arcep
autorité de régulation
des communications électroniques
et des postes

RÉPUBLIQUE FRANCAISE

2018 Code of conduct on internet quality of service

FOR MEASUREMENT AND TESTING STAKEHOLDERS

December 20, 2018

ISSN n°2258-3106

2018 Code of conduct on internet quality of service

For measurement and testing stakeholders

The Code of conduct is intended for stakeholders that perform tests whose purpose is to determine internet quality of service or quality of experience.

This document is the 2018 version of the Code of conduct. It was produced by Arcep based on input from measurement producers, web testers, ISPs, consumer protection organisations and academics, with whom Arcep consulted during multilateral and bilateral meetings over the course of 2018. **This inaugural version will evolve over time** to strengthen the criteria listed, but also to complete them with elements that apply to other areas.

The Code of conduct defines a set of best practices whose purpose is to increase the transparency and quality of the measurements taken, and of the resulting publications. It is meant to act as a guide for stakeholders, but has no normative powers. It is divided into two main parts: Part 1 sets out best practices for the test protocols used to perform measurements, while Part 2 details best practices for the subsequent presentation of findings ("aggregate publications"). **Each part describes the methods that make it possible to guarantee both the transparency of the choices made** – so that any third party will be able to analyse the results produced by the tool – **and the robustness of the practices employed** – i.e. that they are reliable, representative and guarantee that the findings can be compared. These best practices for ensuring the method's robustness seek to avoid debatable practices, while keeping the field open enough to welcome innovation and diversity. As mentioned earlier, these practices will be fleshed out in future versions of the Code of conduct, as the ecosystem becomes more experienced and with the deployment of an "access ID card" API in the main ISPs' boxes. **The measurement tools wanting to declare their commitment to complying with the Code of conduct are asked to employ the following declaration of commitment**:

"For the design of [name of tool]'s test protocols and/or the aggregate publication of the resulting measurements, [Company name] refers to the 2018 Code of Conduct established by Arcep in concert with the ecosystem's stakeholders".

Any party who uses the "Arcep" brand without the permission of the French Electronic Communications and Postal Regulatory Authority may expose themselves to civil liability claims.

1 Test protocols

1.1 Testing methodologies

Transparency over methodological choices is vital to ensuring that any third party can analyse the findings delivered by the tool. **The methodologies used to measure upload and download bitrates, latency, web page load times and video streaming indicators are considered transparent if the characteristics listed in the second column of tables 1, 2, 3 and 4 below are made public.** These characteristics could be streamlined in future versions of the Code of conduct. And new indicators could be added.

If most of the choices made are worthwhile, some existing practices are questionable, and warrant being modified. **Rules that guarantee a basic level of robustness for the methodologies used to measure upload and download bitrates, latency, web page load times and video streaming indicators are listed in the third column of tables 1, 2, 3 and 4.** They will be expanded in forthcoming versions of the Code of conduct. New indicators may also be added.

Table 1: upload and download bitrates

PARAMETERS	TRANSPARENCY CRITERIA	ROBUSTNESS CRITERIA
Measurement protocols	TCP only, UDP only, HTTP/1.1, HTTP/2 or HTTP/3 **Example:** HTTP/1.1	-
Ports	TCP or UDP port numbers **Example:** about 50% on port 80, 25% on port 443, 25% on port 8080	-
Number of threads (possible number of threads)	Single thread or multithread (give number of threads) **Example:** about 30% on 2 threads; 20% on 8 threads ; 50% on 16 threads	-
Test length or volume of downloaded data	Expressed in Mb or second **Example:** stops once one of the two thresholds has been reached: 10 seconds or 500 Mb	Test length > 7 seconds or volume > 100 Mo
Stream encryption	Unencrypted, TLS 1.0, TLS 1.2,TLS 1.3 **Example:** about 50% of unencrypted tests, 50% of TLS 1.2 tests	-
Internet protocol during the test	IPv4 or/and IPv6 **Example:** about 50% on IPv4, 50% on IPv6 (systematically if available end-to-end)	-
Removal of the slow start	Indicate whether the bitrate indicator is calculated after a certain amount of time **Example:** Exclusion of the first two seconds of the test	-
Explanation of displayed indicators	Give the specific formula **Example:** 90th percentile bitrate on the last 10 seconds of the test	-

Table 2: latency

PARAMETERS	TRANSPARENCY CRITERIA	ROBUSTNESS CRITERIA
Measurement protocols	ICMP , TCP only, UDP only, HTTP/1.1, HTTP/2 or HTTP/3 **Example:** HTTP/1.1	Do not use ICMP to measure latency
Ports	TCP or UDP port numbers **Example:** port 80	-
Number of samples	Number of tests **Example:** 20 tests	Number of samples at least equal to 10
Time out	Duration in seconds **Example:** 1 second	-
Stream encryption	Unencrypted, TLS 1.0, TLS 1.2,TLS 1.3 **Example:** about 50% of unencrypted tests, 50% of TLS 1.2 tests	-
Internet protocol during the test	IPv4 or/and IPv6 **Example:** about 50% on IPv4, 50% on IPv6 (systematically if available end-to-end)	-
Explanation of displayed indicators	Give the specific formula **Example:** Minimum latency among the 20 tests	-

Table 3: web browsing

PARAMETERS	TRANSPARENCY CRITERIA	ROBUSTNESS CRITERIA
Number and selection of tested sites	List of websites or method of selecting websites at each iteration **Example:** 5 websites randomly selected from the top 100 most visited sites on Alexa ranking	Do not use operators' websites
Time out	Duration in seconds or no time out **Example:** 15 seconds	Time out is less than 30 seconds
Cache status	Empty cache or as is as **Example:** the cache is emptied after each website visit	-
Explanation of displayed indicators	Describe the indicator(s) **Example:** time to load all the web page's elements except advertisements.	-

Table 4: video streaming

PARAMETERS	TRANSPARENCY CRITERIA	ROBUSTNESS CRITERIA
Tested platform	Name of the platform where the video is hosted **Example:** about 50% on YouTube, 50% on Dailymotion	-
Number and selection of tested videos	Number of videos tested at each iteration Video list or video selection method **Example:** the most popular video in the country (number of views) with a resolution of at least 720p	-
Number of used threads	Single thread or multithread (give the number of threads) **Example:** 2 threads	-
Video testing protocol	HTTP/1.1, HTTP/2 or HTTP/3 **Example:** HTTP/3 for Android, HTTP/2 for iOS	-
Stream encryption	Unencrypted, TLS 1.0, TLS 1.2,TLS 1.3 **Example:** TLS 1.2 or TLS 1.3 depending on the version of the application	Same encryption as the one used by default on the platform being tested
Video test length	Duration in seconds **Example:** test of 30 sec (2 videos of 15 sec each)	-
Video resolution	Video resolution **Example:** 360p for the first video, 1080p for the second one	-
Explanation of displayed indicators	Describe the indicator(s). **Example:** average time of the 2 buffer fills and total number of cuts during the 2 videos	-

1.2 Test targets

Transparency over the test servers used (i.e. target servers) is also vital to understanding the results. **To guarantee this transparency, the characteristics listed in the second column of table 5 below must be published.** Minor alterations could be made to them as the Code of conduct evolves.

Furthermore, the test targets used must comply with certain conditions to ensure the accuracy of the measurements obtained. Arcep will work in concert with the ecosystem to define these robustness criteria, to complete future iterations of the Code of conduct.

Table 5: test targets

PARAMETERS	TRANSPARENCY CRITERIA	ROBUSTNESS CRITERIA
Explanation of default server selection	Explain if random, depending on latency, prioritizing the server on the same network, etc. **Example:** random- each target receives a test out of 4 without the ability for the client to choose a server	-
Physical location of the server	List of AS where test targets are **Example:** AS 12876 Online, AS 39180 Lasotel, AS 21409 Ikoula, AS 5410 Bouygues Telecom	-
Test target capacity in Mbit/s or Gbit/s	List of servers with indication of the maximum capacity in Gb/s **Example:** 50% 10 Gb/s servers, 50% 1 Gb/s servers	-
Ability to conduct IPv6 tests with the target	List of servers with indication of the ability to test IPv6 **Example:** 50% IPv4 only, 50% IPv4 + IPv6	-
Used port(s) by the target	List of servers with port numbers **Example:** 75% on port 8080, 25% on port 443 + port 8080	-

2 Aggregate publications

2.1 Data processing

The post-processing of the collected data is a crucial stage in eliminating false, manipulated or irrelevant measurements. It makes it possible to ensure that the results are representative and as widely comparable as possible, and to protect against attempted fraud.

The tools must have implemented efficient data processing algorithms to deliver the most reliable results possible. In particular, **stakeholders must be sure to exclude measurements obtained from a test target that has proved to be limiting factor** (notably when the target's capacity was below or equal to that of the line being tested).

Arcep will consult with the ecosystem in the coming months to specify possible transparency criteria and the robustness criteria that warrant being added, to complete this general commitment.

2.2 Statistical representativeness

To ensure that any third party can assess the reliability of the published findings, tools need to be transparent about the number of tests performed to obtain the subsequent aggregate publications. The tools must also report any bias due to the testing method that is likely to distort the representativeness or create comparability issues.

At this stage, **an aggregate publication is considered transparent if:**

- **The period covered by publication is clearly indicated;**

- **The number of tests performed to obtain each of the aggregated figures (detailed technology by technology, operator by operator, through a speed map, etc.) is made public (see second column in table 6 below);**

Table 6: number of measurements

PARAMETERS	TRANSPARENCY CRITERIA	ROBUSTNESS CRITERIA
Number of tests per published categorie	Disclose the total number of test per published single result (rather in a excel file attached, when hovering the results, etc.) **Example:** **Category xDSL:** Bouygues Telecom 24 236 tests Free 78 225 tests Orange 145 265 tests SFR 45 872 tests **Category FTTH:** Bouygues Telecom 85 872 tests Free 125 265 tests Orange 278 245 tests SFR 45 236 tests **Category 3G :** Bouygues Telecom 458 tests Free 1 452 tests Orange 782 tests SFR 252 tests **Category 4G:** Bouygues Telecom 2 523 tests Free 7 824 tests Orange 14 526 tests SFR 4 587 tests	-

- **any factor that is likely to introduce a significant bias in the analysis of compared categories (ISPs, technologies etc.) must be mentioned.**

Should a measurement tool publish an operator-by-operator comparison of fixed network performances "all technologies combined", it must clearly indicate the impact that ISPs' technology mix has on the results.

In addition, in cases where some of the test protocol's parameters can be adjusted and could prove discriminating, the publication must clearly mention, for instance, that:

- the download speed tests for ISP A were monothread tests, whereas those performed on ISP B were multithread;
- 80% of the tests on ISP A were performed on one of its internal network servers, whereas all of the tests of ISP B were performed on a target server hosted by a transit operator.

This part will be further strengthened in concert with the ecosystem, to establish relevant transparency and/or robustness criteria. In particular, criteria of transparency and robustness concerning the local aggregation of different measurement points, for example on a map, will be developed in co-construction with the ecosystem.

Moreover, the deployment in the ISPs' CPEs of an "access ID card" API will help improve the characterisation of the measurements significantly, and to round out the Code of conduct with criteria regarding the relevance and publication of the test results.

Personal data protection

It is up to the measurement tools to implement internal policies and procedures to ensure that they continue to comply with Regulation (EU) 2016/679, commonly known as the General Data Protection Regulation (GDPR).