Journal of Electrical Engineering and Information Technologies, Vol. **5,** No. 2, pp. 125–134 (2020)
Article 178 In print: ISSN 2545–4250
Received: October 10, 2020 On line: ISSN 2545–4269
Accepted: October 28, 2020 UDC: 004.77.052:621.391.08

Original scientific paper

NET NEUTRALITY ANALYSIS AND MECHANISMS FOR ITS ASSESSMENT

Kristijan Popovski[1], Toni Janevski[2]

[1]*ZTE Corporation, Skopje, North Macedonia*
[2]*Faculty of Electrical Engineering and Information Technologies,*
"Ss. Cyril and Methodius" University in Skopje, Skopje, North Macedonia
tonij@feit.ukim.edu.mk

A b s t r a c t: Internet's widespread use is mainly attributable to its best-effort concept, as well as being open to all users and services. The principle of net neutrality has been introduced, in essence, to safeguard this concept. Still, net neutrality faces contemporary challenges in the Western world by being continuously disputed or tested. In the United States related regulation has been reversed, while European stakeholders manage to balance and preserve net neutrality's importance. In that direction, the Macedonian regulation has been mostly in-line with that of the European Union. Even so, challenges grow as Internet service providers find various ways to impose Internet traffic differentiation. QoS measurement tools for net neutrality assessment are therefore of great importance, but shortcomings exist. This paper gives the argument that passive measurement tools are more robust in detecting any differentiation. Finally, a proposed model for passively measuring the crucial metric – data throughput – may prove to become better deployable than existing tools, with the goal of general net neutrality assessment.

Key words: net neutrality; Quality of Service (QoS); measurement; QoS tools; data throughput

АНАЛИЗА НА МРЕЖНАТА НЕУТРАЛНОСТ И МЕХАНИЗМИ ЗА НЕЈЗИНА ПРОЦЕНА

А п с т р а к т: Широката употреба на Интернетот главно се припишува на неговиот концепт на најдобар обид, како и на неговата отвореност спрема сите корисници и услуги. Принципот на мрежна неутралност е воведен, во суштина, заради заштита на тој концепт. Сепак, мрежната неутралност се соочува со современи предизвици во западниот свет на начин што постојано се оспорува или испитува. Во Соединетите Американски Држави односната регулатива е повлечена, додека европските засегнати страни сè уште успеваат да ја урамнотежат и зачуваат важноста на мрежната неутралност. Во таа насока, македонската регулатива е во најголем дел усогласена со онаа на Европската Унија. И покрај тоа, предизвиците растат паралелно со различните начини со кои провајдерите на интернетот наметнуваат диференцијација на интернет-сообраќајот. Оттука, алатките за мерење на квалитет на сервис заради процена на мрежната неутралност се од огромна важност, но постојат недостатоци. Овој труд аргументира дека алатките за пасивно мерење се поробусни во откривање на каква било диференцијација. Конечно, се предлага модел за пасивно мерење на клучната метрика, податочната брзина, кој може да се покаже како поефикасен за имплементација поради општа процена на мрежната неутралност.

Клучни зборови: мрежна неутралност; мерење на QoS; алатки за QoS; податочна брзина

1. INTRODUCTION

Since the early 2000s, net neutrality has emerged as a comprehensive way of identifying the openness of the Internet. In its broadest scope, the principle of net neutrality may be defined as a non-discriminatory treatment by Internet service providers (ISPs) of the Internet traffic, routed to and from end-users or content and application providers (CAPs), regardless of content and use. Notable allowed exemptions for net neutrality mainly include reasonable provider practices in order to prevent or

counter illegal activities; maintain network integrity; mitigate effects of network congestion; and in some national regulations, to exercise parental control. Ever since, this approach has been gradually introduced in national telecommunication regulations – initially in the United States, by ISPs being classified as common carrier services, followed by other Western world countries.

During the last three years, the principle of net neutrality has again begun attracting greater attention – only this time as a result to its repeal in the United States in June 2018 by the Federal Communications Commission (FCC). As opposed to net neutrality, ISPs in the United States may now impose so-called fast lanes of Internet traffic for CAPs who are willing to pay more in order to better reach their consumers. As per FCC's findings, merely greater ISP transparency would be enough, i.e. consumers would be better off by easily switching ISPs of choice [1]. Statistics show that, however, during the beginning of the repeal debate, 32% of the US population in developed areas were not able to choose between, at least, two ISPs offering modest 10/1 Mbit/s [2], which also falls well below FCC's benchmark speed of 25/3 Mbit/s [3]. Moreover, at the time of the repeal act (by June 2018), as much as 40% of the total US population could not choose between at least two different ISPs' offers of the same benchmark and the percentages evidently only increased by choosing higher data speed plans (as shown in Table 1). That situation had not changed much in the following year (by June 2019).

Other considerations supported by the FCC include the capital investment incentives in the telecommunication market – eventually one could argue there was hardly any substantial difference when compared to all industries' investments. Neither were they affected by important regulatory decisions during the 10-years period as can be seen in Figure 1. Some projects [4] introduce technical ways in which consumers could set their fast lane preferences in order to alleviate the net neutrality repeal, but this may, as well, prove essentially unfair – users would hardly be willing to include or even get to notice new-born services or start-up CAPs. Eventually, there have been some cases, as in [5], where economists have gone even further and have supported such fast lanes, comparing them to the traditional concept of fast postal delivery for users who pay more. Anyway, it could be argued that this comparison is inadequate because the principle of net neutrality never confronted the varying data plans offered to users of different profile, while CAPs indeed require level playing field. Finally, the existence of fast lanes may be absurdly discriminatory against consumers who usually subscribe for higher data speeds but are deprived of a specific high-quality service due to a lack of such ISP-CAP agreement.

Table 1

Percentage of the total US population where fixed ISPs are present (June 2018 and June 2019) [6]

Minimum data speed (Mbit/s)	Number of ISPs[a]							
	0		1		2		3+	
	06/'18	06/'19	06/'18	06/'19	06/'18	06/'19	06/'18	06/'19
dl: 4 ul: 1	5.16	5.1	21	21.19	62.25	62.16	11.59	11.55
dl: 10 ul: 1	5.5	5.33	21.67	21.82	61.6	61.6	11.23	11.25
dl: 25 ul: 3	7.98	7.71	32.32	32.06	51.81	51.93	7.89	8.3
dl: 100 ul: 10	11.27	9.65	41.21	39.97	41.67	43.9	5.84	6.48
dl: 250 ul: 25	27.03	14.17	50.27	53.88	21.09	29.08	1.61	2.87

[a] Satellite and fixed wireless are not included.
Satellite Internet rarely provides 25/3 Mbit/s, whereas fixed wireless is particularly inconsistent and is generally available where there is already an existing fixed internet service provider.

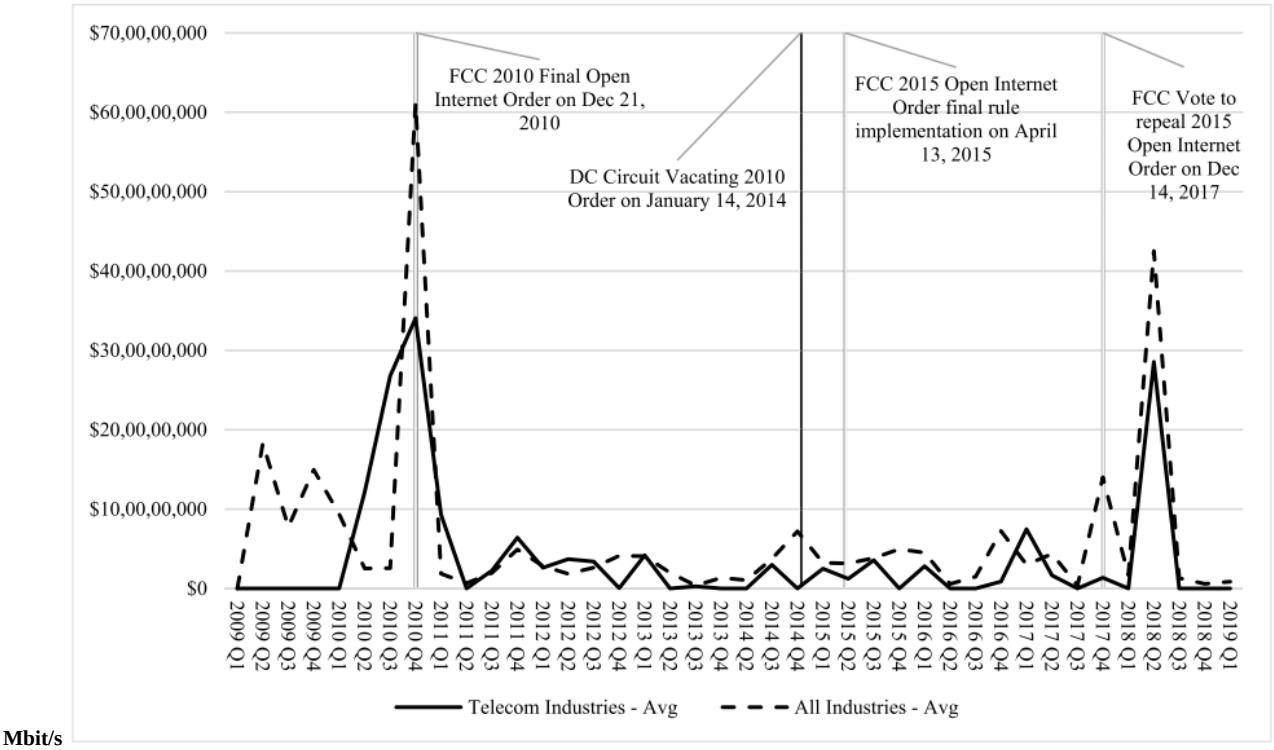

Fig. 1. Average capital expenditures by quarter for telecommunication and all industries [7]

In the European Union, despite the existence of a common regulation (EU Regulation 2015/2120) concerning the Open Internet which implicitly defines net neutrality (in article 3), there has been a lack of uniform interpretation by member-states and their respective national regulatory authorities (NRAs) during the first years after introduction. For example, zero-rating practices have spread in all but two countries [8]. Nevertheless, there are no signs of possible American scenario so far, which means net neutrality is there to stay. This is supported by the Body of European Regulators for Electronic Communications' (BEREC's) efforts to continuously clarify its Guidelines, with the October 2019 Draft being the most recent one.

Given all this, it can be understood that the concept of net neutrality poses challenges. ISPs in the United States are now allowed to differentiate Internet traffic, with FCC laying down transparency as a basis for users' individual decisions – yet such transparency has not always been explicit. On the other hand, Europe's BEREC launched a measurement tool tender in order to assist NRAs in detecting net neutrality issues [9]. In both cases Internet traffic differentiation needs to be detected which might be challenging considering the ways ISPs are practicing it – Deep Packet Inspection (DPI), IP header or TCP port based etc.

This paper is structured to cover different aspects of net neutrality assessment. We will outline existing QoS measurement tools with respect to net neutrality in Section 2. An analysis of the net neutrality and its measurement conditions in Macedonia will be presented in Section 3. A proposal for a new net neutrality assessment tool based on passive monitoring will be elaborated in Section 4. Finally, this paper is concluded in Section 5, along with future work considerations.

2. EXISTING TOOLS AND RELATED WORK

All existing QoS measurement tools rely on two testing methods, as recognized by BEREC – active (software or hardware based) and passive. The former is far more adopted by NRAs and more developed by third-party companies or CAPs than the latter.

Active testing tools may offer a better insight in specific situations – when an ISP wants to detect a specific section of low performance within its network; when users want to test against a specific external server; etc. One such example is Ookla's SpeedTest which maintains more than 9 000 servers worldwide. This tool allows a manual selection of a server which is mostly useful for testing the ISP leg,

by choosing a nearby server in another AS; or to test the only segment whose QoS the provider can guarantee – the last-mile within a user's ISP. In addition, Ookla's tool utilizes 5–8 concurrent TCP connections [10] to simulate real-life user experience. By contrast, the Network Diagnostic Tool (NDT) conforms to the stricter Bulk Transfer Capacity definition by IETF [11] in utilizing a single TCP connection. Its servers are far fewer since they are located at Internet Exchange Points (IXPs) [12] which may cause greater latency. Therefore, one could expect lower speed results for NDT. Anyway, this open-source tool may be used for identifying inner network issues as well.

One major drawback of dedicated measurement servers is that – by simply knowing their IP address – ISPs can easily prioritize traffic heading toward them. In this context, Netflix Fast.com's key advantage is the collocation of the testing servers and the servers used for video content delivery [13]. Users can therefore observe real-life data speed as if they were streaming videos. Nonetheless, this is an application-specific measurement. Where is another mobile tool which tests popular applications (YouTube, Netflix, Spotify, Skype etc.) by one-time recording of non-user original stream, creating a comparable stream by inverting the original's IP payload bits according to the application level protocol in use, and testing against a proprietary server [14]. This method has proven to work against any DPI-based differentiation that makes use of keyword matching. Still, Wehe shares a similar limitation as Ookla SpeedTest and NDT – it always measures against its own dedicated servers.

The Network Access Neutrality Observatory (NANO) is a rare example of a passive measurement tool – it tests actual application traffic originating from CAPs. It uses a statistical method to estimate causal effect, i.e. a given service is indicated to perform poorly when accessed from one ISP compared to another, provided that all other external factors (e.g. time, location, device operating system etc.) are equal [15]. For example, all users browsing via Internet Explorer would belong in a same stratum. Naturally, this stratification process requires a lot more samples from various users so that the tool would output relevant results, compared to active measurement tools – consequently small number of users negatively impacts the result; and the number of strata only grows larger as the values of external factors vary. A major obstacle, on the other hand, exists in the case when the majority of ISPs practice traffic differentiation – the tool compares a given ISP's performance to the mean performance of the rest of ISPs, therefore any end result becomes meaningless. At last, there have been no details for any widespread tests done by NANO.

Finally, some limitations exist for all measurement tools. Server distance (or latency) and overload; bad client configuration; traffic increase during specific period of the day; and many other factors affect the end results and they cannot be simply disregarded. Users' varying data plans, as well, cannot be easily deduced - no known tools have this ability.

3. NET NEUTRALITY ASSESSMENT IN MACEDONIA

A*) Regulation*

The Macedonian regulation regarding net neutrality and openness of the Internet – presented by 2014 Law on electronic communications and 2015 Rulebook by the Agency for Electronic Communications (AEK) – has been largely consistent with that of the EU. The most recent confirmation came in 2019 by the Government's National Broadband Plan [16] with reference to boosting the new 5G capabilities. Anyway, this cannot eliminate the principle of net neutrality for either older generation mobile networks, or for fixed Internet networks.

For that reason, similar challenges remain to be considered. For example, zero-rating offers by the two largest mobile network operators have been observed since the rise of over-the-top applications (Makedonski Telekom's *Speak Out* and A1's *Go Social* are recent examples as of October 2020). This matter could be addressed in line with BEREC's October 2019 revised Guidelines Draft [17], in particular: app-agnostic (i.e. regardless of specific application as long as they belong to a same service category) uncapped offers during a limited period of time; blocking zero-rated apps once data cap is reached (Makedonski Telekom's *Speak Out* is compliant with this); bundling new data plans with a free app subscription for a period of time etc.

B) *QoS measurement scenario*

A promising solution was announced in 2014 by introducing a national IXP [18]. Ideally, this was supposed to serve Internet traffic originating and terminating locally, avoiding any international routing. Equally important, according to BEREC's [19]

guidelines, this would stand for a perfect QoS measurement location – at the edge of all major ISPs, as well as sharing the same user traffic path.

However, after a detailed analysis based on *traceroute* queries (i.e. queries of IP packet routes via OSI-3 level nodes) to 5 typical websites using 3 major ISPs, as in Table 2, that hold 87% of all user contracts in the country [20], it can be argued that there is a lack of operational national IXP. Specifically, in some cases ISPs used *peering* interconnection (e.g. A-1, A-2, C-1) as a result, whereas evident is also the use of foreign IXPs (e.g. B-2, B-5). In addition, Internet traffic exchanged between same two ISPs uses different IXPs depending on the direction of traffic (comparing B-2 and C-1), while a last-mile tier-3 ISP (Telekabel) purchases transit services from different ISPs based on location – all A cases apply for a Skopje user whose traffic transits via Neotel's network, but a Bitola user's traffic is routed via an interconnection to Makedonski Telekom. The whole analysis is illustrated in Figure 2.

Given the previous analysis we suggest, in line with BEREC, that several measurement servers be placed at major ISPs' interconnection (or peering) nodes and that a statistical average be made – this would provide a better estimate of the ISP's QoS. This ensures the measurement traffic shares the same routes with the user traffic. In theory, all tiers' infrastructure may affect the QoS. However, global tier-1 networks provide enough bandwidth as discussed in [21], thus traffic growth and maintaining favourable QoS poses challenges primarily to last-mile connections and tier-3 ISPs. In this context, an observation can be made at the IXPs during the 2020 coronavirus pandemic which has caused an excess of Internet traffic – global IXPs such as those in Frankfurt and Amsterdam are reported to be able to bear the traffic increase, even if it were doubled [22].

T a b l e 2

Cases by visited website and ISP in use

	Telekabel	Makedonski Telekom	A1
fitr.mk	A-1	B-1	C-1
jsp.com.mk	A-2	B-2	C-2
ukim.edu.mk	A-3	B-3	C-3
berec.europa.eu	A-4	B-4	C-4
neotel.mk	A-5	B-5	C-5

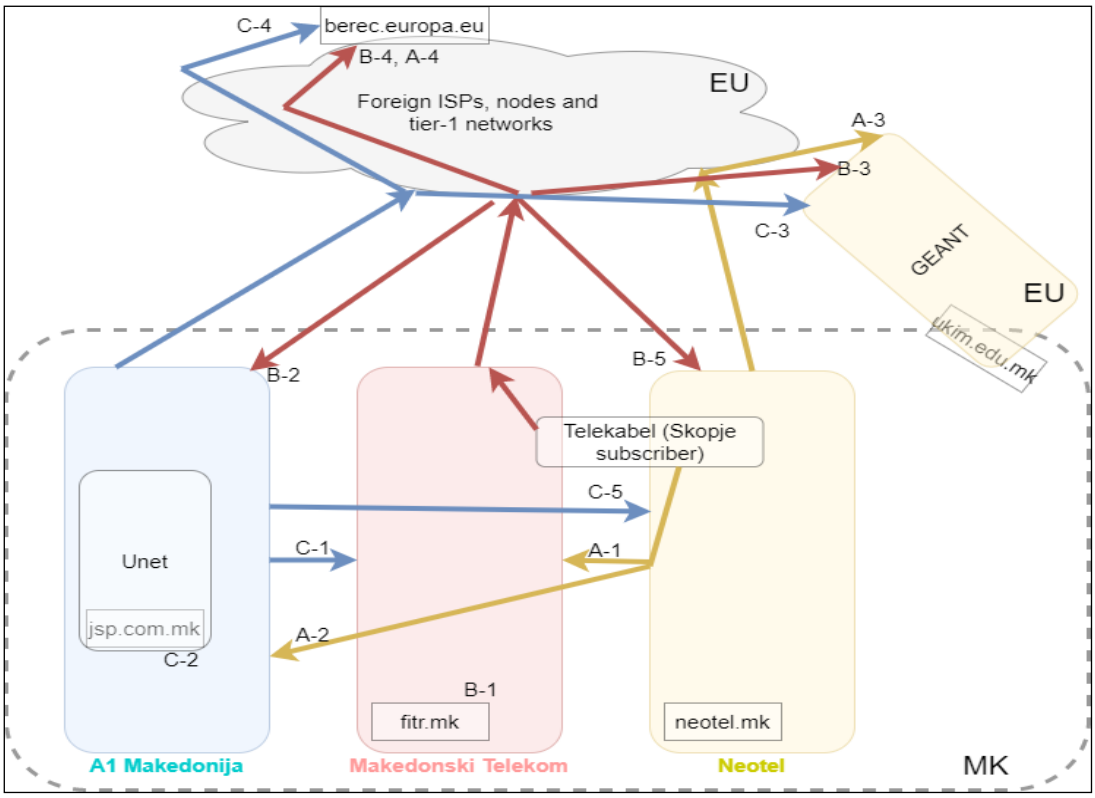

Fig. 2. Illustration of analyzed traffic routing

C) *AEK's Speedtest tool*

Regarding QoS testing, AEK has provided its Speedtest tool. During multiple tests, it was determined that the tool used 5 concurrent TCP connections in order to better saturate the link. This was verified using a packet tracing software by filtering TCP-SYN messages (Figure 3) – TCP-ACK and TCP-SYN_ACK messages were filtered out because only the number of established TCP connections was of interest. Furthermore, the tool tests against a single measurement server. A few *traceroute* queries showed that the three major ISPs in Table 2 were directly interconnected to Speedtest's test server. This leads to the conclusion that, given the circumstances, the server's location within another Autonomous System (AS) is optimal – it allows a complete assessment of the quality of Internet access service beyond the ISP leg, while being close to it, as suggested by BEREC. Nevertheless, Internet traffic rarely does originate and terminate within the network of a single AS, even more, it is often being routed internationally in order to reach popular global CAPs. Such measurement servers need to ensure ordinary user traffic will not bypass it and route via completely different route, which is not the case for AEK's. The test server's redundancy is unknown so possible overload issues may not be accounted for. Finally, ISPs may always designate special treatment to well-known servers, such as that of AEK Speedtest, with the aim of presenting better results to end users.

22724	211.954755	10.3.6.102	88.85.106.109	TCP	66 60180 → 443 [SYN] Seq=0 Win
22751	212.116384	10.3.6.102	88.85.106.109	TCP	66 60181 → 443 [SYN] Seq=0 Win
22794	212.216207	10.3.6.102	88.85.106.109	TCP	66 60182 → 443 [SYN] Seq=0 Win
22862	212.317209	10.3.6.102	88.85.106.109	TCP	66 60183 → 443 [SYN] Seq=0 Win
22932	212.430158	10.3.6.102	88.85.106.109	TCP	66 60184 → 443 [SYN] Seq=0 Win

Fig. 3. Filtered concurrent TCP connections

4. PROPOSED MODEL FOR A NET NEUTRALITY TOOL

In this section a new model for a net neutrality assessment will be proposed. This proposal is essentially different to the existing tools and studied methods analyzed in Section 3. The model partly stems from an announcement of Google for introducing a badge for slow-loading websites in Google Chrome exploiting historical statistics analysis [23]. Similar mechanism via web-browser activity is used in the proposed model which is based on passive measurements and calculates Internet throughput as the single most important and sometimes ambiguous metric.

D). *Motives for a new model*

One aspect should be the complexity of the implementation. Existing tools based on active measurements may involve network modifications such as installing a logical measurement server within the ISP's infrastructure, or at a separate, third-party (incl. CAP, NRA) network infrastructure. Software-based tools require a certain level of technical skills of the users (e.g. application installation, accessing various web-based tools etc.) and need to run on different operating systems, device types and configurations; whereas costly and non-scalable hardware-based probing not only requires changes at the end-user's premises, but they often take a lot of time to complete and usually partially or entirely restrict parallel internet activities of the user.

With respect to active measurements, finding a truly centralized reference solution for all ISPs in a country is a complex task – no two ISPs have same infrastructure, neither does the Internet traffic follow the same path every time. Yet more, user traffic may never be routed via the same path as the measurement traffic (as was the case in AEK's solution). In fact, even if all these conditions were met, ISPs would still be able to recognize measurement traffic (as laid in Section 2) and intentionally prioritize it to deliver better throughput results.

On the other hand, there has been no record of operational passive measurement tools, which may, of course, be more robust in terms of detection by ISPs. Therefore, the goal of this model is to maintain passive detection, as well as being universally adopted.

E) *External information collection*

For the model to be able to properly compare throughput speeds of different users and their respective ISPs, external information needs to be collected. This is easily obtainable and implemented in existing tools (e.g. BEREC tendered Alladin Nettest provides detailed statistics).

First, the public IP address of the device may be looked up within online IP registers (such as the *RIPE network*, *whoismyisp.org* etc.) or simple *whois* queries in order to provide relevant ISP information (e.g. AS number).

Second, geolocation can be additionally confirmed via GPS enabling which has been already adopted in all modern browsers.

Third, all web-browsers provide compatibility (desktop and mobile) for *UserAgents* in their console access which present additional OS and browser information relevant to the comparison. For example, Figure 4 shows the browser model and version, as well as the x64 bit platform. Similarly, Figure 5 shows the result for the number of logical processor cores available at the client device. Such information is essential for eventual comparison as they, both, may adversely affect the user experience and data throughput.

```
> navigator.userAgent
- "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/81.0.4044.129 Safari/537.36"
```

Fig. 4. UserAgent information

```
> navigator.hardwareConcurrency
- 4
```

Fig. 5. Processor cores information

F) *Calculation of data throughput*

Data throughput is the crucial metric that greatly affects net neutrality. This model might not calculate the highest possible throughput value provided by an ISP (e.g. Video streaming may not necessarily use all available bandwidth due to CAP limitations or server overload), but it does give an insight into what a user normally experiences during everyday activities via web browsers.

Modern web browsers have an integrated *DevTools Network* tab which offers a detailed insight in the network activities of any web session. These contain all data uploads and downloads, as well.

In order to simplify the data throughput calculation, we are using a single .jpg file with a size of 40 MB. This size is considered to be sufficient to allow TCP to achieve acceptable speeds, with respect to its window size growth. Also, content caching has been turned off to prevent any false outcomes. The .jpg file is being downloaded from an external web server (https://effigis.com/wp-content /uploads/2015/02/Airbus_Pleiades_50cm_8b *it_RGB_Yogyakarta.jpg;* accessed on 10-Jan-2020).

This download session's network tab is shown on Figure 6. According to the outcome of the download session, the total duration of this traffic flow is 35.1 s while the total transferred content accounts for 39.10 MB, out of which, we can calculate the average data throughput – 8.91 Mbit/s. Additionally, the web browser uses 3 concurrent TCP connections which corresponds better to the real-time scenario, as opposed to tools that use a single connection (e.g. NDT).

The upload data throughput is calculated similarly using a commercial web server (IP address: 89.221.216.129; accessed on 10-Jan-2020) allowing uploads and the same .jpg file. Such server is selected in order to avoid any kind of file compression which would output unexpected results. Figure 7 shows the network activity of the upload session. According to the upload session outcome, the total transferred content again accounts for 39.10 MB, whereas the total runtime of the traffic flow is 9.03 s (found under *Time* column for *upload.php* record on Figure 7). Hence, the average upload throughput stands at 34.64 Mbit/s.

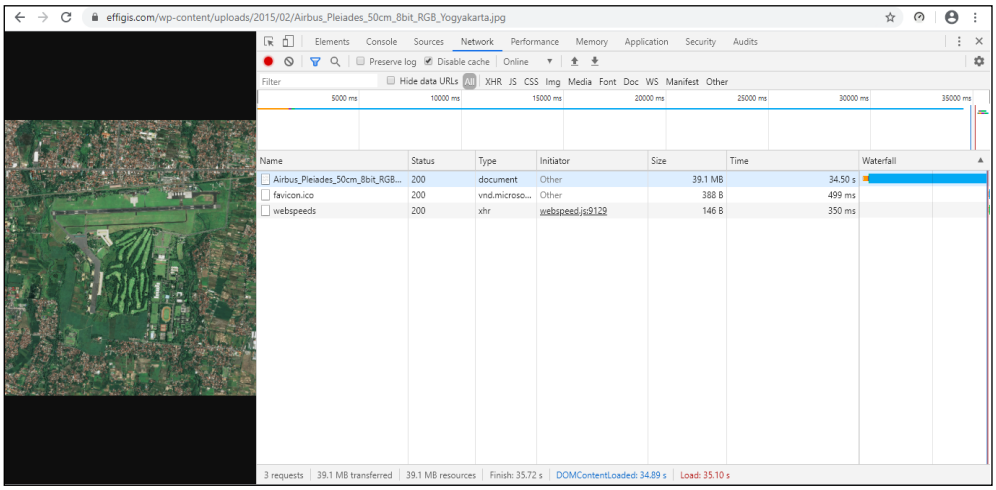

Fig. 6. Network activities display during .jpg file download

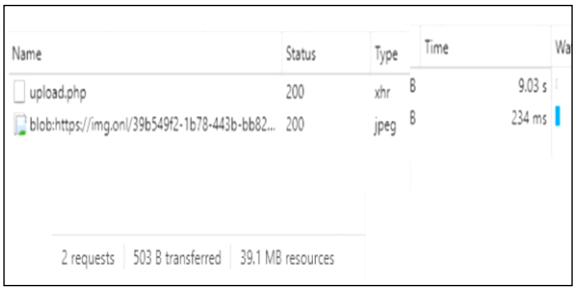

Fig. 7. Network activities display during .jpg file upload

G) *Verification of data throughput results*

A browser-independent verification of these calculations is necessary to be done in order to claim validity of the results. Therefore, a packet analyzer software is needed. In this case, Wireshark was used.

Packet tracing was done simultaneously during each of the download and upload sessions. Figures 8 and 9 (column *Displayed*) present the bitrate graph and the average bitrate statistics for the download session, respectively. Comparing this result to the one obtained previously (Section 4, Sub-section C), an insignificant variation of about 1 Mbit/s can be observed. Such comparisons were done 6 times, i.e. 6 independent measurements, with results being displayed in Table 3. Likewise, comparison results for the upload traffic are shown in Table 4 where, again, the absolute difference is insignificant, at about 2 Mbit/s, which may be attributed to the slight manual shifts of the captured packets frame filter done in Wireshark. Any unintentional shifts, nevertheless, do not affect the initial goal of this check.

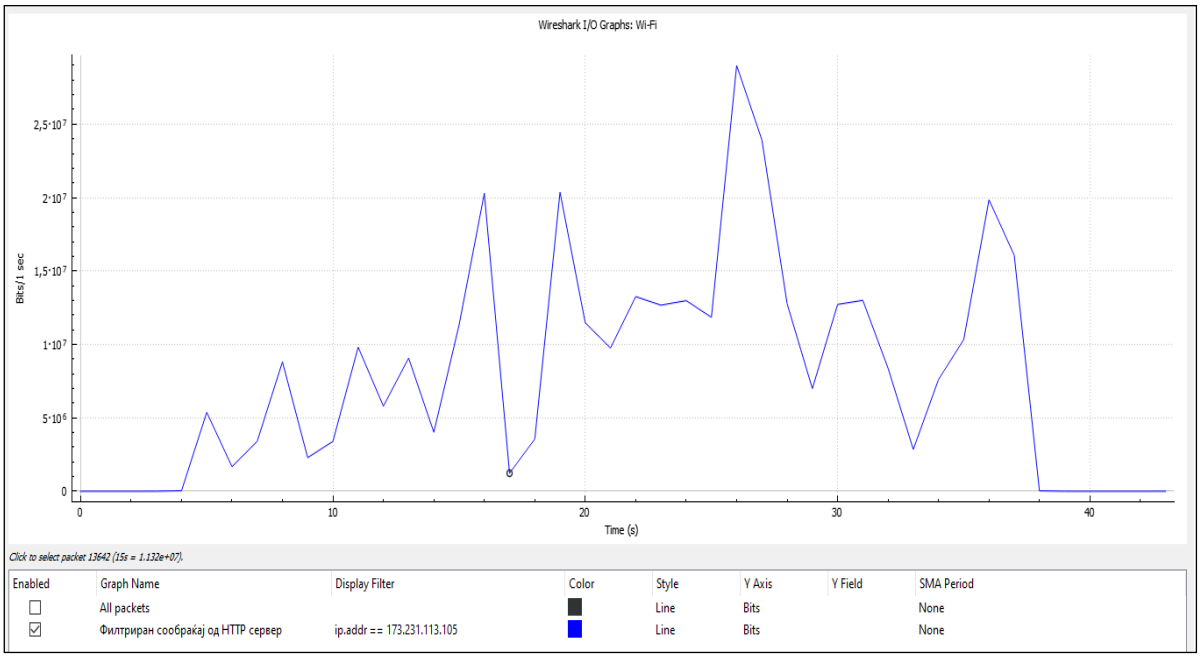

Fig. 8. Bitrate graph during file download.

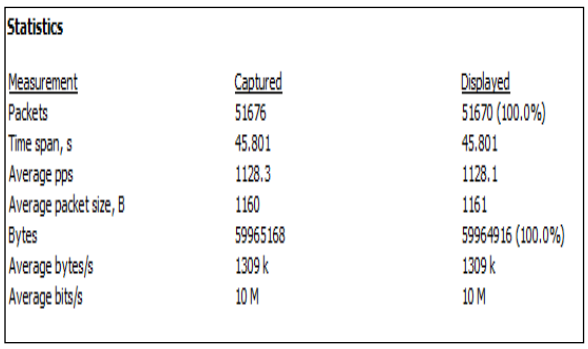

Fig. 9. Bitrate statistics for the selected download session

T a b l e 3

Download bitrate results comparison

	Avg. dl. throughput of the traffic flow (Mbit/s)					
	1 meas.	2 meas.	3 meas.	4 meas.	5 meas.	6 meas.
Google Chrome	8.91	16.00	10.00	10.83	18.20	12.07
Wireshark	10.00	14.50	9.47	11.00	19.00	11.00
Abs. difference	1.09	1.50	0.53	0.17	0.80	1.07

T a b l e 4

Upload bitrate results comparison

	Avg. ul. throughput of the traffic flow (in Mbit/s)					
	1 meas.	2 meas.	3 meas.	4 meas.	5 meas.	6 meas.
Google Chrome	34.64	37.82	34.83	35.16	38.91	29.02
Wireshark	36.00	36.00	34.00	34.00	41.00	30.00
Abs. difference	1.36	1.82	0.83	1.16	2.09	0.98

5. CONCLUSION AND FUTURE WORK

We analyzed the reasons for the constant need of net neutrality assessment tools that provide clarified and simple end results. It was argued that these tools are required however stringent or flexible the principle of net neutrality may be.

The current situation in Macedonia regarding net neutrality has been reviewed. AEK's current tool is optimal enough given the circumstances and possible suggestions have been given in order to improve assessment.

There is no explicit way of concluding which of the existing QoS tools is the most complete, if any. However, we find that tests are more comprehensive when having a big enough pool to choose a measurement server from, while open-source tools are suitable for resolving internal networking issues. Additionally, ISPs' efforts to prioritize active measurement traffic become meaningless when a significant number of users perform simultaneously – highly unlikely scenario, however.

For that reason, this paper proposed a more robust browser-based passive measurement model which is believed to be more universally deployable, compared to existing passive tools. The model's throughput calculation method was validated by a third-party software. The browser's network activities were presented to record HTTP traffic. However, many streaming services use HTTP based video protocols (e.g. Netflix uses DASH, Apple uses HTTP live streaming etc.). Even more, this applies for YouTube's RTSP (Real Time Streaming Protocol) whose traffic is also recorded, as well as sessions by several BitTorrent browser extensions.

Future work may involve exploring mobile solutions, delivering clarified results for a mixture of various types of background data streams and systematic stratification of external factors relevant to the assessment.

REFERENCES

[1] Gilroy, A. A.: *The net neutrailty debate: Access to broadband networks*, Congressional Research Service, p. 11, April 2019.

[2] Federal Communications Commission: *FCC fact sheet – Restoring Internet freedom*, p. 71, 2017.

[3] Federal Communications Commission: *2018 Broadband deployment report*, p. 6, February 2018.

[4] Yiakoumis, Y., Katti, S., McKeown, N.: Neutral net neutrality, *Proceedings of the 2016 ACM SIGCOMM Conference*, ser. SIGCOMM '16. New York, NY, USA: ACM, 2016.

[5] Faulhaber, G. R.: Economics of net neutrality: A review, *Communications & Convergence Review*, Vol. **3**, No. 1, 2011.

[6] N. N.: Federal Communications Commission, https://broadbandmap.fcc.gov/#/ [Accessed: 15-Dec-2019].

[7] Hooton, C. A.: Testing the economics of the net neutrality debate, *Telecommunication Policy*, Elsevier, September 2019.

[8] Lohninger, T. et al.: *The Net Neutrality Situation in the EU: Evaluation of the First Two Years of Enforcement*, Epicenter.works, Vienna, 2019.

[9] N.N.: Body of European Regulators for Electronic Communications, https://berec.europa.eu/eng/news_and_ publications/whats_new/5045-net-neutrality-measurement-tool-result-of-the-tender [Accessed: 23-Nov-2019].

[10] N. N.: Ookl*a*, https://support.ookla.com/hc/en-us/articles/360017436132-Optimizing-Server-Performance [Accessed: 19-Dec-2019]

[11] IETF, *RFC 3148: A Framework for Defining Empirical Bulk Transfer Capacity Metrics*, RFC 3148. DOI 10.17487/RFC3148, July 2001.

[12] N. N.: *Measurement Lab*, https:// www. Measurementlab.net/status [Accessed: 07-Dec-2019].

[13] N. N.: Netflix, https://media.netflix.com/en/company-blog/fast-com-now-measures-latency-and-upload-speed [Accessed: 08-Dec-2019].

[14] Li, F., Niaki, A. A., Choffnes, D., Gill, P., Mislove, A.: A large-scale analysis of deployed traffic differentiation practices, In: *SIGCOMM '19: 2019 Conference of the ACM Special Interest Group on Data Communication*, Beijing, August 19–23, 2019.

[15] Tariq, M. B., Motiwala, M., Feamster, N., Ammar, M.: Detecting network neutrality violations with causal interference, In: *Proceedings of the 5th International Conference on Emerging Networking Experiments and Technoloies*, ACM, 2009.

[16] Ministry of Information Society and Administration (N. Macedonia), *National Operational Brodband Plan*, p. 38, April 2019.

[17] Body of European Regulators for Electronic Communications, *Draft BEREC guidelines on the implementation of the open Internet regulation*, pp. 13–14, October 2019.

[18] N. N.: *Министерство за информатичко општество и администрација*, http://arhiva.mioa.gov.mk/?q =node/3 658 [Accessed: 25-Nov-2019]

[19] Body of European Regulators for Electronic Communications, *Monitoring quality of Internet access services in the context of net neutrality*, pp. 24–30, September 2014.

[20] Агенција за електронски комуникации, *Извештај за развој на пазарот за електронски комуникации во првиот квартал од 2019 година*, 2019.

[21] Rose, C.: Internet capacity, network traffic and net neurality, *International Journal of Management & Information Systems*, Vol. **14**, No. 5, p. 10 (2010).

[22] N. N.: *Politico*, https://www.politico.eu/article/coronaviruscovid19-internet-data-work-home-mobile-internet/ [Accessed: 01-May-2020]

[23] N. N.: *Chromium Team*, https://blog.chromium.org/2019/11/moving-towards-faster-web.html [Accessed: 12-Nov - 2019.