IP Performance Working Group
Internet-Draft
Intended status: Informational
Expires: February 28, 2018

K. Nieminen
FICORA

August 28, 2017

Net Neutrality Measurements: Regulatory Use Case and Problem Statement
draft-nieminen-ippm-nn-measurements-01.txt

Abstract

This document describes a regulatory use case for net neutrality measurements based on the new European open internet regulation. The purpose of this document is to give sufficient details for developing the actual net neutrality measurement metrics.

This document describes the problem statement. According to the Regulation European regulators has to supervise and enforce the net neutrality obligations. Especially the reliability of measurement results is important. However, monitoring net neutrality is a complex topic lacking standardized measurements.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on February 28, 2018.

Copyright Notice

Table of Contents

1. Introduction

According to the European open internet regulation [1], providers of internet access services shall treat all traffic equally, when providing internet access services, without discrimination, restriction or interference, and irrespective of the sender and receiver, the content accessed or distributed, the applications or services used or provided, or the terminal equipment used.

The Regulation allows only few exceptions for this rule that are subject to strict interpretation and to proportionality requirements.

The Regulation imposes an obligation for European regulators to closely monitor and ensure compliance with the Regulation. Regulators must also promote the continued availability of non-discriminatory internet access services at levels of quality that reflect advances in technology.

The Regulation imposes also new transparency obligations for internet access service contract conditions. Regarding fixed networks, internet access service providers must publish among other things a clear and comprehensible explanation of the minimum, normally available, maximum and advertised download and upload speeds.

The Body of European Regulators for Electronic Communications (BEREC) has given guidelines on implementation of the Regulation [2]. The guidelines provide further information regarding the regulatory use cases.

This document strives to provide sufficient details about regulatory use cases for developing the actual net neutrality measurement metrics.

Although legal challenges can change the status of policy, the take-away for IPPM purposes is that many policy-makers are looking for measurement solutions to assist them in discovering discriminatory treatment of traffic flows. The exact definitions and requirements vary from one jurisdiction to another.

2. Problem statement

The regulators have a need to reliably assess violation of net neutrality with respect to the recently published BEREC guidelines on net neutrality and the underpinning EU legislation. In the broader sense, the regulators' need is to determine whether illegal traffic management practices is being applied to end-user traffic as per application, as well as monitor the evolution of the performance of the internet access service (IAS) over time.

It is envisaged that in order to carry out such assessment reliably, a reliable technical measurement of end-user Internet traffic behaviour needs to be conducted.

In 2015, Ofcom (communications regulator in the UK) commissioned a study to better understand the existing techniques that could be potentially used to detect traffic management. The study identified a number of techniques that have been developed and that are able to detect presence of particular kinds of differential traffic management. The study also found that a gap exists for effective detection of the presence of traffic management along the digital delivery chain, but that a potential standardized solution may still be possible. The study concluded that further work is required to develop a broader framework for traffic management detection solution.

When measurement tasks are run by an end-user, end-user environment specific factors like cross-traffic, measurement interface (fixed/wireless), firewalls, client operating system and hardware can influence the measurement result. These factors have to be detected and taken into account when assessing measurements performed by end-users. The topic is discussed further under Section 3.4.

According to BEREC guidelines speed should be calculated based on IP packet payload. Currently BEREC is also considering using TCP packet payload as raw sockets are not universally available to standard users on most operating systems. For software based crowdsourcing approach it is essential that measurements can be performed using all common operating systems. Measurements should also support measurement client software installed by the end-user and as well as web browser based measurements.

The European Regulation requires internet service providers (ISPs) to specify new speed values for example minimum, maximum, and normally available speeds in fixed network. The measurement use case is to assess if these contractual speed values are met. The problem is to define measurements that can be run by end-users and is accurate enough to have legal value.

In addition to the mandatory requirements there are features that should be taken into account when planning the measurements to make them more usable and user friendly such as that the measurement does not block the internet access usage for whole day and does not generate excessive network load.

In principle, any solution should be equally applicable to both fixed and mobile Internet access services from narrow band to multi-gigabit connections. Certain variations may be accepted if they can be justified.

3. Regulatory use cases

Some regulatory use cases are already listed at a high level in RFC 7536 [3]. The purpose is to build on these use cases to further elaborate what is needed to fulfil EU regulatory

requirements in view of the recent EU legislation and BEREC guidelines publications. This document targets the level of detail that is sufficient for developing actual measurement metrics and methodologies.

The goal of this document is to help to understand what metrics need to be defined and how they should be measured in order to produce repeatable results with high degree of accuracy. This document also gives a high level explanation of how these measurement tasks and results can be used for assessing net neutrality in different regulatory use cases.

The identified high-level measurement tasks are:

- Monitoring the performance of internet access services
- Detecting traffic management practices that impact the availability of individual applications
- Detecting traffic management practices that impact the quality of service for individual applications
- Detecting end-user dependent factors that may impact the measurement results

An end-user should be able to run a measurement process from an appropriate client. A regulator may provide additional complementary tests as part of a larger suite of testing. Both panel based and crowdsource solutions could be considered. It is possible to use both active and passive measurements to fulfil the regulatory requirements.

The solutions should be based on a minimum measurement time and data volume in order to ensure the validity of the measurements while taking care to avoid the possibility of harmful effect on end-user’s Internet consumption.

3.1. Monitoring the performance of internet access services

This use case is used to measure speed and other relevant internet access service (IAS) quality of service (QoS) parameters (e.g. delay, jitter and packet loss) for the IAS as a whole. It enables end-users to check their individual internet access speed and whether the IAS performance meets what has been specified in the

contract. This has traditionally been the main motivation for end-users to use the tool provided by regulators.

Regulators may also run these measurements independently of any net neutrality assessment and use this information for multiple purposes such as increasing transparency in service provisioning (e.g. coverage maps) and monitoring the overall IAS quality, which may be aimed at:

- Ascertaining whether (or not) specialised services are provided at the expense of IAS, and/or
- Determining whether IAS performance is evolving in tandem with advances in technology.

The European open internet regulation [1] states that an end-user may use a monitoring mechanism certified by the regulator to check that the performance meets what has been specified in the contract. This measurement information can be used for triggering the remedies available to the consumer in accordance with national law.

BEREC guidelines [2] defines further that the certified monitoring mechanism should mitigate, to the extent possible, confounding factors which are internal to the user environment. Examples of these factors include existing cross-traffic and the usage of wireless/wireline interfaces.

According to BEREC guidelines speed should be calculated based on IP packet payload. Measurements should also be performed beyond the internet service provider (ISP) leg.

According to the Regulation ISPs must specify the minimum, normally available, maximum and advertised download and upload speed in their fixed network contracts. For mobile network subscriptions ISPs must specify estimated maximum and advertised download and upload speeds.

According to the recitals of the Regulation the normally available speed is understood to be the speed that an end-user could expect to receive most of the time when accessing the service. BEREC has given further guidance that the speed should be available during the specified daily period. For example a regulator may set a requirement that the normally available speed should be available during off-peak hours and 90% of time over peak hours, or 95% over the whole day.

Other factors that require special attention are how the minimum and maximum speed should be measured. According to BEREC guidelines the

- maximum speed is the speed that an end-user could expect to receive at least some of the time (e.g. at least once a day).

- minimum speed is the lowest speed that the ISP undertakes to deliver to the end-user. In principle, the actual speed should not be lower than the minimum speed, except in cases of interruption of the IAS.

Number and distribution of measurement tasks should be defined so that the adequate confidence level such as 95% is achieved.

3.2. Detecting traffic management practices that impact the availability of individual applications

The goal of this use case is to detect traffic management practices that affect the connectivity and availability of content, applications and services. Examples of this kind of practices may include blocking communication ports, VoIP and P2P file sharing applications in addition to other web content like streaming services, network based parental control and ad-blocking.

Internet service providers may use several different traffic management practices that block the connectivity to content, applications and services. Examples of these traffic management practices include: - Blocked communication ports

- IP addresses blocking
- DNS manipulation and HTTP proxy blocking
- Content or application based blocking with deep packet inspection

The challenge is to define specific measurement tasks that allow regulators to detect any blocked applications. A solution should minimise the probability of false positives. In principle, the solution is to comprise of measurement metric(s) and respective measurement methodology(s); as well as quantification of the probability of false positives.

3.3. Detecting traffic management practices that impact the quality of service for individual applications

The goal of this use case is to detect possible unequal treatment of traffic namely prioritisation and/or throttling of applications.

These traffic management practices may be detected by measuring the QoS experienced by the application and comparing the results with the QoS measurement results for the same IAS subscriptions and with the similar application specific QoS measurement results from other users and ISPs. Other techniques may also be possible.

A solution is required that correctly identifies whether prioritisation and/or throttling of applications is taking place, with minimum probability of false positives. In principle, the solution is to comprise of measurement metric(s) and respective measurement methodology(s); as well as quantification of the probability of false positives.

For this case, in particular, regulator may need to conduct additional complementary measurement tasks as part of a larger suite of testing, in order to eliminate any false positives.

3.4. Detecting end-user dependent factors that may impact the measurement results

Especially when measurements are run by an end-user in a crowdsourcing measurement setup, the local environment specific factors like cross-traffic, interface type (fixed/wireless), firewalls, processor load, client operating system and hardware can influence the measurement result.

It is preferred that the measurement client should capture this additional data of the end user local environment. This environment data can then be used in assessing the validity of the measurement results with the aim of improving overall accuracy and minimising false positives.

In principle, the solution is to comprise of measurement metric(s) and respective measurement methodology(s), and how this environment data can be used to ascertain measurement reliability in each use case.

4. Security Considerations

This document defines a use case and problem statement for net neutrality measurements. Security considerations for specific measurements will be discussed in solution documents.

5. IANA Considerations

This document includes no requests to the IANA.

6. References

6.1. Informative References

[1] Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union, November 2015, <http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32015R2120>.

[2] BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules, August 2016, <http://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/6160-berec-guidelines-on-the-implementation-by-national-regulators-of-european-net-neutrality-rules>.

[3] Linsner, M., Eardley, P., Burbridge, T. and Sorensen, F., "Large-Scale Broadband Measurement Use Cases", RFC 7536, May 2015, <http://www.rfc-editor.org/info/rfc7536>.

7. Acknowledgements

The author wish to thank Ahmed Aldabbagh, Mick Fox, Jose Hernan, Frode Sorensen and Volker Sypli for their invaluable comments and contributions.

This document was prepared using 2-Word-v2.0.template.dot.

Author's Address

Klaus Nieminen
FICORA
Itamerenkatu 3 A, P.O Box 313
Finland

Email: klaus.nieminen@ficora.fi