aceleași entități pot juca mai multe roluri diferite, în funcție de piețele la care se raportează.

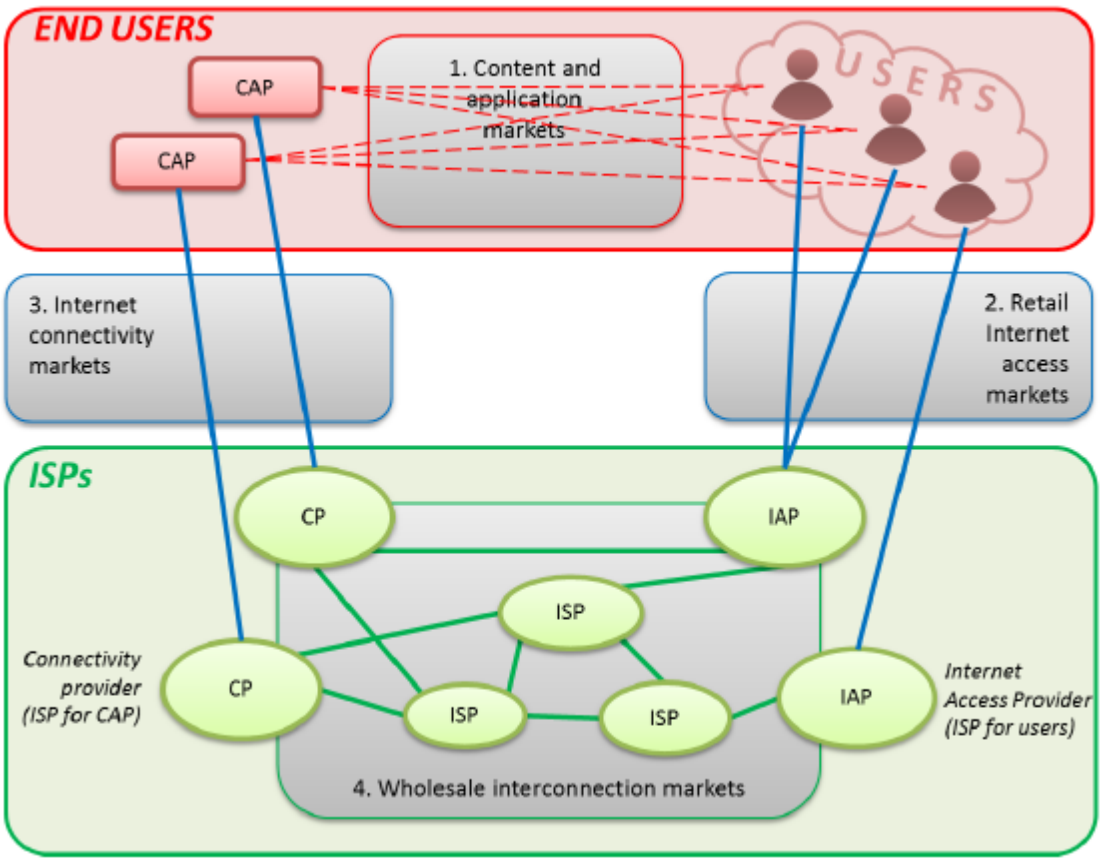

Fig. 8 Rolul entităților în funcție de pieţele la care se raportează

Așa cum reiese din Figura 8, furnizorii de servicii de internet sunt activi pe una sau mai multe pieţe din sfera comunicațiilor electronice, astfel:

- Pe *piața cu amănuntul de acces la internet*, furnizorii de acces la internet reprezintă furnizori de servicii de internet pentru utilizatori;
- Pe *piața conectivității la internet*, furnizorii de conectivitate sunt de fapt ISPs care furnizează servicii către furnizorii de conținut și aplicații;
- Pe *piața de gros a interconectării,* furnizorii de servicii de internet pot interacționa (se pot interconecta între ei).

5.2 Posibile efecte ale practicilor de managementul traficului

Tratarea diferențiată a traficului poate fi făcută din mai multe motive, care implică mai multe obiective. În anumite cazuri, această practică poate afecta competiția, inovația sau poate dăuna utilizatorului, însă este dificil de stabilit în ce cazuri tratarea diferențiată a traficului este rezonabilă sau nu. Aprecierea acestui aspect depinde de o serie de obiectivele avute în vedere, de efectele tratării diferențiate a traficului, precum și de structura pieței unde se aplică aceste practici.

Așa cum a fost prezentat pe larg în cap.2, furnizorii practică tehnici de managementul traficului din mai multe motive (congestie, securitatea și integritatea rețelei, motive legale, diferențierea serviciilor sau protejarea afacerilor existente).

În contextul neutralității rețelelor, raportul BEREC privind competiția își propune să evalueze impactul practicilor de diferențiere descrise mai sus, asupra utilizatorilor finali.

Efectele acestor practici de gestionare a traficului asupra utilizatorului final pot fi împărțite în două categorii:

- **Directe (pe termen scurt)** - orice măsură care prevede modificarea prețului sau calității serviciilor furnizate utilizatorului final, care limitează posibilitatea acestora de a alege, care restricționează posibilitatea de utilizare a serviciului de acces la internet e probabil să aibă un impact

imediat. Dacă, de exemplu, o aplicație care nu are mulți utilizatori activi a fost blocată, impactul imediat poate fi limitat. Impactul depinde de numărul de utilizatori care pot fi afectați. Impactul poate fi redus atunci când există oferte alternative disponibile, deoarece utilizarea acelei aplicații e posibilă în cazul în care se optează pentru o altă ofertă sau pentru schimbarea furnizorului.

- **Indirecte (pe termen lung sau mediu**)
    a. având în vedere evoluția condițiilor de pe piața serviciilor de comunicații electronice, practicile de diferențiere pot avea impact asupra competiției. O scădere a nivelului competiției ar fi în defavoarea utilizatorului, pentru că ar reduce posibilitatea de a alege și ar permite creșterea prețurilor sau scăderea calității;
    b. având în vedere evoluția condițiilor de pe piața privind conținutul și aplicațiile; în ceea ce privește CAPs, practicile diferențiate conduc la posibilitatea de reducere a competiției dintre furnizorii de conținut și aplicații. Impactul poate fi diferit, în funcție de mărimea CAP. Introducerea unor tarife diferite sau condiții tehnice (de ex. diferite scheme de QoS) poate fi văzută ca o barieră pentru unii CAP, cum ar fi cei mici, sau cei noi intrați pe piață.

Posibile efecte ale aplicării unor practici de TM asupra ecosistemului internet

Analiza efectelor gestionării traficului realizată de BEREC a relevat, de asemenea, următoarele aspecte:

- ✓ Dezvoltarea ofertelor de tip premium, care ar permite operatorilor să satisfacă cererea din partea utilizatorilor finali și CAP, ar conduce la scăderea motivării ISP de a investi în creșterea capacității benzii de transmisie a datelor.
- ✓ Dezvoltarea practicilor de managementul traficului care blochează sau reduc posibilitatea dezvoltării de noi aplicații în internet pot conduce la situația în care achiziționarea ofertei de acces la internet simplu se poate dovedi prea costisitoare pentru oamenii obișnuiți.
- ✓ Dezvoltarea de acorduri bilaterale între ISPs și CAPs pentru prioritizarea conținutului furnizorului de aplicații și conținut în rețeaua ISP poate conduce la evoluția internetului cu două viteze, situație în care doar furnizorii mari de aplicații și conținut deja existenți pot ajunge la utilizatorul final cu o calitate bună a serviciului, limitând astfel oportunitățile noilor CAPs intrați pe piață.
- ✓ BEREC a admis faptul că ISPs ar trebui să aibă oportunitatea de a-și gestiona propriile rețele pentru a crește eficiența, minimizând resursele necesare pentru furnizarea serviciului și asigurând cele mai bune condiții pentru utilizatorii finali. De subliniat faptul că o congestie în rețea implică anumite aspecte dificil de cuantificat, pentru că într-o astfel de situație, sunt afectați toți utilizatorii conectați la rețea. În acest scop, un management corect al traficului ar duce la o îmbunătățire a situației.
- ✓ Restricționarea sau blocarea accesului utilizatorilor finali la conținut sunt măsuri care implică diminuarea opțiunilor disponibile pe legăturile lor. Acest lucru poate deveni o problemă atunci când ISP tind să blocheze sau să degradeze aplicații sau CAPs, mai ales când un anumit ISP blochează o anumită aplicație sau CAP, un alt ISP blochează o altă aplicație sau CAP și așa mai departe. În acest context, caracteristicile actuale ale internetului vor fi greu de menținut, utilizatorii finali fiind în cele din urmă afectați.

De asemenea, BEREC a identificat câteva elemente cheie care ar putea împiedica ISP să implementeze practici de diferențiere, care afectează utilizatorii finali:

- ✓ Competiția de pe piața cu amănuntul; Autoritățile de reglementare dețin în cadrul actual de reglementare instrumente pentru a spori competiția și a preveni consolidarea poziției furnizorilor având putere semnificativă pe piață.
- ✓ Gradul de conștientizare al consumatorului, transparența de pe piață și costurile mici implicate de schimbarea furnizorului- cu cât un consumator poate detecta mai ușor o practică restrictivă și schimbă furnizorul ISP, cu atât este mai mare presiunea asupra furnizorilor de acces la internet de a reduce practicile discriminatorii și injuste.

6. Interconectarea IP

Acordurile de interconectare între rețele nu sunt strâns legate de neutralitate atâta timp cât toate fluxurile de trafic sunt tratate în mod egal. O încălcare a principiului neutralității este considerată ca fiind puțin probabilă în condițiile în care tot traficul este tratat în modul best effort. Însă o întrerupere (perturbare) a interconectării la nivel de gros ar putea afecta accesibilitatea tuturor destinațiilor din internet, caracterul de neutralitate al rețelelor fiind astfel afectat.

Modalitatea tehnică de interconectare, precum și alte aspecte care privesc interconectarea rețelelor IP (noțiuni, procese, elemente constitutive) sunt descrise în *Raportul referitor la chestionarul privind interconectarea pe suport IP a rețelelor de comunicații electronice din România*[29] publicat de ANCOM în 2013.

Acest capitol va prezenta concluziile enunțate în raportul BEREC *An assessment of IP interconnection in the context of Net Neutrality*[30] în privința mai multor aspecte, precum: **dezvoltarea acordurilor de interconectare**, **tendințele în lanțul de valori, calitatea serviciului în raport cu livrarea de tip *best effort*, principii referitoare la taxare,** precum și **aspecte de reglementare.**

Dezvoltările acordurilor de interconectare

- În vederea interconectării rețelelor există două tipuri de acorduri posibile: peering și tranzit. Furnizorii de servicii de internet, care îndeplinesc condițiile pentru a putea încheia un acord de tip peering, pot opta pentru una din cele două forme de interconectare. Decizia în această privință (de a încheia acord de tip peering sau de a cumpăra tranzit) depinde de planificarea rețelei și de optimizarea costurilor. De cele mai multe ori, furnizorii optează pentru ambele forme de interconectare, acestea putând fi folosite în mod complementar (pentru majoritatea furnizorilor încheierea cel puțin a unui acord de tranzit este o necesitate);
- Ecosistemul internet a reușit adaptarea acordurilor de interconectare IP la schimbările tehnologice, precum și la schimbările privind modelele de afaceri. Acest lucru a fost posibil fără o reglementare în acest sens;
- În general, acordurile de interconectare nu sunt încheiate sub formă de contracte scrise;
- Nu sunt stabilite clasele de trafic privind calitatea serviciului în rețelele interconectate.

[29] http://www.ancom.org.ro/regimul-interconectarii_5011

[30] Versiunea integrală a documentului este disponibilă la următoarea adresă: http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/1130-an-assessment-of-ip-interconnection-in-the-context-of-net-neutrality

Tendințele în lanțul de valori

În schema de mai jos sunt prezentate categoriile de servicii de comunicații electronice din cadrul lanțului de valori.

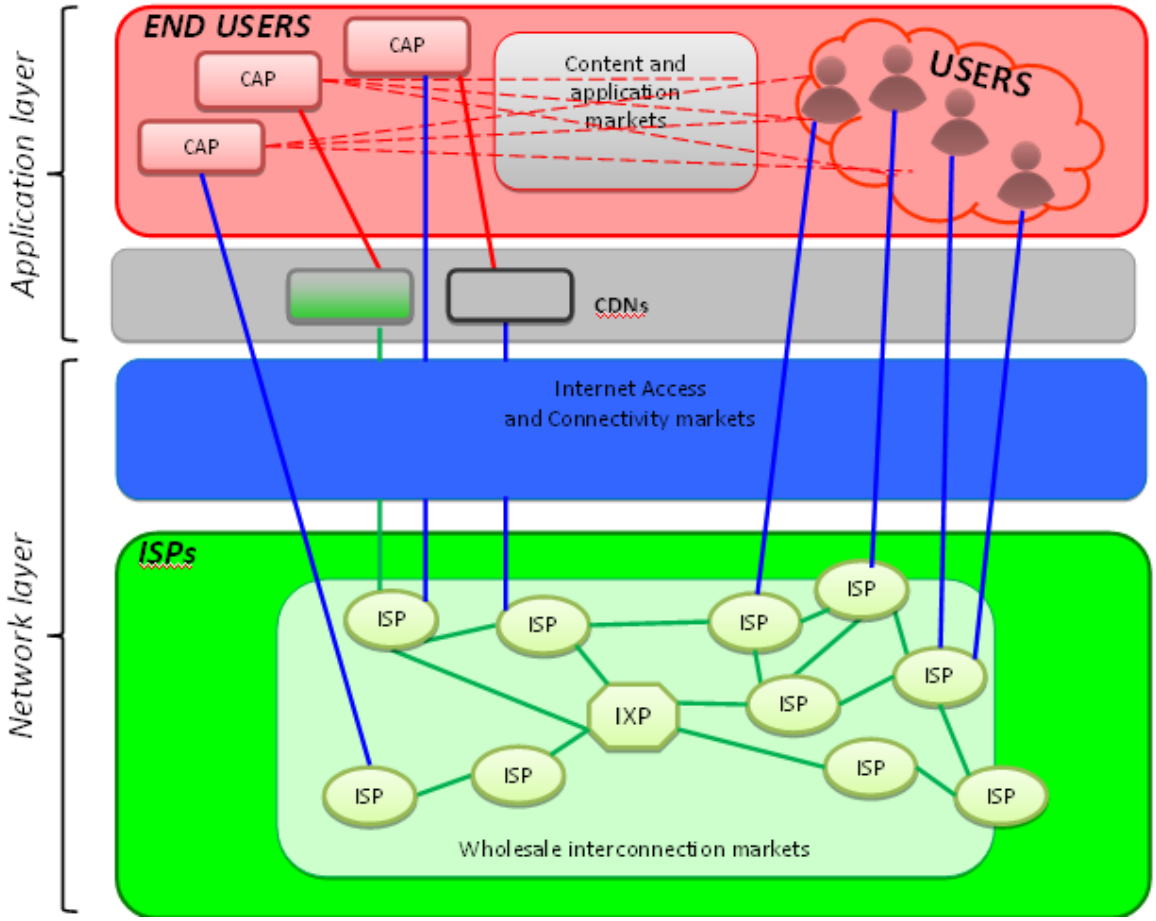

Fig. 9 Categoriile de servicii de comunicații electronice din cadrul lanțului de valori

Entitățile active pe piață (furnizorii de servicii de internet, furnizorii de conținut și aplicații și utilizatorii) care apar în figura de mai sus au fost descrise în capitolul 5.

CDNs (Content Delivery Networks) sunt rețele de livrare de conținut, care servesc la agregarea de conținut, de obicei, în folosul furnizorilor de aplicații și conținut. În principiu, CDN este un sistem de servere dezvoltat în cadrul rețelei furnizorului de servicii de internet, astfel încât furnizorii de aplicații și conținut să poată folosi conținutul spre a fi distribuit. În cadrul CDN, conținutul este multiplicat în copii pe servere strategic dispersate, iar direcționarea conținutului către utilizatori se face pe bază de proximitate.

Mai jos sunt prezentate concluziile BEREC cuprinse în Raportul privind analiza interconectării IP din punct de vedere al tendințelor în lanțul de valori, în contextul neutralității internetului.

- Apariția de CAP și CDN mari (Google, Akamai, Amazon) precum și a noi tipuri de acorduri de tip peering (de ex. peering regional) au contribuit la aplatizarea topologiei internetului. Granițele dintre jucători în lanțul de valori devin tot mai neclare, din moment ce jucătorii pot îndeplini funcționalități noi și/sau diferite;
- CAPs plătesc sume substanțiale pentru hosting și conectivitate. Mai mult decât atât, ei plătesc pentru servicii CDN care transmit conținutul către utilizator. În privința costurilor suportate de operatorii de rețea există probabilitatea ca acestea să fie deja acoperite în cadrul lanțului de valori al internetului (atât prin plățile din partea CAPs, cât și din partea utilizatorilor);

- CDNs au contribuit la furnizarea unei calități mai bune către utilizatori. Acest lucru poate însemna că este puțin probabil ca împărțirea traficului în clase de trafic să asigure nivelele de calitate implementate în acordurile de interconectare;
- Atâta vreme cât calitatea serviciului nu este garantată în afara rețelelor, CDN au un avantaj competitiv față de rețelele de tranzit, deoarece acestea pot contribui la livrarea de conținut cu o calitate mai bună către utilizatorii ISP conectați;
- Mai mulți ISP care furnizează conectivitate către utilizatori pe o scară largă dobândesc statut de Tier 1, în sensul că aceștia se bazează exclusiv pe peering și nu mai este nevoie să cumpere tranzit.

Calitatea serviciului în raport cu livrarea de tip best effort

- Deși transferul de date de tip best effort nu implică livrarea garantată a datelor, aceasta nu rezultă neapărat într-o performanță scăzută. Din contră, internetul de tip best effort implică, de cele mai multe ori, o calitate ridicată a experienței pentru utilizatori, chiar și în cazul aplicațiilor sensibile la timp, cum ar fi VoIP.
- În cadrul acordurilor de interconectare între rețelele IP nu se poate vorbi despre încălcarea principiului neutralității. O astfel de abatere poate fi observată doar în cadrul rețelei furnizorului și s-ar putea datora furnizării la o calitate diferențiată a serviciului.
- În internet, garantarea calității serviciului cap-la-cap nu este oferită în mod practic și nici realistă din punct de vedere tehnic.
- Până acum, interconectarea având calitatea serviciului garantată dincolo de granițele rețelei nu există, mărirea capacității reprezentând strategia potrivită în cazul congestiei.
- Posibile încălcări ale principiului neutralității cum ar fi blocarea sau limitarea traficului apar de obicei în rețelele ISPs și nu se regăsesc în cazul interconectării IP.
- Serviciile specializate sunt furnizate folosind protocolul IP, dar sunt operate în rețele IP în cadrul cărora sunt aplicate practici extensive de management al traficului, în scopul de a asigura caracteristicile adecvate ale serviciului. Prin urmare serviciile specializate pot furniza o calitate garantată a serviciului.
- În rețelele de tip best effort au fost dezvoltate mecanisme alternative în scopul de a crește performanța cap-la-cap a rețelei. Exemple sunt punctele terminale bazate pe controlul congestiei pentru reducerea încărcării traficului, utilizarea IXPs, precum și utilizarea tot mai frecventă a peering-ului. De asemenea, CDNs sunt folosite pentru a îmbunătăți percepția utilizatorului în privința calității aplicațiilor.

Principii referitoare la taxare

- Interconectarea se realizează în baza acordurilor de tip peering sau tranzit, într-un regim de tarifare în care fiecare furnizor suportă costurile de terminare a traficului provenind de la alți transportatori în propria sa rețea, tarifând exclusiv proprii utilizatori (bill & keep).
- Spre deosebire de traficul de voce din rețelele PSTN, datele nu sunt transportate pe o legătură (conexiune) de rețea dedicată, exclusivă și nu se poate stabili natura sau volumul unui anumit flux de date cap-la-cap. Pachetele aparținând aceluiași flux pot fi transmise pe rute diferite.
- Prin urmare, taxarea în cazul interconectării IP se face de obicei în funcție de capacitatea furnizată la punctul de interconectare și nu în funcție de locul de unde este originat sau este terminat traficul.
- Separarea nivelelor rețea și aplicație este o caracteristică specifică internetului best effort. Datorită acestei caracteristici, relațiile comerciale dintre CAP și utilizatori sunt posibile fără ca operatorul de rețea să fie implicat. În prezent, la nivel de aplicație, există un nivel de concurență și inovație fără precedent.

Aspecte privind reglementarea

- Actualul Cadru de Reglementare prevede faptul că autoritățile de reglementare pot impune obligația de interconectare într-un mod nediscriminatoriu. Cu toate acestea, nu furnizează neapărat un temei juridic pentru mandatarea peeringului gratuit.
- Până în prezent, piața interconectării IP s-a dezvoltat fără o intervenție semnificativă din partea reglementatorului.
- Perturbări în interconectarea IP, cauzate de litigiile dintre furnizori, ar putea conduce la situația în care nu pot fi atinse toate destinațiile din internet.
- Piețele din cadrul lanțului de valori sunt în continuă schimbare, implicând apariția unor noi tipuri de jucători, ca și de noi tipuri de acorduri de interconectare. Autoritățile de reglementare trebuie să înțeleagă mai bine aceste piețe.
- Abordările Autorităților de reglementare depind de la un stat la altul.
- Orice măsură poate fi dăunătoare, de aceea trebuie analizate cu atenție.

7. Proiecte BEREC prevăzute pentru 2014

Încă din anul 2010 BEREC a studiat mai multe aspecte legate de neutralitatea rețelelor, acumulând până în prezent experiență substanțială în acest sens. În tot acest timp, BEREC și-a exprimat opinia prin intermediul mai multor ghiduri și rapoarte pe tema mai multor aspecte, cum ar fi calitatea serviciului, interconectarea IP și transparența, iar principalele concluzii despre problema neutralității cuprind următoarele:

- Competiția ar trebui să disciplineze furnizorii și să asigure cele mai bune oferte pentru consumatori; un rol critic în acest sens îl au atât transparența cât și posibilitatea utilizatorului final de a schimba ușor furnizorul.
- Atât autoritatea națională de reglementare cât și utilizatorii finali ar trebui să poată monitoriza performanța aplicațiilor și a serviciului de acces la internet
- În cazul în care măsura de promovare a concurenței și transparenței se dovedește a fi insuficientă în combaterea degradării serviciului, autoritatea națională de reglementare ar trebui să intervină fără ezitare folosindu-se de instrumentele de reglementare existente (de exemplu impunerea unor cerințe minime de calitate)

BEREC va continua monitorizarea îndeaproape a evoluției pieței, încercând să se asigure de faptul că NRA vor putea răspunde în mod rapid și eficient oricărei evoluții viitoare legată de neutralitate. În acest sens, conform *Draft Work Programme 2014 Board of Regulators*[31], activitatea pe care BEREC își propune s-o desfășoare în direcția neutralității rețelelor în anul 2014 cuprinde două mari proiecte pentru anul 2014, anume: Monitorizarea calității serviciului și ECODEM (Ecosystem dynamics and demand side forces in net neutrality developments from an end-user perspective) -Dinamica ecosistemului internet și forțele din partea cererii.

Monitorizarea QoS

În cadrul acestui proiect, început încă din 2013 prin redacterea unui draft[32] al *Raportului de monitorizare a calității serviciului de acces la internet în contextul neutralității rețelelor* se are în vedere analiza unui sistem de monitorizare, care să asigure transparența pentru utilizatorii de servicii de comunicații electronice și să prevină degradarea serviciului furnizat de ISPs către utilizatorii finali. De

[31] http://berec.europa.eu/eng/document_register/subject_matter/berec/annual_work_programmes/3939-berec-work-programme-2014

[32] Versiunea integrală a documentului este disponibilă la următoarea adresă: http://berec.europa.eu/files/document_register_store/2014/3/BoR%20(14)%2024%20Draft%20BEREC%20Report%20on%20NN%20QoS%20Monitoring%20Report.pdf

menționat faptul că la momentul redactării Raportului ANCOM privind neutralitatea rețelelor, draftul mai sus amintit a fost supus consultării publice pe pagina web a BEREC.

În scopul atingerii obiectivelor propuse, acest raport prevede o abordare în trei pași: primul constă în determinarea modului în care sistemele deja existente pot fi folosite în scopul asigurării transparenței, al doilea constă în crearea unor recomandări pentru sisteme viitoare de monitorizare, iar al treilea reprezintă posibilitatea dezvoltării unei platforme comune de monitorizare, toate aceste etape fiind analizate și descrise în cadrul raportului.

De asemenea, raportul mai face referire la sistemul de măsurare a calității, aspectele tehnice ale diferitelor metode de măsurare (bazate pe software/hardware, active/pasive), ipoteza creării unei platforme multi-NRA de măsurare a calității, descrierea câtorva instrumente și platforme de măsurare a calității serviciului de acces la internet (Glasnost, Network Diagnostic Tool și NANO, respectiv RIPE Atlas și M-Lab), precum și prezentarea inițiativelor la nivel național a statelor UE în privința măsurării calității serviciilor (scopul aplicațiilor, conceptul măsurătorii, parametrii măsurați, etc.).

ECODEM

ECODEM (Dinamica ecosistemului internet și forțele din partea cererii) este un proiect concentrat pe percepția utilizatorului final în privința neutralității rețelelor.

Obiectivele proiectului constau în furnizarea unei mai bune înțelegeri (documentată, dovedită) asupra dinamicii pieței, în special din perspectiva utilizatorului final.

Proiectul își propune următoarele:

- Să înțeleagă de ce ISP au practici diferite de management al traficului în condiții (tehnice, legale și de piață) similare; în urma investigațiilor de management al traficului (TMI), s-a constatat că ISP care se confruntă cu aceleași constrângeri/condiții (creșterea traficului în rețea, piața competitivă), aplică diferite restricții sau prioritizări.
- Să înțeleagă în ce măsură așteptările consumatorilor și dinamica pieței sunt reflectate în oferte;
- Testerea ipotezei că problemele pot fi rezolvate simplu prin competiție, transparență și schimbarea furnizorului; faptul că problemele pot fi rezolvate folosind aceste instrumente, conduce la câteva presupuneri:
    - ✓ Că informațiile despre restricții sau prioritizări sunt tratate într-un mod transparent;
    - ✓ Că utilizatorii înțeleg implicațiile restricționărilor sau prioritizărilor;
    - ✓ Că utilizatorii pot folosi aceste informații atunci când iau decizii în privința alegerii unei oferte sau a unui furnizor;
    - ✓ Că schimbarea furnizorului se poate face ușor.

8. Neutralitatea rețelelor în România

În ceea ce privește acțiunile întreprinse în România, situația se prezintă astfel:

- în anul 2012 ANCOM și ApTI[33] au organizat (o dezbatere publică) un eveniment[34] pe tema neutralității rețelelor, la care au participat reprezentanți ai companiilor de comunicații, ai autorității de reglementare, ai consumatorilor și ai organizațiilor care protejează drepturile civile. S-au discutat aspecte privind neutralitatea internetului, reglementări și practici de management al traficului (caracterul lor rezonabil/nerezonabil), transparența, calitatea serviciului și politici de conținut.
- În 2013 ANCOM a organizat o primă întâlnire a Grupului de lucru pe tema neutralității rețelelor, la care au participat mai mulți actori de pe piața comunicațiilor electronice. În cadrul grupului de lucru au fost făcute mai multe sugestii de direcții ale acțiunilor grupului. De asemenea, a fost prezentată activitatea BEREC în domeniul neutralității internetului.

[33] Asociaţia pentru Tehnologie şi Internet

[34] Pentru mai multe informaţii accesaţi link-ul http://www.ancom.org.ro/nn-2012_4714

- În vederea asigurării transparenței cu privire la calitatea serviciului, în cursul anului 2014, ANCOM va pune la dispoziția publicului o aplicație interactivă prin intermediul căreia se pot măsura indicatorii tehnici de calitate. Astfel, prin intermediul acestei platforme se va testa calitatea serviciului de acces la internet între echipamentul terminal al utilizatorului final și un server de test amplasat într-un nod de tip internet exchange, rezultatele fiind afișate utilizatorilor.
- În 2014, ANCOM a prevăzut în planul de acțiuni modificarea Deciziei nr. 77/2009 privind obligațiile de informare a utilizatorilor finali de către furnizorii de servicii de comunicații electronice destinate publicului, în scopul creșterii transparenței și a gradului de informare a utilizatorilor finali.

Bibliografie

- *A framework for Quality of Service in the scope of Net Neutrality*-December 2011
- *Guidelines on Transparency in the scope of Net Neutrality: best practices and recommended approaches* -December 2011
- *BEREC's Response to the European Commission's consultation on the open Internet and net neutrality in Europe -September 2010*
- *BEREC findings on Traffic management and other practices resulting in restrictions to the open Internet in Europe* -May 2012
- *Summary of BEREC positions on net neutrality*
- *Report on differentiation practices and related competition issues in the context of Net Neutrality* -December 2012
- *An assessment of IP interconnection in the context of Net Neutrality* -December 2012
- *Guidelines for Quality of Service in the scope of Net Neutrality* -December 2012
- *BEREC response to EC questionnaire on specific aspects of transparency, traffic managementand switching in an Open Internet*
- *Voluntary industry code of practice on traffic management transparency for broadband services* -OFCOM
- *How to determine whether a traffic management practice is reasonable*- Scott Jordan
- http://www.f5.com/glossary/traffic-management/
- *Network traffic management and the evolving internet- IEEE 2010*
- *http://en.wikipedia.org/wiki/Routing*
- *Cisco Systems*

http://www.cisco.com/c/en/us/td/docs/ios/12_2/qos/configuration/guide/fqos_c/qcfconmg.html

- *http://mynetworkingwiki.com/index.php/Weighted_Fair_Queuing*
- *https://secure.wand.net.nz/pubs/19/html/node6.html*
- *http://www.cisco.com/c/en/us/td/docs/ios/12_2/qos/configuration/guide/fqos_c/qcfconav.html#wpxref13328*
- *http://www.routeralley.com/ra/docs/qos_congestion_avoidance.pdf*
- *http://www.cisco.com/c/en/us/td/docs/ios/12_2/qos/configuration/guide/fqos_c/qcfconav.html#wpxref11066*
- *Evaluation of Hybrid Scalable Video Coding for HTTP-based Adaptive Media Streaming with High-Definition Content*
- *http://www.cisco.com/c/en/us/td/docs/ios/12_2/qos/configuration/guide/fqos_c/qcfpolsh.html#wpxref26748*
  - http://www.cisco.com/c/dam/en/us/td/docs/nsite/wan_optimization/WANoptSolutionGd.pdf
- *http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfacls.html*
- *RFC 2001*
- *http://en.wikipedia.org/wiki/Fast_retransmit*

- *TCP Congestion Control- "Computer Networks A Systems Approach", Third Ed.,Peterson and Davie, Morgan Kaufmann, 2003*
- *Draft Work Programme 2014 Board of Regulators*
- *Monitoring quality of Internet access services in the context of net neutrality*- Draft BEREC report