

2019

The state of the internet in France

2019 REPORT



The state of the internet in France

2019 REPORT



TABLE OF CONTENTS

ENSURING THE INTERNET FUNCTIONS PROPERLY	08	ENSURING INTERNET OPENNESS	47
1. IMPROVING INTERNET QUALITY OF SERVICE MEASUREMENT	10	4. GUARANTEEING NET NEUTRALITY	48
1. Potential biases of quality of service measurement	10	1. Arcep's commitment at the European level	48
2. Work begun in 2018 on characterising the user environment	11	2. Work in progress	49
3. Towards more transparent and robust testing methodologies	12	3. Analysing observed practices	57
4. Importance of choosing the right test servers	17	4. European cooperation for a coherent application of the Regulation	59
5. How to maximise a QoS test's reliability?	20	5. FOSTERING THE OPENNESS OF DEVICES	61
6. Arcep's monitoring of mobile Internet quality	20	1. Arcep's work	61
2. MONITORING DATA INTERCONNECTION MARKET	23	2. Regulatory review	62
1. The internet's evolving architecture	23	3. Review of market practices	63
2. State of data interconnection in France	27	Lexicon	66
3. ACCELERATING THE TRANSITION TO IPv6	34	Annex 1: Implementation of an Application Programming Interface (API) in boxes	71
1. IPv4 addresses are running out quickly, the transition to IPv6 is a growing imperative	34	Annex 2: Test servers provided by the different quality of service measurement tools	74
2. Barometer of the transition to IPv6 in France	35	Annex 3: Increasing the accuracy of QoS testing	79
3. Co-construction with the ecosystem to accelerate the transition to IPv6	41		

Arcep's 2019 Internet check-up

Arcep examines Internet components and vital signs that it is responsible for monitoring: quality of service, data interconnection, the transition to IPv6, net neutrality and the openness of devices. To what end? To ensure that the Internet continues to develop as a "common good".

The Internet has become a vital part of French people's daily lives. It is a shared asset and an "infrastructure of freedoms": freedom of expression and communication, freedom to access knowledge and to share it, but also freedom of enterprise and the freedom to innovate.

Assessing the Internet's health means evaluating its ability to withstand the risks and threats that currently weigh on this vital shared asset: endless controversy over personal data and fake news, the spread of harmful content and hate speech on social media, cyberattacks, the environmental impact of digital tech, challenges to net neutrality, the concentration of power amongst a small handful of online platforms, as well as unequal ability to access the Web. Looking after the Internet's health means guaranteeing users' access to it, and that it is running smoothly and remains open.

As architect and guardian of communication networks in France, Arcep is involved in making this diagnosis. This report delivers a didactic presentation of the current state of networks, and the work being done to best guarantee users' ability to exchange information. For each component, Arcep identifies the symptoms, and draws up a prescription in order to either heal what troubles the Internet or offer preventive remedies.

This document is Volume 3 of Arcep's annual report: it focuses on the Internet health concerns that fall directly under Arcep's scope of competency. Issues of resilience and security are not addressed here, but readers wanting to delve deeper into the topic, and explore other aspects of the Internet's well-being, can turn, for instance, to the work being done in this area by ANSSI¹.

The status of network deployments, another vital sign for the Internet in France, is examined in a different report titled: "Arcep and smart territories" – which is Volume 2 of the Authority's annual report².

What comes next?

The Internet is continually evolving... To keep pace with networks' technological development, Arcep began investigating "Future networks". The first findings of this exercise, which focus in particular on network virtualisation, are available on the Arcep website³... and will no doubt be reflected in future editions of this report.

1. <https://www.ssi.gouv.fr/agence/rayonnement-scientifique/observatoire-de-la-resilience-de-linternet-francais/>

2. https://www.arcep.fr/uploads/tx_gspublication/rapport-conf-TC-RA2019-mars2019.pdf

3. <https://www.arcep.fr/actualites/les-communiqués-de-presse/detail/n/reseaux-du-futur.html>

Arcep's 2019 internet health check

1

QUALITY OF SERVICE

To improve Internet quality of service (QoS), we need to be able to measure it correctly. But the comparison tools available today deliver such disparate results that it's hard for users to truly employ performance as a criterion when choosing their Internet service provider (ISP). To remedy this, the "scanner" is being fine-tuned. Installing an API in ISPs' boxes that can obtain each device's "Access ID card" will enable a more detailed and accurate diagnosis. This API is the fruit of work performed in concert with the ecosystem's stakeholders, and is completed by a Code of Conduct. As it is gradually adopted by stakeholders involved in measurements, it will help increase the accuracy, transparency and clarity of the results.

2

DATA INTERCONNECTION

Interconnection is the cornerstone of the internet. It enables all networks to communicate with each other, and appear to users as a single, unified system. This constantly evolving ecosystem can, on occasion, be a source of conflicts, which in turn can threaten the quality of service experienced by users. This is why Arcep keeps a close watch over the interconnection market, and publishes the data gathered through its collection campaigns in a dedicated annual barometer of interconnection in France. A detailed examination of the market's metabolism and how it is changing, providing the sector's stakeholders with valuable information. Arcep can also be required to "police" certain situations, and settle disputes between the players

#INTERNETCHECKUP2019

1

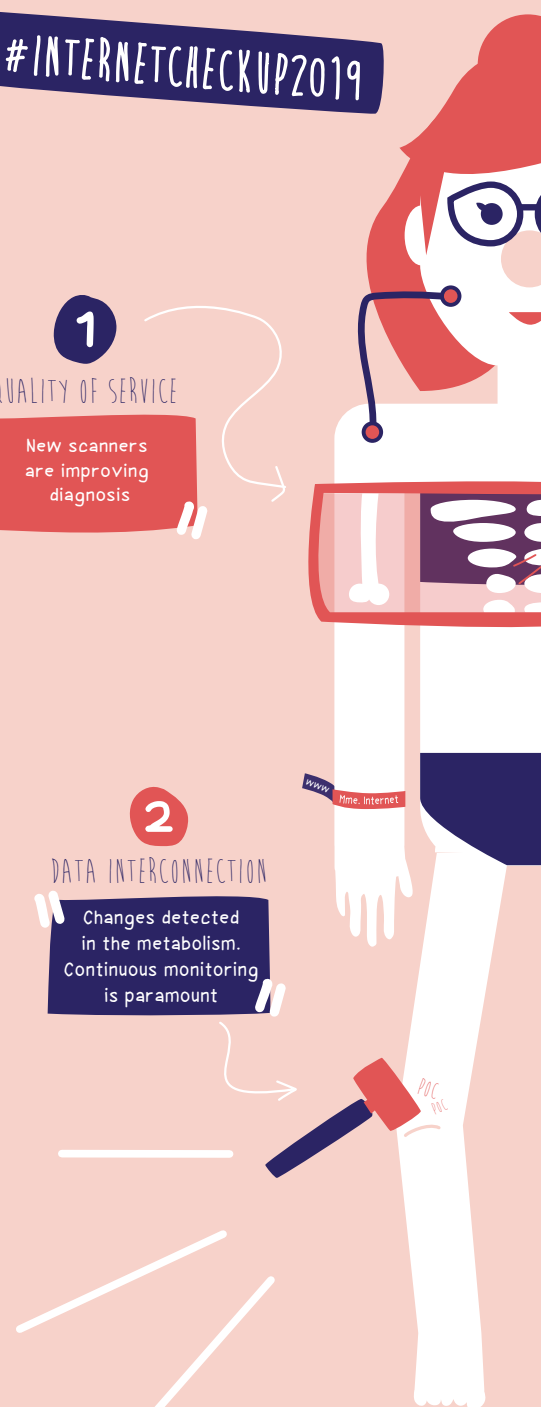
QUALITY OF SERVICE

New scanners are improving diagnosis

2

DATA INTERCONNECTION

Changes detected in the metabolism. Continuous monitoring is paramount





3

TRANSITION TO IPV6

The rate at which the last blocks of IPv4 addresses were acquired accelerated yet again this year. Upshot: June 2020 is now being announced as the end date for IPv4. Accelerating the transition to IPv6 is no longer an option, it is imperative. Despite which, fixed and mobile operators' planned IPv6 deployments may well make it impossible to deal with the overall dearth of IPv4 addresses. To galvanise the ecosystem around this pressing issue, Arcep will be hosting the first meeting of its IPv6 Task Force in the second half of 2019. These biannual meetings will provide an opportunity for stakeholders to share their experiences and define the actions that need to be put into place to accelerate the transition to IPv6 in France. To this end, Arcep is examining the possibility of creating an online platform to sustain an ongoing dialogue amongst Task Force participants.

4

NET NEUTRALITY

Two years after the Open Internet regulation came into effect, it's time for the first assessments. National regulatory authorities' enforcement of net neutrality helped reveal that BEREC guidelines on the matter still require some clarification, but have proven effective by and large. In France, along with the "J'alerte l'Arcep" reporting platform, the "Wehe" app published in late 2018 is now part of the arsenal of tools that Arcep employs on a daily basis for detecting traffic management practices that contravene net neutrality rules. Although France scores well on net neutrality, Arcep continues to keep a close watch to ensure that French ISPs persist in adjusting their behaviour to comply with the regulatory framework. Lastly, the Open Internet regulation's obligation of technological neutrality has enabled Arcep to pave the way for 5G and its innovations in a calm and orderly fashion.

5

OPENNESS OF DEVICES

Thanks to the adoption of Europe's net neutrality regulation, Arcep has been able to fulfil its duty to protect the networks. But there is still a weak link at the end of the chain: devices. Awareness of this issue has been growing in recent months. In Europe, Android was fined for abusing its dominant position in the mobile operating systems market. Adopted in early 2019, the "Platform-to-Business" regulation brings greater transparency to how online platforms treat their corporate clients. Although Arcep welcomes these first steps towards ensuring users' freedom to innovate and freedom of choice, the "Platform-to-Business" regulation does not yet guarantee device neutrality. In its February 2018 report devoted to this issue, Arcep delivered 11 concrete proposals for achieving an internet that is open from end-to-end.



Ensuring the internet functions properly

- 1.**
IMPROVING INTERNET QUALITY
OF SERVICE MEASUREMENT
- 2.**
MONITORING DATA
INTERCONNECTION MARKET
- 3.**
ACCELERATING THE TRANSITION
TO IPv6

Improving Internet quality of service measurement



“New scanners are improving diagnosis”

5

QoS testing tools have been declared compatible with Arcep's Code of Conduct



How healthy is quality of service (QoS) on the Internet in France? If a body need only be at 37° to be considered at the “right” temperature, measuring and analysing the networks’ ability to relay traffic under the right conditions is a more complex affair: not only do several indicators (speed, latency, jitter, etc.) need to be measured to obtain this assessment, but the measurement process itself is also complex.

1. POTENTIAL BIASES OF QUALITY OF SERVICE MEASUREMENT

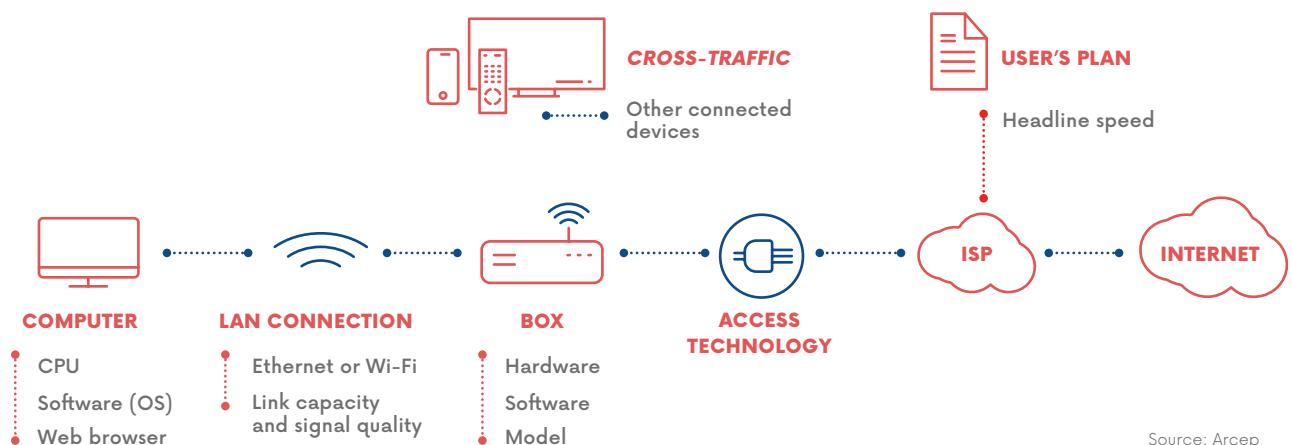
Today, users can easily obtain the results of the speed tests performed on their Internet connection using crowdsourcing tools.

However, a substantial number of technical and use-related characteristics will influence these results, and it is very difficult to know if a low score is due to the poor quality of the ISP's access network, the quality of the Wi-Fi connection and/or the parallel use of other devices connected to the local network during the test.

The “user environment” is the first element that can affect test results. The following diagram summarises the main characteristics of the user environment that can influence the results.

Other features (test target's location and capacity, tool's measurement methodology) can also be biasing factors when measuring quality of service. Potential biases are explored in more detail in the following sections.

CHARACTERISTICS OF THE USER ENVIRONMENT



2. WORK BEGUN IN 2018 ON CHARACTERISING THE USER ENVIRONMENT

To obtain an accurate diagnosis of any quality of service issue, it is vital to have detailed knowledge of the user environment for a fixed connection. The ability to obtain this detailed characterisation will vary depending on the type of measurement tool being used. Some hardware probes¹ are, for instance, capable of testing a LAN² connection and even estimating cross traffic³ on the local network. Meanwhile web testers⁴ can be rapidly deployed on a large scale, they are only able to detail a small number of elements (web browser used, etc.). In any case, no tool is capable of characterising all of the parameters that define the user environment and influence quality of service testing results.

To improve this ability to characterise the user environment, in 2018 Arcep led a co-instruction initiative with a broad spectrum of stakeholders from the crowdsourced metrology ecosystem⁵:

- measurement tools: ASSIA, Case on IT, Cedexis, Directique, Ip-label, M-Lab, Ookla, nPerf, QoSi, SamKnows, V3D;
- ISPs: Bouygues Telecom, Free, Orange, SFR;

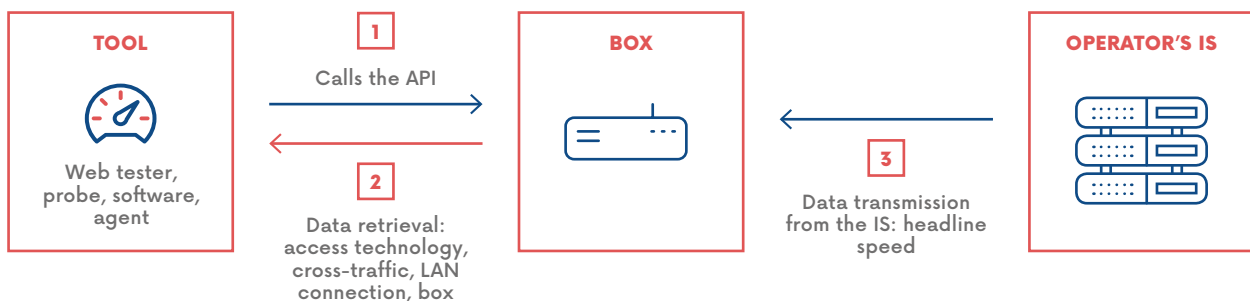
- academia and R&D: CNES, Inria;
- consumer protection organisations: INC, UFC Que-Choisir, which have also developed their own tools.

Thanks to the efforts of a series of working groups, a consensus was reached in December 2018 on the definition and introduction of an application programming interface (API) to be installed directly on operators' boxes, and accessible to any measurement tool that complies with the QoS Code of Conduct published by Arcep⁶. This interface would make it possible to transmit the information that makes up the connection's "access ID card".

To set a clear scope of application for this API, on 23 April 2019 Arcep launched a public consultation on a draft decision that details the rules of deployment.

This API is a software interface that will be implemented in each box, and in 5G-compatible fixed access boxes. Its purpose is to send back information such as access technology, advertised speed and Wi-Fi quality, at the moment when an xDSL, cable or FTTH Internet customer performs a QoS test on their connection. The API thus makes it possible to characterise the user environment at the time of testing, without diminishing the quality of the user experience.

THE "ACCESS ID CARD" API FOR CHARACTERISING THE USER ENVIRONMENT



Source: Arcep

When a test is performed, the tool (whether a web tester, hardware probe, software agent on a box or software that can be installed on a device) sends a request to the API located on the tester's box. The measurement tool launches the Internet QoS test immediately after receiving this request.

The API answers the tool by sending it the characteristics of the user environment at the time of testing. Most of the information is available natively on the box: access technology, information on the LAN and WAN connection and byte counter that makes it possible to detect cross-traffic.

Other properties, such as the user's advertised speed, are not available locally on the box, so will be transferred from the operator's information system (IS). This gives operators the freedom to choose how to transmit these details, and provides Internet QoS measurement tools with a single interface for gathering information on the user environment.

The main information that the API transmits was defined in concert with the ecosystem's stakeholders:

- metadata: version of the API, timestamp;
- information on the box model and version of the software it is running;

1. See lexicon.

2. See lexicon.

3. See lexicon.

4. See lexicon.

5. Arcep invites any players who are not listed and who would like to take part in the co-construction efforts to get in touch.

6. 2018 Code of Conduct on Internet QoS: https://www.arcep.fr/uploads/tx_gspublication/code-of-conduct-internet-qs-2018_EN.pdf

- the advertised speed of the customer's Internet plan;
- type of Internet connection: FTTH, ADSL, VDSL, etc.;
- speed of the connection between the box and operator-side equipment, and the box and terminal equipment;
- type of connection between the terminal equipment and the box: Wi-Fi, Ethernet, PLC;
- specifically for Wi-Fi: Wi-Fi version (802,11n, 802,11ac, etc.) and Wi-Fi signal strength;
- information on cross-traffic: complete number of bytes used on the box between the beginning and end of the quality of service test.

An exhaustive list of the parameters can be found in Annex 1 of this report. It is taken from Annex 1 of the public consultation for the draft decision that Arcep published.

The Arcep draft decision published for consultation provides for a beta testing phase for the API. Following a series of interim milestones, the draft decision stipulates that operators will implement and activate the API by default, within 28 months, on 95% of the boxes affected by the API's introduction, and on 100% of boxes distributed to new retail market, residential fixed access customers. A committee for monitoring the API's development will be created, to bring together stakeholders and run the project in as agile a fashion as possible.

3. TOWARDS MORE TRANSPARENT AND ROBUST TESTING METHODOLOGIES

3.1. Arcep's Code of Conduct

In addition to the characteristics of the user environment, testing methodologies also have a tremendous influence on QoS test results. In 2017, Arcep identified the need for greater transparency on testing methodologies. In December 2018, it published a Code of Conduct for stakeholders involved in testing. This Code of Conduct addresses two aspects in particular: first, requesting that the tools include a clear explanation of their methodological choices when publishing their results, so that any third party can analyse them. Second, establishing best practices that are vital to obtaining reliable results. This approach creates an incentive for stakeholders to satisfy a set of minimum requirements in terms of transparency and robustness, both in their test protocols and in the delivery of their findings.

The Code of Conduct is structured into two main parts:

- The first part concerns test protocols, test targets, and the methodologies employed for measuring upload and download speed, latency, web page loading time and video streaming quality;
- The second part concerns aggregated publications. A general commitment to use algorithms designed to exclude erroneous, manipulated or irrelevant results. Moreover, to guarantee statistical representativeness, tools that comply with the Code of Conduct commit to publishing the number of tests performed and the factors that are likely to introduce a significant bias when analysing the compared categories, for the period in question.

Both parts set out the rules to follow to ensure transparency over the choices made, and a base level of robustness for the practices employed:

- **transparency criteria:** concerning testing protocols, measurement tools must, for instance, indicate the different parameters of the testing protocols that make it possible to determine whether or not the test is representative of the most common uses of the Internet. One concrete example: a quality of service measurement tool that uses port 8080 or 8443, which are ports used primarily by speed testing tools themselves, will, in principle be less representative than a tool that employs ports 80 or 443, which are used to access web pages. Regarding aggregate publications, the tools must, for instance, publish the number of underlying measures;
- **robustness criteria:** concerning testing protocols, for speed measurement, for instance, the robustness criterion requires a test to last more than 7 seconds and involve a download of more than 100 Mb of data. To measure latency, the robustness criterion requires that the Internet Control Message Protocol (ICMP) should not be used to measure latency as ICMP is a protocol that is not representative of actual use cases, and could therefore indicate a latency that is not representative of the reality observed with the TCP or UDP protocols. Regarding aggregated publications, the tools must, for instance, set up efficient data processing algorithms to be able to produce the most accurate results possible.

The 2018 version of the Code of Conduct on Internet quality of service introduces minimum requirements in terms of transparency and robustness which will evolve over time to strengthen those criteria, but also to complete them with elements from other categories. Any changes will be made in concert with stakeholders. In the near future, this Code of Conduct will also include details on measuring Internet quality of service on mobile networks.

3.2. The first tools starting to adopt the Code of Conduct on Internet quality of service

Arcep published the Code of Conduct on 20 December 2018, and by early 2019 several tools had already declared themselves in compliance.

The tools for measuring fixed Internet quality of service which have declared themselves to be in compliance with the Code of Conduct on Internet quality of service are:

- nPerf, developed by nPerf;
- UFC-Que Choisir Speedtest, developed by UFC-Que Choisir;
- DébiTest 60: the connection tester from *60 Millions de consommateurs* (consumer advocacy association) developed by QoS;
- 4GMark, developed by QoS;
- IPv6-test: IPv4 and IPv6 QoS test, developed by IPv6-test.

The tools for measuring mobile Internet quality of service which have declared themselves to be in compliance with the Code of Conduct on Internet quality of service are:

- nPerf, developed by nPerf;
- DébiTest 60: connection tester from *60 Millions de consommateurs*, developed by QoS;
- 4GMark, developed by QoS.

OPEN FLOOR TO ...



Martin Thierry, Research engineer at the Comparative Testing Centre, Institut National de la Consommation (INC)

Comparing connection quality with DébiTest60, the collaborative tool from INC

Paradoxically, the more fixed and mobile very high speed networks expand, the more dissatisfaction over performance we will see. Having access to a high quality network is vital, regardless of what part of France one is in. But there is still a tremendous gap between operators' promises and consumers' actual experience – a gap that reaches unacceptable proportions in certain rural, mountain and remote regions, so as not to say absurd when one end of a street has a good ADSL connection while speeds on the other are slow.

Consumers view all of these network accessibility and performance issues as an unacceptable and incomprehensible

source of inequality. So, more than ever before, they need to have QoE-centric tools to better understand geo-technological impediments, along with tools dedicated to ascertaining the user experience in the field. On this last point, INC welcomes the efforts that elected officials and the French Telecoms Users Association (AFUTT) are making to spread the word about citizens' expectations and dissatisfactions, as well as Arcep's initiatives tied to its "J'alerte l'Arcep" reporting platform and the French Digital Agency's "France Mobile" initiative.

For its part, INC released the DébiTest 60 collaborative service in 2018. A veritable testing toolkit, it is designed to measure

fixed and mobile connections' performance, and respond to this vague sentiment we have of "being lied to" about network and connection quality with objective truths. DébiTest 60 thus allows consumers to see how their connection performs compared to other users' connection, and provides performance maps along with an instructive approach to promoting a better understanding of how connections behave. Today, INC is working on designing reliability indicators for the information supplied by its performance maps, and exploring a basic code of conduct for entities involved in crowdsourced testing solutions.



Vincent Néguier, founder, IPv6-Test

Measuring the quality of IPv6 Internet services

It was around ten years ago that we began to see the first reports expressing concern about the alarming depletion in the number of unallocated blocks of IPv4 addresses, and the need for a long-term term solution for this growing dearth of available addresses in a 5G connected IoT world.

This solution already existed, and it was and is the IPv6 protocol, of course. But IPv6 connectivity was not a simple matter for a business back then, even less so for consumers, and rare were the websites that had an IPv6 address.

So it was against this backdrop that we launched ipv6-test.com in 2010: it is a platform for running technical tests on IPv6

connectivity. The site makes it possible to test several aspects of a connection: from comparing its v4/v6 bandwidth to detecting certain configuration or security issues.

The anonymous data that have been collected since we launched the site reveal significant progress with respect to IPv6 in the top Internet players' policies in France, and around the world.

Our figures for France reveal that over 99% of the IPv6 addresses tested are now native whereas, back in the day, close to 20% of sites were using transition protocols such as 6to4 or Teredo. This shift, combined with the efforts made by transit providers and exchange points, have allowed us to

reach the current stage where IPv6 and IPv4 are performing identically in our bandwidth tests, whereas in 2010 IPv6 lagged behind by an average of about 20%.

This is a trend we are seeing worldwide, with similar figures. Ninety nine percent of IPv6 addresses are native in 2019 compared to 74% in 2010, and the 25% performance gap observed in 2010 has now been eradicated.

The 2010s marked the transition decade towards IPv6. Although the process was far too slow, the protocol is now a well-oiled machine and there is no longer any reason not to use it.



Renaud Keradec, CEO/CTO and founder, nPerf SAS

The deceptive simplicity of crowdsourcing

At nPerf, we realised that, seen from outside, speed measurement tools often appeared quite simple, and something that any developer could create.

This is far from the truth, however. Although simple in appearance, it is no easy task to implement a reliable speed test. It involves a set of links in a chain (from the app that measures the speed to the server that provides its) connected by an intelligent information system that needs to know, at all times, where the user is located, who their ISPs is, and tell them which (currently available) server to use to run their test, without having to worry about being limited by this server's connectivity. Added to this, of course, are

the performance imperatives for the testing algorithm, which needs to make full use of the user's computer or smartphone's capacity to obtain an accurate and reliable measure their speed. And, finally, to be viable worldwide, the test needs to rely on a global network of servers. In other words: a whole lot of moving parts to deal with!

Next comes the analysis, filtering and compilation of the millions of measurements collected, to then extract the overall trends and generate map-based findings. Welcome to the world of big data!

In addition to the technological difficulties, the process of building a community around such a technical tool is a real challenge. You need to offer a user-friendly and attractive tool that is precise enough to attract the technophiles, but also easy enough to use to get the average consumer on board. We are constantly looking to strike the right balance between obtaining useful measurements for data analysis and ensuring the tool is easy to use.

Simply put, all of this requires a real *savoir-faire*, of which we are truly proud. Our determination has enabled a small French company such as ours, little by little, to build a global reputation.



Fabien Renaudineau, CEO, QoSi

Data: a crucial tool for regulating the sector

Data have become an essential component in the entire telecom ecosystem's industrial strategies, as well as a vital tool for regulating the sector.

As an independent network QoS measurement expert, who relies on crowdsourcing among other things, we have become convinced that, regardless of methodology, an isolated approach to testing will

necessarily be limited in scope, and deliver results that fall well short of the potential offered by a global approach that taps into what is now a mature ecosystem.

This is why we at QoSi are committed to forging ties with an ever growing number of contributors – whether large private sector (corporate) accounts, public sector players (local authorities and national government

bodies), consumer associations or media outlets. Their contributions are what continue to strengthen our platform, and to increase the value of the tests and the collected data.

In 2019, it is this collective and collaborative approach, of which we have become the aggregators, that is being used to help fuel Arcep's data-driven regulation policy.



Antoine Autier, Deputy Head of Research, UFC-Que-Choisir

Towards a more accurate quality of service assessment

In addition to the individual information tool that Internet QoS tests provide to consumers, UFC-Que Choisir believes that, ideally, these tests should also help fuel public debates over regional digital development.

It was this dual desire that led our association to launch its Fixed Internet QoS Observatory last year, focusing on two main avenues: combining performance (speed, latency) and usage (web browsing, video streaming) tests on the one hand and, on the other, breaking down the results by geographical area.

After a year of running tests, results reveal that consumers are treated differently with

respect to Internet access, depending on where they live. The results also underscore the need to fully understand that even tiny differences in ADSL speeds can have a considerable impact on the user experience. On the other hand, very large differences in speeds over superfast access lines (due to the different technologies used) are far from having a significant impact on common uses.

For QoS measurement tools to produce strong and influential results, they need to be technically robust, flexible enough to adapt to network developments, and relevant enough to describe these networks' capacity to deliver speed. Here, the API

that is currently being developed under the aegis of Arcep will be especially valuable, making it possible to obtain details on the user environment in which the test is being performed, and so reduce potential biases.

To be able to make the utmost of this API, UFC-Que Choisir recently upgraded its technical mechanism by opening it up to everyone (online speed test + downloadable web browser extension for testing uses). This means: more finely tuned and telling results, providing an even more detailed description of Internet quality across the country.



FYI

SINGLE THREAD VERSUS MULTI-THREAD TESTING

Some quality of service measurement tools are only single thread, while others are multi-thread, i.e. transmit the speeds measured by adding together the speeds of multiple simultaneous connections. A third type of tool gives user the choice of running a single or multi-thread test.

Both types of speed measurement are useful, and satisfy different objectives.

- Multi-thread mode makes it possible to estimate a link's capacity during the test by determining its maximum throughput at that moment, using several parallel streams;
- Single thread mode makes it possible to provide speed results for a representative use of the Internet. Because most uses employ one or two connections simultaneously to transfer data, single-thread mode provides a more accurate measure of users' actual experience, especially if the speed is an average speed that includes a slow start, in other words the period just after the handshake is established during which the TCP connection speeds up. In contrast, other tools provide the speed in steady state, once the nominal speed is reached. And, lastly, the information provided by some speed tests is the speed based on the 70th percentile (average duration for the best time, representing 30% of the test's duration), which is close to the peak speed.

It is not uncommon for multi-thread tests to deliver a faster connection reading than single thread ones, which can be for several reasons:

- **Latency:** the higher the latency, the longer the TCP connection takes to reach peak speed. The speed on a single thread test will increase sixteen times slower than a multi-thread test using 16 TCP connections. The higher the latency, the more the average speed for a single-thread test will decrease.
- **Limitation on the size of the TCP receive window** (i.e. the number of bytes the recipient wants to receive before acknowledgment). This window is only limiting on older operating systems. For example, in some instances, Microsoft Windows 7 limits this window to 255 KB per TCP connection. With an end-to-end latency of 30ms, the speed would therefore be limited to 68 Mbit/s for a single-thread test, and 1088 Mbit/s for a quality of service test which adds up the speeds of 16 simultaneous connections.
- **Jitter:** a connection whose jitter makes it impossible to guarantee that packets will arrive in the right order will degrade connection speed considerably. When packets arrive out of order, TCP cannot identify the connection speed, thus, it can be divided by ten¹.
- **LAG link saturation:** Link Aggregation (LAG) is a technique used on computer networks for aggregating several network links and using them as if they were a single one. Ethernet LAGs are almost always used

to distribute packets by scanning their IP headers. As a result, in a given TCP session, with all of the same elements in the header in both directions (MAC address, IP address, ports), the packets will all be transmitted over the same physical link. A single thread test will therefore always use the same physical link, which could be saturated, whereas a multi-thread test will use several physical links. To give a fictional example: you have a 1 Gbit/s connection. Your operator's backhaul relays collect from your region through a 100 Gbit/s link, made up of an aggregation of ten 10 Gbit/s links. The link is 97% full when you perform the test, so 3 Gbit/s are available on the entire LAG. Operating under the supposition that the LAG is perfectly balanced (each link is exactly 97% full, so each has 300 Mb/s available) a single thread test will display a speed of 300 Mbit/s, whereas a multi-thread test will display a speed of 1 Gbit/s, by using several LAG links simultaneously.

- **Saturation of the terminal's processor core:** a single thread quality of service test may not employ all of a processor's cores fully, unlike multi-thread tests. A machine with a four-core processor could have a smaller processor-related speed limitation during a single thread test than during the same test performed in multi-thread mode.

The speed measured by a single thread QoS test will be close to the one measured by a multi-thread test if:

- end-to-end latency is low (below 15ms);
- the operating system has a recent TCP/IP stack (as is the case with the different recent OS, such as Microsoft Windows 8 and higher, macOS 10.9 and higher, Ubuntu 11.10 and higher);
- packets arrive systematically in the order in which they were sent;
- the connection is far from all saturation, as much on the ISP end as that of the hosting service and any possible service providers located between the hosting company and the ISP;
- the processor on the terminal being used is able to manage the connection speed without saturating a single microprocessor core;
- the Internet connection speed is below 1 Gbit/s. For connections above 1 Gbit/s, the slow start period may cause a significant gap between the results produced by single thread and multi-thread QoS measurements.

A single thread speed that is substantially lower than a multi-thread one reveals a problem, which will negatively impact the user's quality of experience. Without a special investigation, it is nonetheless impossible to determine whether this problem is due to the computer used to perform the test, the equipment used on the client's local network, to the ISP, the hosting service, or to any of the possible service providers located between the hosting service and the ISP.

1. Source:

<https://www.semanticscholar.org/paper/Packet-reordering-in-high-speed-networks-and-its-on-Feng-Ouyang/4acae5f78578273071f23832ca799278126149d>

4. IMPORTANCE OF CHOOSING THE RIGHT TEST SERVERS

The choice of test servers – i.e. the server that the QoS measurement tool will use to measure download speed, upload speed and latency – is important. It is also a parameter that will influence test results.

4.1. Impact of the bandwidth between a test server and the Internet

A test server needs to have enough available bandwidth to ensure that it is not a source of impediment. This is especially true when the target’s capacity is less than or equal to the capacity of the line being tested.

To give a concrete example: a test performed on an FTTH line that can deliver a connection speed of 1 Gbit/s will be limited to 500 Mbit/s if two FTTH customers are performing this same test on a test server that is connected to the Internet with only 1 Gbit/s.

The 2018 Code of Conduct therefore contains a set of minimum transparency criteria for the test servers used by measurement tools – criteria that are due to be strengthened in future versions of the Code of Conduct, in concert with the ecosystem.

The 2018 Code of Conduct does not contain criteria setting a minimum bandwidth for test servers (setting a minimum of 10 Gbit/s would reduce the choice considerably, and have a potentially substantial financial impact). It is nevertheless recommended that the results of tests performed on target servers that proved a source of impediment should be excluded from publications.

Other robustness-related criteria are expected to be added in the next version of the Code of Conduct.

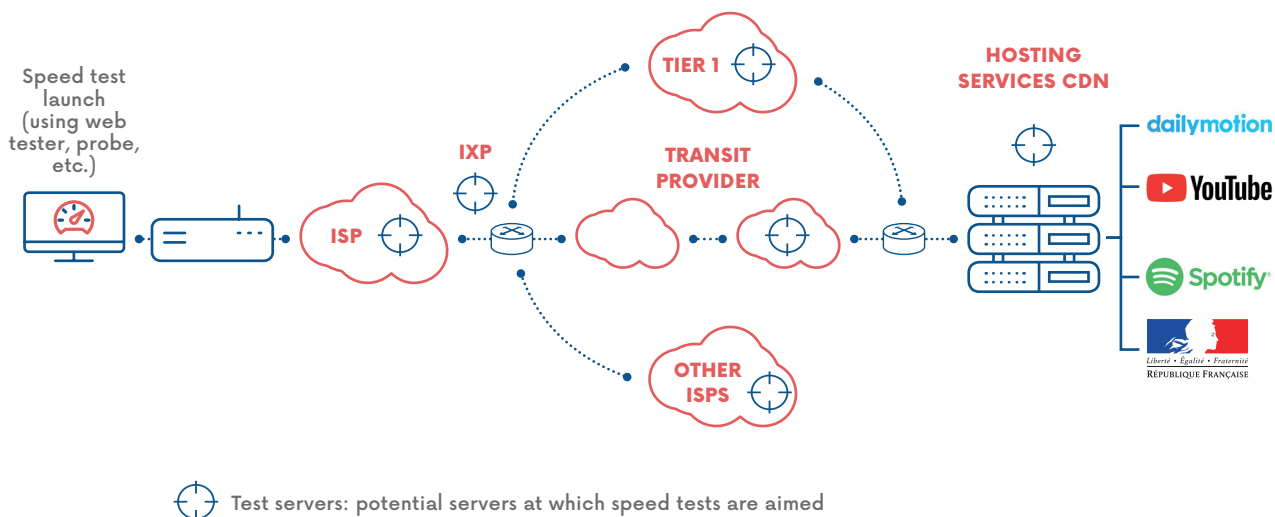
FYI

CLOSE-UP ON ANYCAST TEST SERVERS

Some tools offer the ability to use the Anycast protocol for certain test servers. Anycast is an addressing technique whereby the network identifies the “closest” server in terms of overall topology. There will therefore be several physical servers behind a test target being accessed via Anycast. This allows the network to select the server that is closest to the customer.

For instance, a person living in Nice will use the Anycast test target belonging to their ISP which has three physical servers: in Paris, Lyon and Marseille. If the choice is made in terms of geographical distance, the server in Marseille would be chosen. However, if the customer needs to go through Lyon to reach the Marseille server, then the network will choose the server in Lyon which is closer to the customer on the network than the one in Marseille.

THE TEST SERVERS’ LOCATION: A CHOICE THAT HEAVILY IMPACTS RESULTS



Source: Arcep

4.2. Impact of the test server's location

The test server's location is fundamental for latency and for single thread tests on super high-speed access. Location is less important for multi-thread quality of service tests, as latency has little effect on speed.

As detailed in the above diagram, the test target can be in different locations:

- on the user's ISP network: the results of the test depend only on the ISP but it is not terribly representative of the actual experience of using Internet services, which are often hosted outside this simple network;
- on another ISP's network directly interconnected (via peering) with the user's ISP: the test takes into account not only the user's ISP's network but also the quality of the network and interconnection with another ISP. This test is very rarely representative of the actual experience of using Internet services;
- at an Internet Exchange Point (IXP): the tested network depends almost only on the ISP and more closely matches the actual user experience, with a portion of Internet traffic transiting through the IXP;
- on the transit provider's network: the test will only be relevant if the transit provider exchanges a great deal of traffic with the user's ISP. It should be noted that the observatories produced by transit providers (e.g. the one from Akamai) only represent quality of service towards a specific point on the Internet;
- on a Tier 1⁷ network: the tested network extends beyond just the ISP's network performance, and the measurements are even more representative of the actual user experience if the test targets are located at an IXP;
- close to CAPs' servers: the tested network is the one employed end-to-end up to a given web host. The tests are thus very representative of one particular type of use (the Netflix speed index, for instance, only measures the quality of the connection to its own service).

Geographical location is misleading. Using the server that is the closest to one's home geographically does not mean that it is the closest server from a network standpoint. For instance, someone who lives in Nice might think they should use a server hosted in that city. But it is entirely possible that their connection will need to go through Paris before coming to Nice, if that server is not hosted on their ISP's network.

FYI

IMPACT OF THE TCP PORT USED FOR THE TEST SERVER

This is an important aspect in terms of the tests' representativeness. A considerable number of Internet applications use TCP port 443. A quality of service test that uses the same port will be more representative of actual Internet use than one that uses a different port. The technical choices of routing traffic can differ depending on the port.

Four TCP ports are used by the different QoS measurement tools:

- port 80: http traffic port used for unencrypted access to web pages;
- port 443: port used by https (http with an encryption layer, typically via the TLS protocol);
- port 8080: most of the traffic relayed through this port is tied to speed tests. Port 8080 traffic today is generally encrypted, which was not the case a few years ago;
- port 8443 is the encrypted counterpart of port 8080.

Which test targets do the different QoS measurement tools offer?

For information purposes, Arcep lists the test targets used by the different tools in Annex 2 of this report.

Arcep makes a test script available to users for verifying the speeds of certain QoS test servers, to be able to select a test target that will not be an impediment to running accurate QoS tests. The script is available here: <https://github.com/ARCEP-dev/testDebitMire>

7. Tier 1 networks are the networks that are capable of interconnecting directly with any other internet network. See lexicon.

OPEN FLOOR TO ...



Isabelle Chrisment, Professor at TELECOM Nancy, Université de Lorraine

BetterNet: collaborative mapping of the Internet

As Internet traffic is increasing exponentially, the services being made available to users have become more complex. More and more intermediaries have appeared, and defined new solutions for improving access to these services. Content distribution networks (CDN) have been deployed. Entities that provide OTT (over-the-top) multimedia services – i.e. that are not part of ISPs' access plans – have deployed their own cache servers to improve the quality of the services on offer. New protocols, such as QUIC, have been developed to enable faster access to web applications. The local user environment also has become increasingly complex (firewalls, NAT, wireless networks, Internet boxes...). To display a single web page, a browser often has to interact with several servers since different parts of a single web page are often distributed separately over the Internet. As a result, how well a web application loads no longer depends only on a single ISP, but rather on other factors and strategies that are determined by content providers.

It is therefore worth taking a close look at how this complexity affects users' quality of experience (QoE), to be able to then improve the protocols and applications, and pinpoint intermediary players' potentially biased behaviours. Processing is said to be "neutral" if every data packet is treated equally, regardless of type, origin or destination, at

each network node. Neutrality is required by law in Europe, but has been challenged recently, for instance in the United States.

Through the BetterNet project, we are working to build a collaborative scientific and technical observatory to measure and improve access to Internet services, based on the user experience. BetterNet is an Inria Project Lab (IPL) initiative involving several Inria research teams (Diana, Dionysos, MiMove, Resist, Spirals), ip-label, the Triangle lab (ENS-Lyon/CNRS) and Arcep.

To design, integrate, validate and improve new or existing testing methods, we have developed a testing platform that federate different tools developed at Inria:

- APISENSE® (<https://apisense.io>) and its Android Bee application, which provides a distributed mobile crowdsensing solution to collect quantitative measurements (from physical sensors) and/or qualitative ones (by interacting with users) in the field, promoting a participatory approach that respects participants' privacy;
- Hostview for gathering measurements on network traffic, annotated with user feedback on the quality of their experience. A mobile version of Hostview was developed and incorporated into the Bee mobile app to make it easy for a user to take part in the information gathering process;

- ACQUA in an Android application for measuring Internet access performances (speed, latency, packet loss, etc.) at regular intervals, and predict users' QoE based on these measurements.

The collected data are then stored at the High Security Laboratory (<https://lhs.inria.fr>) and later analysed and aggregated, before being made available to users and other Internet players. Anyone will therefore be able to see how Internet usage and performance is evolving. This work should lead to improvements in the defined models and metrics.

We are also working on developing metrology tools for measuring whether biased behaviour can be observed, e.g. in how packets are being treated, for instance, or in the choice of data being cached close to users to provide a better quality of service. The purpose will therefore be to define neutral or fair behaviour for the different types of network player, along with the associated metrics, and to implement corresponding testing techniques. Rounding out this work is our endeavour to perform as broad a cultural translation of these measurements as possible, by producing maps that combine measurements, demographics and geography, and by examining the effects that these maps (and others produced by various bodies, such as Arcep) have on our representation of today's world.

5. HOW TO MAXIMISE A QOS TEST'S RELIABILITY?

A user may want to maximise the reliability of their quality of service test. To do so, a number of parameters will need to be taken into account to eliminate any bias induced by the user environment or the test servers that could affect the measurements. These parameters are detailed in Annex 3 of this report.

FYI

BOOTABLE USB DRIVE

The software installed on a machine also appears to be significant when performing a quality of service test. To run a QoS test that ignores the installed software, readers can follow the approach available on the Arcep website⁸, to create bootable USB drive and perform a QoS test that ignores the installed software.

MEASUREMENT TOOL DEVELOPED BY BEREC

In September 2018, BEREC began developing its open source tool for measuring Internet quality of service. This tool will include a mobile app (Android and iOS), a browser-based version and an installable version (Windows, Mac and Linux compatible).

In addition to measuring the usual indicators (speed, latency, etc.), this tool will be able to measure certain usage indicators such as web browsing and video streaming quality, along with net neutrality-related indicators such as port blocking, proxy detection and DNS manipulation.

The tool's development is due to be complete by late 2019. Because its adoption will be on a voluntary basis, national regulatory authorities will be able to implement the tool in their country after having adapted it to local requirements (translating the user interface, installing local test servers, adding any supplementary test indicators, etc.).

In time, this tool could become a new quality of service and net neutrality diagnostic instrument for Arcep.

6. ARCEP'S MONITORING OF MOBILE INTERNET QUALITY

If mobile operators' coverage maps – which are produced based on operators' digital simulations and verified by Arcep – provide necessary information on the entire country, they also only give a simplified picture of mobile services' availability. These maps are completed by quality of service data. Using information obtained under real life conditions, these maps do not deliver an exhaustive picture of the situation across France, but do make it possible to obtain an accurate view of the level of service that each operator provides in the tested locations.

Every year since 1997, Arcep has performed a QoS audit on the mobile services provided by operators in Metropolitan France. The goal is to assess the quality of the services that mobile operators provide to users on a comparative basis, and thereby reflect the user experience in various situations (in cities, in rural areas, on different forms of transport, etc.), and for the most popular services

(calling, texting, web browsing, video streaming, file downloads, etc.). This audit is part of Arcep's data-driven regulation strategy, and is designed to keep users informed. In 2018, more than a million measurements were taken in every department across the country on 2G, 3G and 4G systems, both indoors and outdoors and on transportation systems (TER, Transiliens, RER, metro, TGV, roadways).

To make the most of these findings, in 2017, Arcep launched an interactive mapping tool called monreseau-mobile.fr (my mobile network), which allows users to view all of the data collected through this QoS audit. monreseau-mobile.fr thereby provides consumers with customised information by allowing them to see on a map which operator is likely to offer them the best quality of service, in any given location. France's overseas territories have also been an integral part of monreseau-mobile.fr since July 2018.

8. Creation of a Bootable USB drive: www.arcep.fr/usbBootable

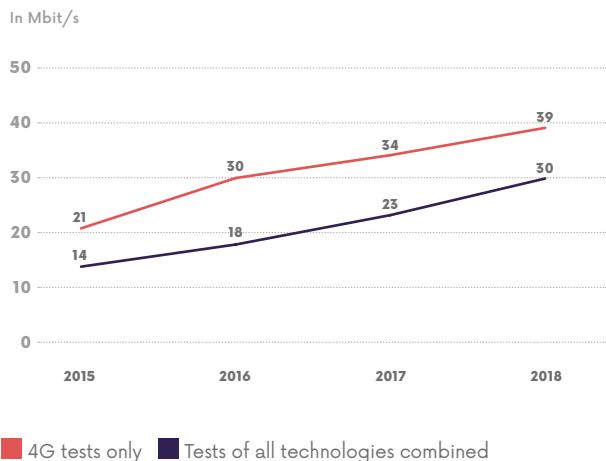
As data usage exploded, the smartphone became the most commonly used device for accessing the Internet⁹. And mobile data traffic had doubled every year as a result, reaching an average 6.8 GB¹⁰ a month in 2018, for every customer with an active 4G SIM card. These 4G users represent more than 90% of all mobile data traffic.

4G is thus spearheading operators' investments, to keep pace with this massive surge in usage. Arcep's annual audit provides an opportunity to measure the progress of quality of service on each operator's network.

6.1. Average mobile connection speed in Metropolitan France: 30 Mbit/s

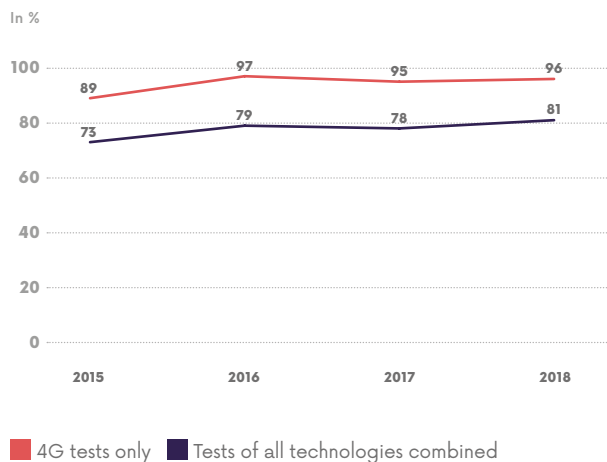
The average speeds measured by Arcep continue to rise. In particular, and for the first time ever, the average download speed measured on mobile networks in Metropolitan France, all operators and all types of location (rural, medium density and high density) combined, now stands at 30 Mbit/s. Looking only at 4G: connection speeds are also increasing, now reaching an average 39Mbit/s. The performance gap between the average 4G download speed and the average speed for 2G/3G/4G combined is tending to shrink as 4G becomes increasingly ubiquitous nationwide.

AVERAGE DOWNLOAD SPEEDS IN METROPOLITAN FRANCE, MEASURED BY ARCEP



Source: Arcep

PERCENTAGE OF WEB PAGES THAT LOAD IN UNDER 10 SECONDS IN METROPOLITAN FRANCE



Source: Arcep

On the web browsing front, 81% of the web pages Arcep tested in 2018 – from amongst a sample of the 30 most visited websites in France – loaded in under 10 seconds. 4G has also driven considerable gains in this area, as the percentage of web pages that load in under 10 seconds over a 4G connection now stands at 96%¹¹. There is therefore evidence that 4G delivers a clear improvement in the quality of operators' data services, which in turn bolsters the rise of mobile Internet use.



9. Digital market barometer 2018.

10. Arcep's electronic communications market scorecard, Q3 2018.

11. Arcep test results are available as open data: <https://static.data.gouv.fr/resources/monreseaumobile/20181019-104845/2018-10-lieuxdevie-arcepqos2018.csv>

6.2. Ongoing improvements to monreseau-mobile.fr

In December 2018, Arcep unveiled a roadmap for its “*Mon réseau mobile*” (My mobile network) tool, in response to local authorities wanting to perform their own tests and make use of crowdsourcing solutions. Part of this response was to give renewed impetus to its data-driven and crowdsourcing-based approach to regulation, by publishing a “regulator’s toolkit” for local authorities to perform tests in a controlled environment, to complement those performed by Arcep as part of its annual audit. This “regulator’s toolkit” is aimed at local authorities, and any other stakeholder wanting to perform comparable tests to satisfy their own needs, e.g. in as yet unexplored geographical areas. It will allow tests to be carried out in a controlled environment, thereby separating out the many outside factors that can influence the results, and distort their relevance, such as the type of mobile phone used, time of day or whether the test is performed outdoors or indoors. By making it easy to reuse these protocols, and making them more understandable, Arcep is hoping to encourage initiatives designed to complete its own set of actions.

Concerning apps for testing the quality of users’ mobile experience, such as crowdsourced app-based tests, Arcep has also published a preliminary version of its “Code of Conduct on mobile quality of experience” which addresses aspects that are specific to mobile networks, and whose goal is to ensure a minimum set of requirements in terms of the relevance, presentation and transparency of the test results. The mechanism will be designed in concert with stakeholders, to ensure that any additional results produced will enrich its own publications – as Arcep already publishes information as part of its legally mandated duties. For measurement tools, such as crowdsourcing apps, to be officially recognised by Arcep they will need to comply with the Code of Conduct. Arcep will consult with concerned stakeholders to fine tune this Code of Conduct, and so allow local authorities to rapidly have access to the list of compliant players. Here, Arcep’s aim is to support local elected officials in their use of tools whose findings can further improve the quality of coverage maps. The data collected could also be published on monreseau-mobile.fr

J’alerte l’Arcep

Launched in October 2017, the “*J’alerte l’Arcep*” platform is available to any citizen wanting to report an actual problem encountered with their mobile Internet, fixed Internet or postal services. Arcep received more than 34,000 reports in a single year through the platform. Of these, 62% concerned quality and availability issues with fixed or mobile services and 1.2% related to a net neutrality issue.

These reports provide valuable feedback for Arcep’s diagnostic capabilities. They help make it possible to quantify and identify the problems that users are encountering, to then steer Arcep’s actions towards the most appropriate solutions possible. When it comes to Internet quality of service, these reports have helped steer Arcep’s strategy for building tools to make test results more accurate and easier to compare. Reports regarding net neutrality issues have enabled Arcep to identify weak signals that constitute possible net neutrality infractions within a short amount of time, and help achieve a rapid remedy to the situation.

Arcep is continually working to improve the “*J’alerte l’Arcep*” platform, and especially its classifications and sub-classifications. Particular focus is on the “quality of service” classification, which represents the majority of customer complaints. It is also by increasing the number of details requested about particular cases that Arcep will be able to better examine certain topics in future.

2

Monitoring the data interconnection market



“The metabolism is changing. Continuous monitoring is essential”



53%

of the traffic to the main ISPs in France come from four content providers: Netflix, Google, Akamai and Facebook

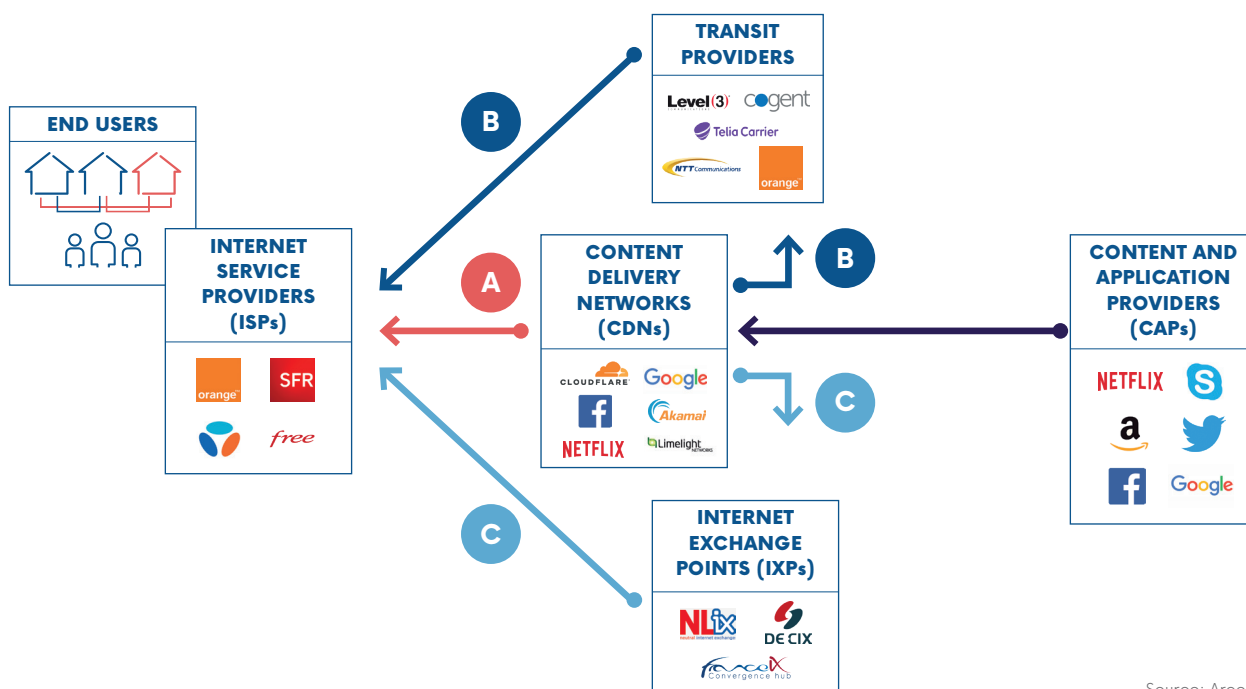
1. THE INTERNET'S EVOLVING ARCHITECTURE

Several stakeholders interact within the internet ecosystem: content and application providers (CAPs), hosting services, transit providers, Internet Exchange Points (IXPs), Internet Service Providers (ISPs), etc.

As the volume of data traffic being routed over the internet has increased, a new type of player has emerged: content delivery networks, or CDNs, which specialise in delivering large volumes of traffic to several ISPs, thanks to cache servers located near end users. These CDN get data from CAPs and may either have peering agreements directly with ISPs (A), go through a transit provider (B) or an IXP (C) to convey these data to the end user.

HOW CDN INTERCONNECT WITH DIFFERENT INTERNET STAKEHOLDERS

For illustrative purposes only. Does not depict the real interconnection relationships between the actors cited as examples.



Source: Arcep

1. N.B.: for more details on the technical terms employed, Arcep invites readers to refer to its barometer of data interconnection in France: <https://www.arcep.fr/cartes-et-donnees/nos-publications-chiffrees/linterconnection-de-donnees/barometre-de-linterconnection-de-donnees-en-france.html>



A CDN offers several types of added-value to CAPs, including:

- improving quality of service and quality of experience for the user;
- international connectivity (as with a transit provider);
- technical and business intermediation (as with a transit provider);
- serving as an alternative supplier to transit providers, which helps bring down overall routing costs.

As Arcep indicated in the 2018 edition of its report on the state of the internet in France², the internet's architecture is continually evolving, and several vertical integration scenarios can be observed. The current trend is one of convergence between different types of player. This includes shifting dynamics such as CDNs deploying their own infrastructure around the globe, and CAPs installing their own network infrastructure and CDN platforms closer to end users.

Newcomers to the market (CDNs or large CAPs) are thus able to circumvent the usual traffic routing intermediaries to some degree.

Another major trend is the advent of internal – aka on-net – CDNs. These servers are managed by the entity that owns them (CAP, CDN or ISP) but are installed within the ISP's network. To improve quality of service by moving closer to end users, CAPs form partnerships with ISPs in order to have their content hosted in cache servers placed inside operators' network. These on-net CDNs may belong to the operator that hosts them, or to a third party. They enable CAPs/CDNs to eliminate the need to host their own infrastructure, as operators do it for them. The advantage for operators lies in no longer having to transport traffic from an interconnection point (e.g. Paris or Marseille) right to end users.

In France, Google and Netflix are the two main companies that have installed on-net CDN in the largest French ISPs' networks.

2. https://www.arcep.fr/uploads/tx_gspublication/rapport-etat-internet-2018_conf050618.pdf

OPEN FLOOR TO ...



Sylvie LaPerrière, Interconnection and global infrastructure

Interconnection and investment in infrastructure to improve quality of service and competitiveness

A recent study from Analysys Mason¹ highlights online service providers' investments in infrastructure: between 2014 and 2018, these companies invested more than 300 billion dollars in internet infrastructure, or 75 billion a year, which is double their annual spending from 2011 to 2013. In Europe, these investments rose by 68% compared to that same period.

This trend is particularly pronounced with Google, as infrastructure is a key area of investment for us. Google Capex totalled 47 billion dollars between calendar years 2016 and 2018, and we are continuing to expand our infrastructure in 2019, which includes deploying our own submarine cables. And particularly one transatlantic submarine cable called Dunant – which will land on France's Atlantic coast by the end of 2020² – in partnership with Orange³. Dunant will be

the first submarine cable running between the United States and France to be installed in more than 15 years.

“Infrastructure is a key area of investment for Google.”

On the interconnection front, Google continues to offer an open peering policy⁴ which is designed to promote direct links with operators as much as possible, for the benefit of users. In France, we have peering links with all of the country's main operators.

Moreover, as part of this same drive to promote open peering, Google has supported the France IX⁵ exchange point from the start, which now has a PoP in Marseille and has become one of Europe's main hubs. More recently, in 2017 we joined RezoPole and the LyonIX⁶ internet exchange point.

These investments make it possible to provide French users with an excellent quality of service, as much for consumer services such as Google or YouTube as for all of the Google Cloud services for French businesses. This second area is crucial at a time when use of the cloud – and the associated technologies: data analysis, machine learning, etc. – has become vital to enterprises' ability to compete.

1. <http://www.analysismason.com/Consulting/content/reports/Online-service-providers-Internet-infrastructure-Dec2018/> (December 2018)

2. <https://www.blog.google/products/google-cloud/delivering-increased-connectivity-with-our-first-private-trans-atlantic-subsea-cable/>

3. <https://www.orange.com/fr/Press-Room/communiqués/communiqués-2018/Orange-et-Google-s-associent-pour-un-nouveau-cable-sous-marin-a-travers-l-Océan-Atlantique>

4. <https://peering.google.com/#/options/peering>

5. www.franceix.net

6. <https://www.rezopole.net/fr/news-rezopole/tag/google>

OPEN FLOOR TO ...



Nicolas Pisani, Network strategy manager – Southern Europe, Akamai

Akamai, a major interconnection market player

WHAT IS YOUR OVERALL VIEW OF THE INTERCONNECTION MARKET IN FRANCE?

France represents one of the biggest European markets for Akamai in terms of traffic volume. This position can be attributed to a solid development of the OTT market and to an accelerated pace of high speed network deployment.

In France, like in other countries, Akamai has good relationships with ISPs. Our philosophy is to work closely with them, to build future-proof and reliable interconnection architectures.

That said, France differs from other European markets in at least two respects.

First, certain French ISPs' interconnection costs are still quite high compared to other countries, where access providers prefer to apply a "content strategy" that gives priority to a technical partnership which guarantees performance and reliability.

Second, the interconnection market is highly concentrated in Paris. Internet service providers still have little desire to host CDN on their networks in other cities, despite the very positive impact that distributed architectures have on both performance and the cost of routing traffic to subscribers.

WHAT VALUE DO CDNS BRING TO THE CURRENT INTERCONNECTION MARKET? WHAT DISTINGUISHES AKAMAI FROM OTHER PLAYERS?

When it comes to distributing content, a distinction should be made between the owners (UGC platforms, VOD platforms, etc.) and aggregators like Akamai, which provide a distribution service but do not own or control the content.

Aggregators enable ISPs to receive and distribute a multitude of popular sources of content, while minimising the number of interconnection agreements that need to be established and managed. This is a major advantage for ISPs, as this consolidation of traffic sources allows them to optimise their interconnection costs.

In addition, and even if content consumption is becoming more and more local, the existence of CDN minimises the amount of traffic being relayed over international networks considerably, which in turn means better performance and a more efficient global internet. With traffic peaks of more than 80 Tbps, if our platform were to break down suddenly worldwide, or even in Europe, the internet would probably become congested.

More generally, the services available on the Internet (IPTV, e-Commerce, e-Banking, social networks, etc.) need to rely on distributed infrastructures offering robustness, performance, extreme scalability and security. Using a CDN like Akamai is the only way to cover these four basic needs while controlling costs.

Akamai's success lies in the power and reach of its infrastructure, its closed ties with more than 1200 ISPs around the globe, and its ability to provide customers with distribution-related services, such as security, resource optimisation, performance analysis and, more recently, customer identity and access management (CIAM).

WHAT DIRECTIONS WILL AKAMAI'S STRATEGY TAKE IN FUTURE?

Akamai is investing in virtualisation, automation and more generally in the industrialisation of its global platform. To give an example, we have begun to deploy standardised clusters capable of generating up to several Tbps of traffic. Akamai has also taken its model to the next level by deploying its own international backbone over the past two years – whereas, prior to that, traffic between Akamai infrastructures had been relayed over the public internet. Lastly we are deploying our own datacentres in the US, and gearing up to do so in Europe as well.

Our aim in all of these areas is twofold. First, to improve the quality of service we provide to our customers on an ongoing basis and, second, to optimise our cost structure to stay competitive in a fiercely competitive market.

2. STATE OF DATA INTERCONNECTION IN FRANCE

Thanks to the information gathering it does on data interconnection and routing, Arcep has technical and financial data on interconnection from the first half of 2012 to second half of 2018. For confidentiality reasons, the published findings³ are only aggregate results.

To sustain the future of these publications on data interconnection, in December 2018 Arcep created a dedicated barometer. This barometer will be updated annually, to coincide with the publication of the report on the state of the internet in France⁴.

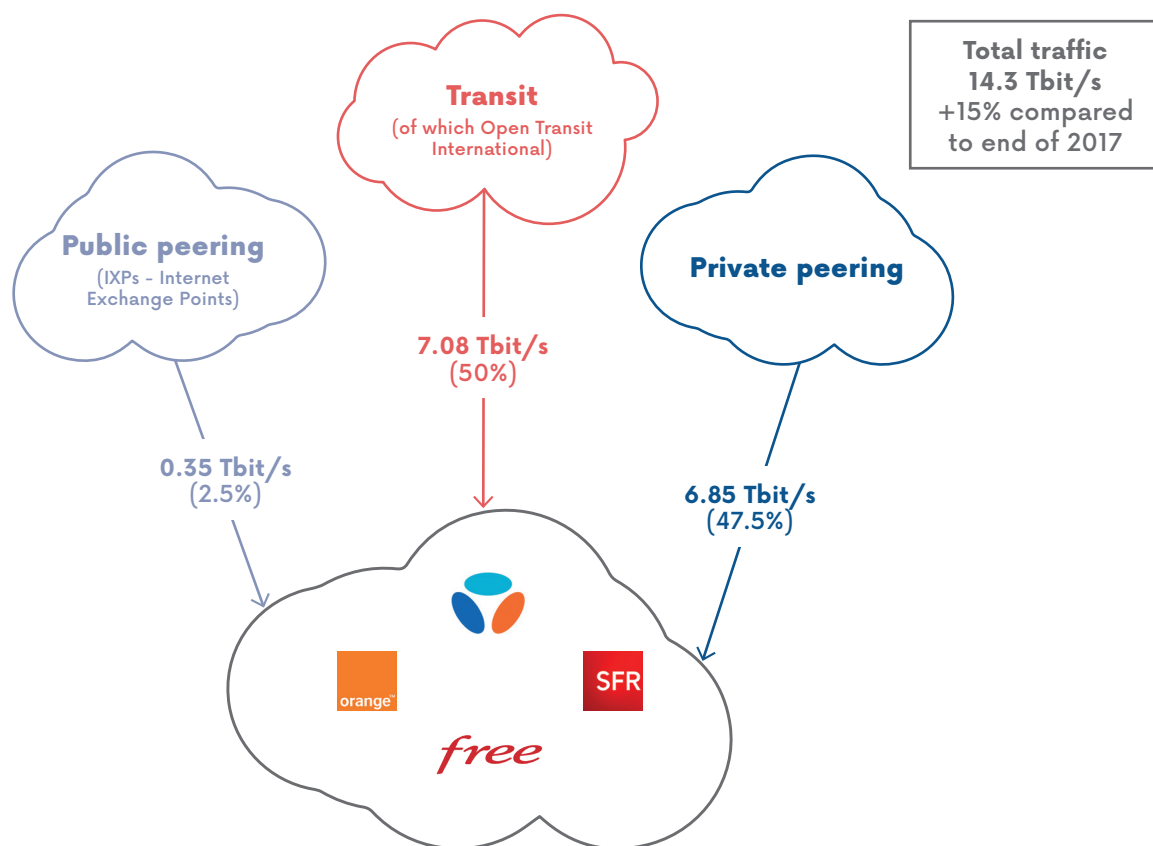
2.1. Inbound traffic

Inbound traffic to the four main ISPs in France has increased from more than 12 Tbit/s at the end of 2017 to 14.3 Tbit/s at the end of 2018, which translates into a 15% increase in a single year. Half of this traffic comes from transit links. This relatively high rate of transit is due in large part to transit traffic between Open Transit International (OTI), a Tier 1 network belonging to Orange, and the Orange backbone and backhaul network (RBCI), which makes it possible to relay traffic to the ISP's end customers.

The country's other ISPs do not operate as transit providers, and so make greater use of peering.

Also worth noting is the slight decrease in peering in favour of transit. This change is due in large part to the increasing amount of traffic coming from on-net CDN (Cf. 2.5. Breakdown of traffic by interconnection mode)

BREAKDOWN OF INBOUND TRAFFIC (95TH PERCENTILE) ON THE NETWORKS OF THE MAIN ISPs IN FRANCE (END OF 2018)

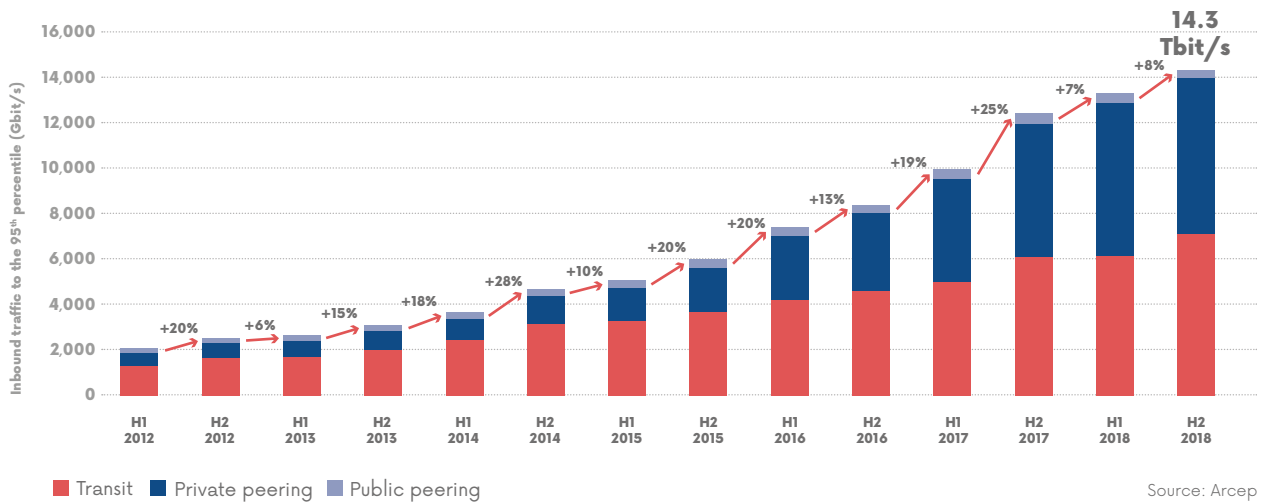


Source: Arcep

3. Results obtained from operators' responses to information gathering on the technical and financial conditions of data interconnection and routing, whose scope is detailed in Arcep Decisions No. 2014-0353 and No. 2017-1492-RDPI amending Arcep Decision No. 2012-0366.

4. <https://www.arcep.fr/cartes-et-donnees/nos-publications-chiffrees/linterconnection-de-donnees/barometre-de-linterconnection-de-donnees-en-france.html>

INBOUND TRAFFIC TO THE MAIN ISPs IN FRANCE, FROM H1-2012 TO H2-2018

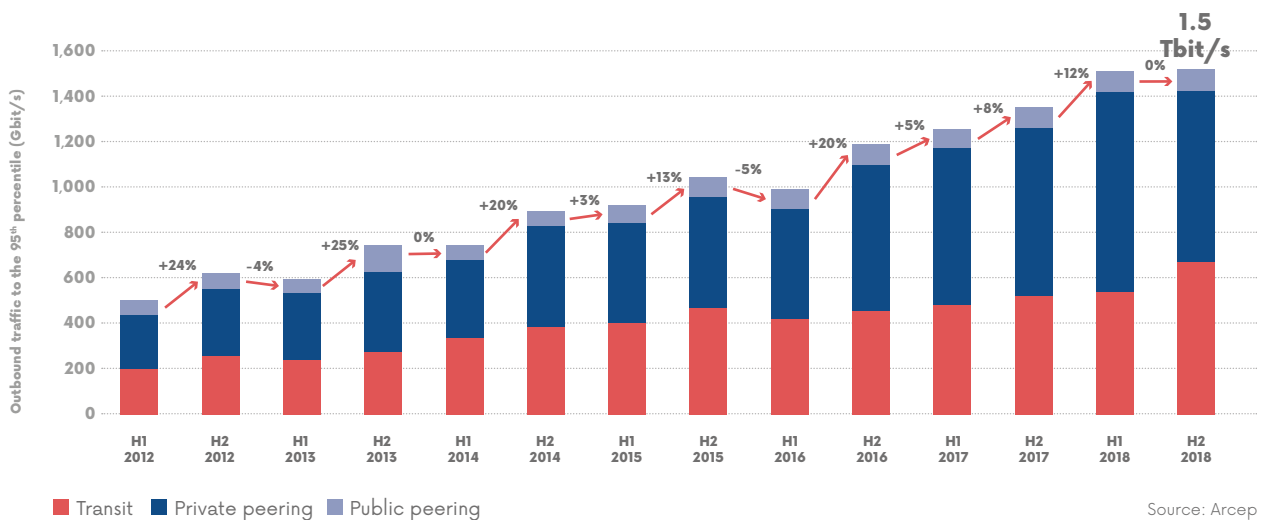


2.2. Outbound traffic

By the end of 2018, outbound traffic on the networks of France's four main ISPs reached of 1.5 Tbit/s, or 12% more than at the end of 2017. This traffic tripled between 2012 and 2018. Also worth

noting is that there appears to be a greater increase in outgoing traffic in the second half of the year.

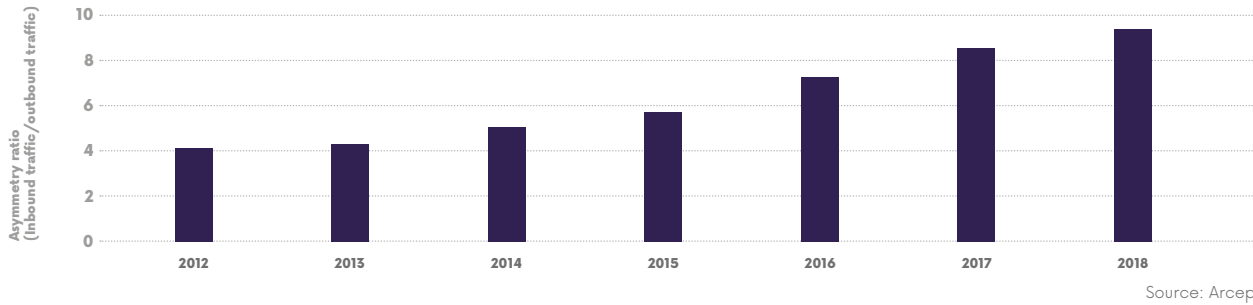
OUTBOUND TRAFFIC FROM THE MAIN ISPs IN FRANCE, FROM H1-2012 TO H2-2018



There is far less outbound than inbound traffic. The asymmetry between the two has in fact increased from a ratio of 1:4 in 2012 to one of more than 1:9 in 2018. This widening gap is due chiefly

to the increase in the amount of multimedia content (audio and video streaming, downloading large media files, etc.) customers consume.

ASYMMETRY RATIO BETWEEN INBOUND AND OUTBOUND TRAFFIC FOR THE MAIN ISPS IN FRANCE BETWEEN 2012 AND 2018

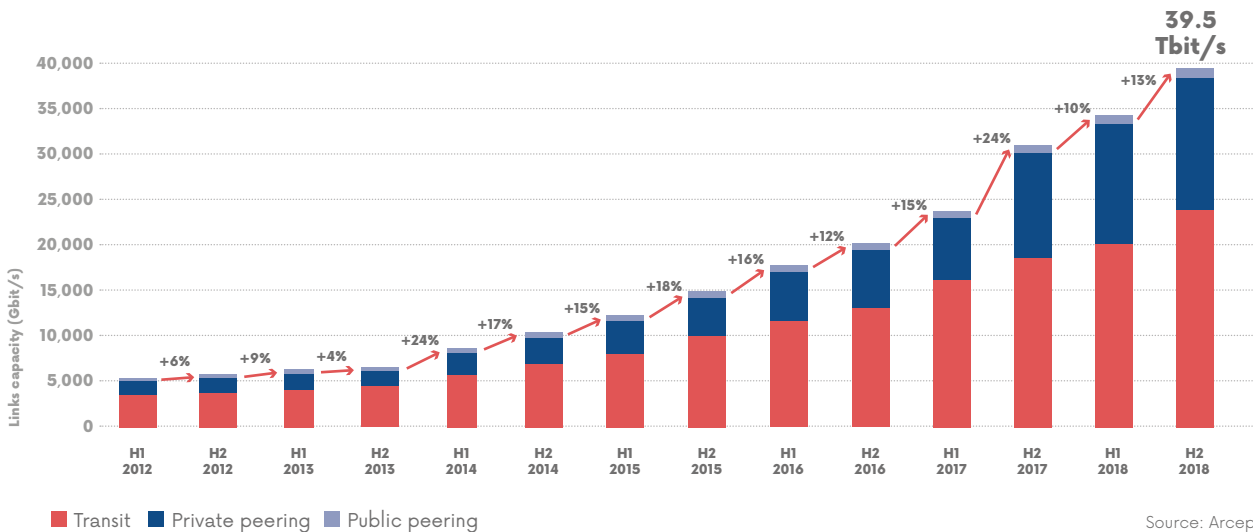


2.3. Evolution of installed capacities

Installed interconnection capacities have increased at the same pace as incoming traffic. Installed capacity at the end of 2018 is estimated at 39.5 Tbit/s, or 2.8 times incoming traffic. This ratio

does not exclude occasional congestion incidents, which can occur on a particular link or links, depending on their status at a given moment in time.

PROGRESSION IN THE INTERCONNECTIONS CAPACITY OF THE MAIN ISPs IN FRANCE BETWEEN H1-2012 AND H2-2018



2.4. Evolution of interconnection methods

Peering vs. Transit

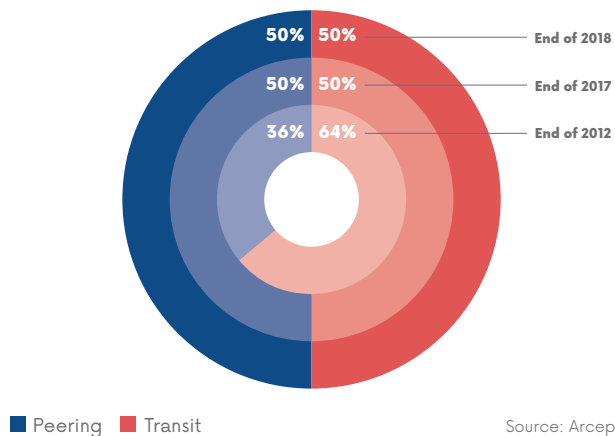
The overall trend has been a sharp rise in peering's share of interconnection link, due chiefly to the increase in installed private peering capacity between ISPs and the main content providers.

Between the end of 2017 and the end of 2018, however, peering's share (50%) did not increase, which can be attributed chiefly to the fact that a percentage of peering traffic has been replaced by traffic from on-net CDN.

Public peering traffic remains more or less unchanged: its relative share (4% at the end of 2017 vs. 2.5% at the end of 2018) is decreasing in favour of private peering (46% at the end of 2017 vs. 47.5% at the end of 2018).

EVOLUTION OF PEERING AND TRANSIT FOR THE MAIN ISPs IN FRANCE

(in proportion of inbound traffic volume)

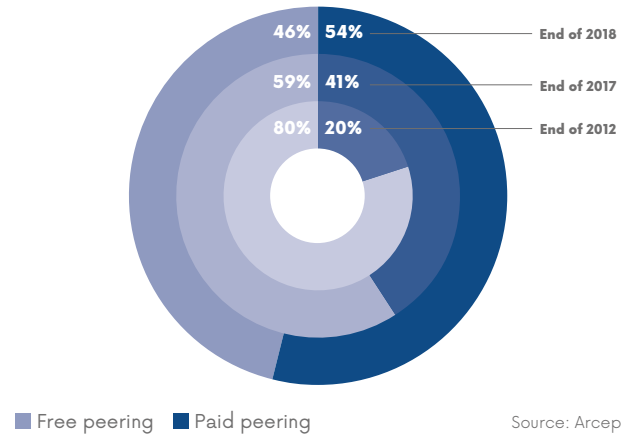


Free vs. paid peering

The percentage of paid peering rose from 41% at the end of 2017 to 54% at the end of 2018. This change is due primarily to the increase in private peering traffic, of which a sizeable share is paid, notably when there are considerable traffic asymmetries. Peering between companies of a comparable size still remains free, by and large.

EVOLUTION OF PAID PEERING PARTS FOR THE MAIN ISPs IN FRANCE

(in proportion of inbound traffic volume)

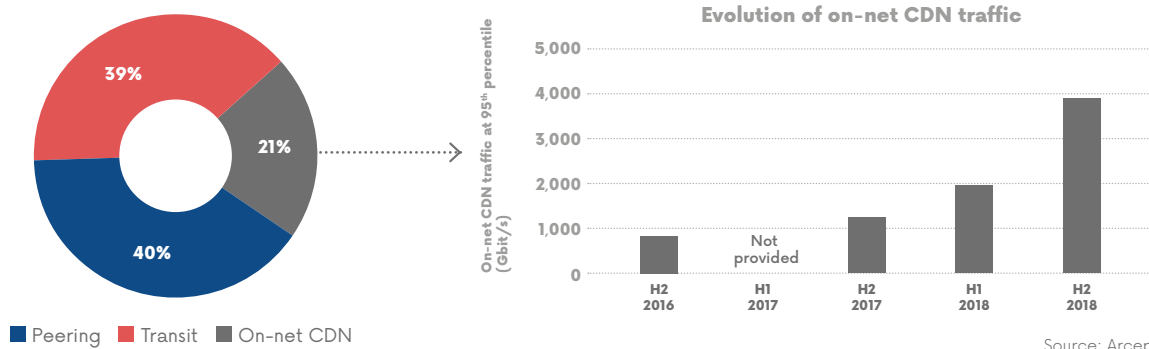


2.5. Traffic breakdown by interconnection type

By the end of 2017, traffic coming from on-net CDN had increased to around 1.2 Tbit/s. At the end of 2018, this traffic had tripled to 3.8 Tbit/s, or 21% of those four ISPs' total traffic to final customers. This percentage – which increased considerably from 9% at the end of 2017 – varies considerably from one ISP to the next: for some operators this traffic represents not even 1% of their traffic to final customers, while for others it accounts for more than a third of the incoming traffic being injected into their networks.

In addition, the ratio of inbound/outbound traffic varies between 1:5 and 1:20 depending on the operator. In other words, data made available through on-net CDN are viewed between five and twenty times, on average.

TRAFFIC BREAKDOWN IN FRANCE BY INTERCONNECTION TYPE (END OF 2018)

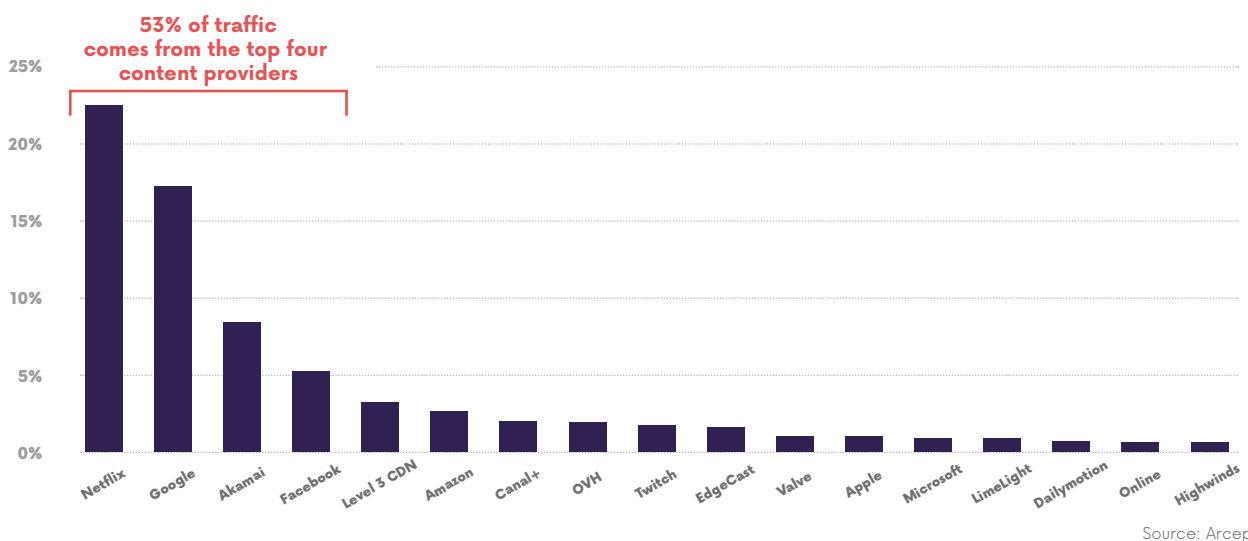


2.6. Traffic breakdown by origin

More than half (53%) of all traffic to France’s main ISPs’ customers comes from four providers: Netflix, Google, Akamai and Facebook. This testifies to the increasingly clear concentration of traffic around

a small number of players whose position in the content market is more and more entrenched.

TRAFFIC BREAKDOWN BY ORIGIN FOR THE MAIN ISPs IN FRANCE (END OF 2018)



2.7. Evolution of costs

The range of transit and peering fees has not changed since last year.

The negotiated price of transit services still ranges €0.10 (plus VAT) and several euros (plus VAT) per month and per Mbit/s. As to paid peering, prices range from between €0.25 (plus VAT) and several euros (plus VAT) per month and per Mbit/s⁵.

On-net CDN are free in most cases. They can be charged for, however, as part of a broader paid peering solution that the CAP has contracted with the ISP.

5. Price ranges only reflect the prices that the companies who answered the questionnaire pay for transit, peering or on-net CDN solutions.

OPEN FLOOR TO ...



Theresa Bobis, Regional Director, Southern Europe, DE-CIX

Marseille: a new Cloud, Interconnection and Digital Hub

As traditional global traffic flows are changing and heading towards the south, DE-CIX took the right steps years ago in establishing its Internet Exchanges in the South of Europe – including DE-CIX Marseille in 2015. For DE-CIX, Marseille is one of the key European landing stations for a large number of international subsea cables and global Internet transit pathways.

Marseille serves as a gateway to Western Europe, connecting carriers from the Middle East and Africa (MEA) and the Asia-Pacific to vital European peering nodes for access to the global Internet. Unlike most of the markets in which DE-CIX invests, this market is more influenced by growth in demand far afield than it is by growth in local demand. Marseille is tightly intertwined with the markets of Africa, Asia, and the Middle East – significantly, the three markets with the fastest growing appetite for Internet bandwidth among all global markets. While global bandwidth demand growth has slowed in the past five years, each of these regions has retained more than 40 percent compound annual growth in Internet bandwidth usage.

By positioning itself in Marseille, DE-CIX provides neutral interconnection facilities at the prime intersection between key subsea routes in the Mediterranean and the continental hubs of Europe. DE-CIX's strategy benefits from the rapid expansion of bandwidth between Europe and Asia, the Middle East and Africa. A robust bandwidth demand growth between these regions is forecast to continue over the next five years. Capacity between Europe and the Middle East could more than quadruple by 2022 and increase more than 6-fold between Europe and Africa during the same period.

As the interconnection environment in Marseille continues to expand, DE-CIX customers will benefit from improved economies of scale, with access to more than 130 peering partners at Interxion's rapidly growing MRS campus alone. The launch of Microsoft's France South Azure region will also fuel demand and opportunity in the local IX environment. For customers who require onward connectivity to Frankfurt or Paris, a plethora of carrier options is available in Marseille providing onward connectivity at on-net rates that are comparable to route pricing found in any major European market. DE-CIX's GlobePEER Remote route from Marseille to Frankfurt provides another connectivity option for customers that require access to the Frankfurt market – as one of the biggest international interconnection ecosystems around the globe – but prefer to keep their colocation footprint in Marseille.

The growth in demand from the Middle East and Africa to Europe indicates that European carriers and content providers will need to move closer to the network edge with these rapidly growing markets. This movement is already taking place, transforming Marseille into one of Europe's largest bandwidth and interconnection hubs. With few promising interconnection ecosystems on the vast and heavily populated subsea route between Singapore and Europe, Marseille will continue to be an appealing destination for networks in the Mediterranean Basin and beyond for decades to come.



OPEN FLOOR TO ...



Bertrand Yvain, partner-founder, HOPUS

A different kind of interconnection – The HOPUS vision for network development

The many changes in how we use the internet have driven an increase in connection speeds and interactivity. These two basic requirements have naturally led content and application providers – whose innovations have been the driver of this change – to move closer to end customers. The different forms of convergence between the internet ecosystem's players seek to increase the networks' performance and reliability, as much in terms of bandwidth as latency. These changes are reflected in the growing use of peering, and especially paid peering, for interconnection. Transit providers have become increasingly less relevant for handling highly asymmetric data exchanges on a local scale. However, the growing number of peering agreements constitute a heavier technical, business and legal burden.

HOPUS wants to facilitate these exchanges, notably via its hybrid, peering and transit IP network. This network serves as an intermediary, committed to technical excellence and providing a clear and no-surprises business relationship, based on a distinction between inbound and outbound traffic. Connected stakeholders therefore pay for the traffic they send, and receive compensation for relaying the traffic they receive. We believe that this business model enables us to keep pace with the networks' expansion. It also constitutes a form of private mediation, enabling less powerful players to enjoy the benefits of private peering, while also opening the way for new content and applications providers to emerge.

For twenty years now, we have been witnessing the internet ecosystem's transition.

Once composed mainly of integrated players, providers of both access and content, their exchanges were primarily symmetric. Today, most of the traffic comes from specialised players: content and application providers, hosting services and content distribution networks. Their traffic is both increasing on massive scale and highly asymmetric. This is a challenge for building networks and occupying installed capacities. The issues at hand can be clearly seen in the congestion on the network and tensions between the different players, which are threatening the networks' neutrality.

“Speed is no longer the sole criterion for measuring quality.”

One of the virtues of how we do business is ensuring that all of our members are treated equally. The remuneration that each of them can receive is rooted in the quality commitments they make on relaying the traffic they receive. We believe upholding this value is the key that opens the floodgates on ever increasing speeds: 5G networks, the Internet of Things, the proliferation of streaming services, etc.

The nature of the content itself has also changed. Once static, monolithic and sometimes viewed offline. The ubiquity of mobile devices and the growing focus on

interactivity has made it composite, dynamic and personalised – all properties that have meant that speed is no longer the sole criterion for measuring quality. Latency is critical for ensuring smooth interactions with users, as testified by the very existence of the different types of content distribution. Improving latency is crucial to the HOPUS network's development, achieved notably by establishing distributed points of presence close to users. This directly benefits every type of player, all eager to ensure their customers' satisfaction.

The special business relationship we have with our members forbids us from calling on transit providers, whose approach is not compatible with our commitments. This means that the HOPUS network cannot be joined by the entire internet, but rather constitutes a closed set of connected networks. This is an added advantage that guarantees secure exchanges and protects against denial of service attacks, on top of circuit provisioning and the arsenal of tools required to manage networks properly.

The HOPUS way stands out from the usual internet stakeholders in how it operates. Our disruption is not technological, but lies rather in the invitation to a new brand of cooperation. After five years of existence, our alternative model has proven its relevance and ability to support the market's development, providing another way to manage interconnections.

Accelerating the transition to IPv6



“The dearth of IP addresses is deepening: switch to IPv6 now”

2020

According to current Arcep estimates, the supply of available IPv4 addresses will have run out by 2020



1. IPv4 ADDRESSES ARE RUNNING OUT QUICKLY, THE TRANSITION TO IPv6 IS A GROWING IMPERATIVE

IPv4, which stands for Internet Protocol version 4, has been used since 1983 to allow the Internet to function: each device or machine that is connected to the Internet (computer, phone, server, etc.) has an IPv4 address. The protocol is technically limited to 4.3 billion addresses¹, but the Internet's popularity, the range of uses and the proliferation of connected objects have steadily depleted the number of available IPv4 addresses, with some parts of the world being more deeply affected than others. At the end of June 2018, France's four largest operators (Bouygues Telecom, Free, Orange, SFR) had already assigned between 88% and 99% of their supply of IPv4 addresses².

IPv6 specifications were finalised in 1998. They incorporate functions for increasing security by default and optimising routing. Above all, though, IPv6 delivers a virtually infinite number of IP addresses: 667 million for each square millimetre of the earth's surface³.

Because of the size, disparity and complexity of today's Internet, the transition from IPv4 to IPv6 can only take place gradually, starting with a cohabitation phase. Then, once every player has migrated, IPv4 will be fully replaced (switch-off phase). The transition to IPv6 began in 2003 but, in 2018, the Internet was still only in the early part of the cohabitation stage⁴.

The slow pace of the transition could result, first, in malfunctions for certain types of Internet service (smart home control systems, online gaming, etc.) because of the solutions for sharing IPv4 addresses between several customers that were put into place to deal with the dearth. Second, it is likely to create a barrier to entry for newcomers to the market. IPv4 will need to stay in place for as long as the Internet's entire technical chain has not fully switched over to IPv6 – otherwise a website that is unable to obtain an IPv4 address will be inaccessible to customers whose ISP is not IPv6-enabled. But the date on which IPv4 addresses are no longer available in Europe is fast approaching.

In the 2018 edition of its report on the state of the Internet in France, Arcep estimated that the supply of available IPv4 addresses would run out by the end of 2021. The pace at which the last remaining IPv4 blocks are being acquired is accelerating, however, and Arcep now estimates that the supply will run out towards the end of Q2 2020⁵.

1. IPv4 addresses use a 32-bit code. A maximum 232, or 4,294,967,296 addresses can theoretically be assigned simultaneously.

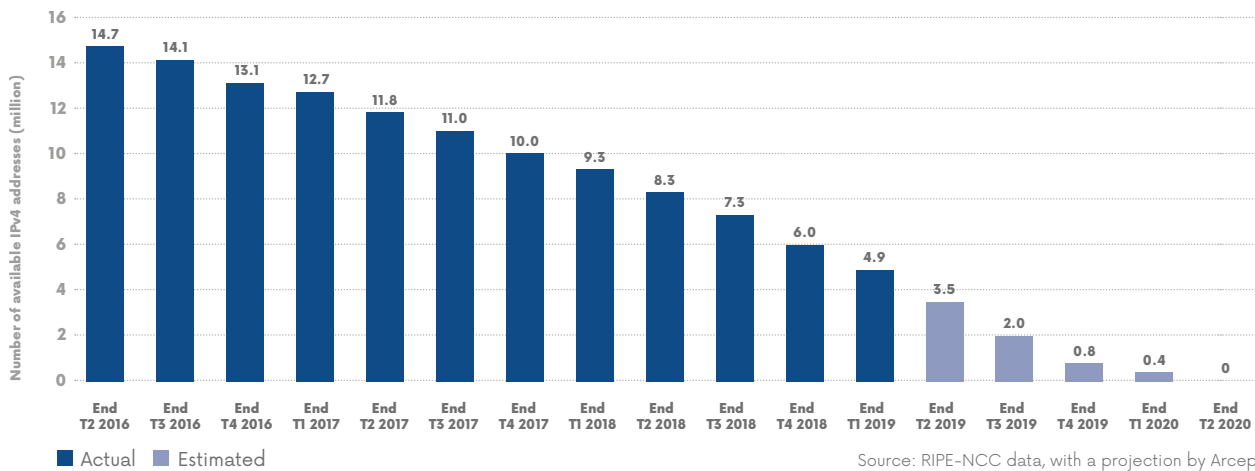
2. Data that Arcep collected from ISPs, in accordance with Arcep Decision No. 2018-0268 of 15 March 2018.

3. IPv6 addresses use a 128-bit code. A maximum 2128 (i.e. around 3.4×1038) addresses can theoretically be assigned simultaneously.

4. Arcep specifies that the conclusions and work mentioned pertain only to the internet, and do not apply to private interconnection between two players, notably the interconnection of two operators' networks for terminating VoIP calls.

5. RIPE-NCC data, with a projection by Arcep

ASSESSMENT AND ESTIMATE OF AVAILABLE IPv4 ADDRESSES⁶



In June 2016, Arcep delivered a report to the Government that was produced in cooperation with Afnic, and which contained several actions designed to support and accelerate the transition to IPv6. Since then, Arcep has been publishing a barometer of the transition to IPv6, as part of its data-driven regulation. It has also begun a co-constructed initiative with the Internet ecosystem in France, to federate the community and help speed up this transition.

2. BAROMETER OF THE TRANSITION TO IPv6 IN FRANCE

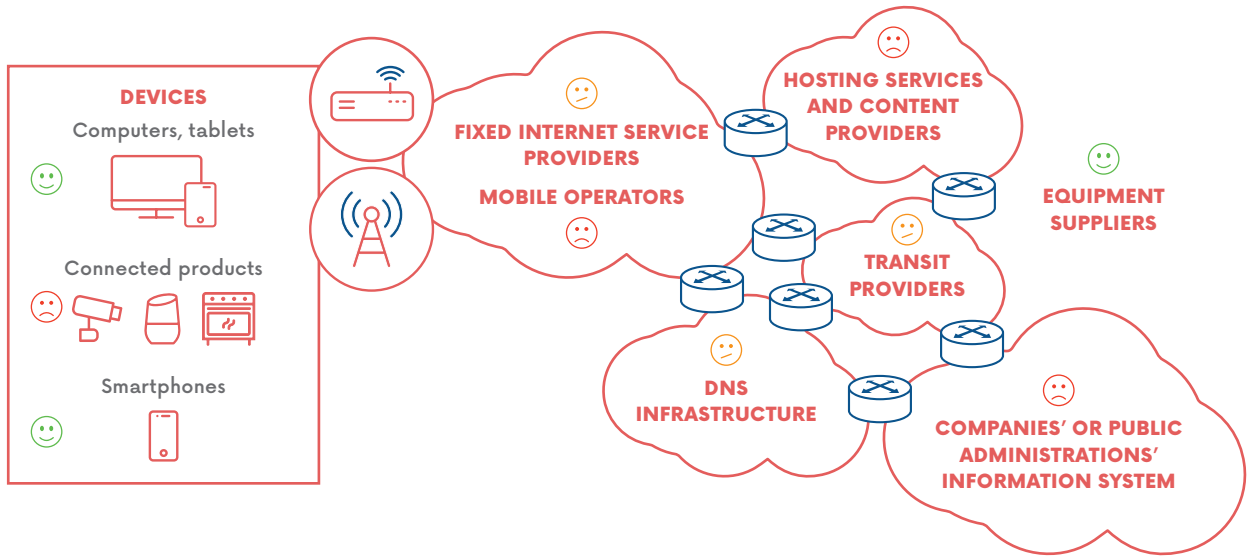
As recommended in its June 2016 report, Arcep has been publishing a barometer of the transition to IPv6 since December of that year. The purpose is to keep users informed in an ongoing fashion. The barometer compiles data produced and provided by third parties (Cisco, Google and Afnic) and data that Arcep collects directly from the main operators in France. It provides a snapshot of the progress being made in France, along with three-year deployment forecasts. Arcep published the 2018 edition of the barometer on 10 October 2018.

Arcep uses a number of different indicators to assess the status of IPv6 deployment in France, for the different stakeholders involved in the transition. As the diagram below reveals, stakeholders are at varying stages in their deployment.



6. Simulation performed with a polynomial interpolation, and with a hypothesis of assigning 1,024 IPv4 addresses per LIR until the last one million available IPv4 addresses, then 256 IPv4 addresses per LIR until they run out. Using RIPE data from 2 April 2019, the simulation gives an end date for IPv4 of 17 July 2020.

STATUS OF THE TRANSITION TO IPv6 FOR THE ECOSYSTEM'S DIFFERENT PLAYERS



😊 Full or high compatibility with IPv6 😐 Partial compatibility with IPv6 😞 Little or no compatibility with IPv6

Source: Arcep

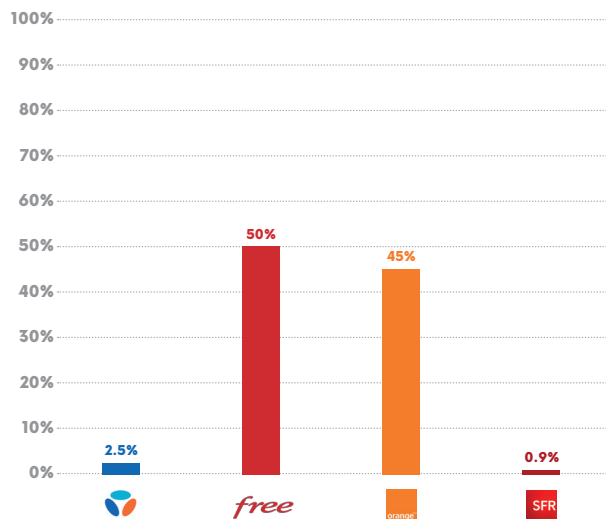
These findings confirm the progress made in the rate of IPv6 use in France, which stood at 23% in October 2018. The barometer provides a detailed look at the status of the transition for each of the ecosystem's stakeholders.

2.1. Fixed Internet service providers

The following charts provide a snapshot of the current status of IPv6 deployment, along with forecasts for the main operators' fixed network in France.

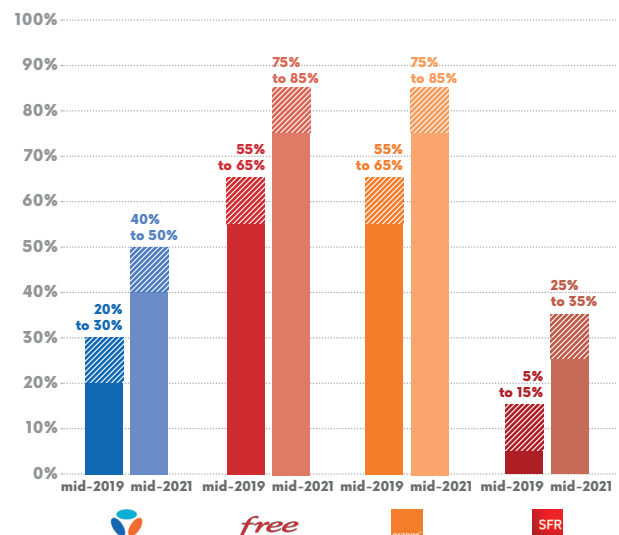
Even though predictions indicate that the supply of available IPv6 addresses will run out by Q2-2020, some operators still have no plans for deployments on their fixed networks that will allow them to respond to this dearth in the medium-term which, as indicated above, would seem problematic.

PERCENTAGE OF IPv6-ENABLED CUSTOMERS ON THE MAIN OPERATORS' FIXED NETWORK IN FRANCE



Source: Data collected by Arcep from operators in mid-2018, regarding their own network.

PERCENTAGE OF IPv6-ENABLED CUSTOMERS FORECAST ON THE MAIN OPERATORS' FIXED NETWORK IN FRANCE

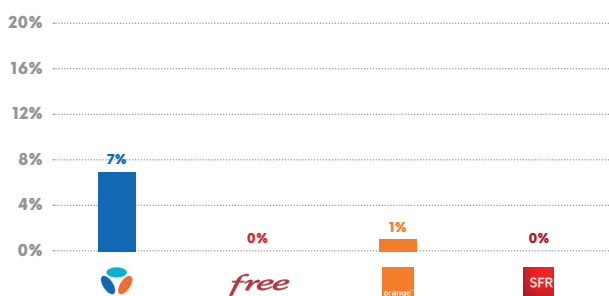


Source: Data collected by Arcep from operators in mid-2018, regarding their own network. Figures subject to change.

2.2. Mobile operators

The following charts provide a snapshot of the current status of IPv6 deployment, along with forecasts for the main operators' mobile network in France.

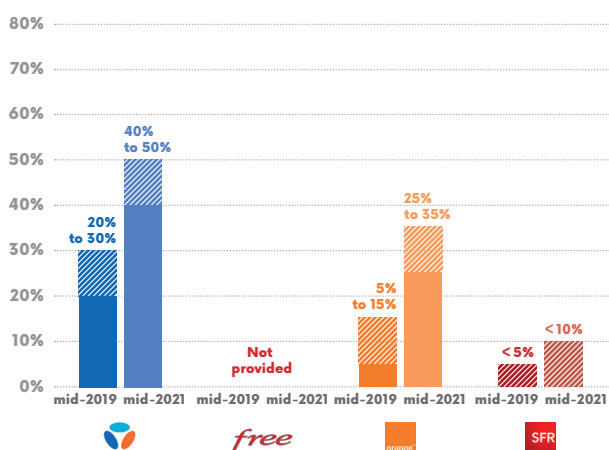
PERCENTAGE OF IPv6-ENABLED CUSTOMERS ON THE MAIN OPERATORS' MOBILE NETWORK IN FRANCE



Source: Data collected by Arcep from operators in mid-2018, regarding smartphones (default APN for voice + data plans).

Even more than on fixed networks, the pace of mobile networks' future IPv6 deployments is very likely to make it impossible to deal with the issues of an overall dearth of IPv4 addresses.

PERCENTAGE OF IPv6-ENABLED CUSTOMERS FORECAST ON THE MAIN OPERATORS' MOBILE NETWORK IN FRANCE



Source: Data collected by Arcep from operators in mid-2018, regarding their own network. Figures subject to change.

More specifically:

- If 100% of xDSL and FTTH SFR customers are already compatible (0% on cable), fewer than 1% of them are enabled – i.e. able to send and receive IPv6 traffic. Upcoming activations, although higher than the latest announcements from the operator, remain very weak (25% to 30% in mid-2021). Since a large majority of clients do not enable IPv6 manually, Arcep is urging SFR to perform this default activation as most other operators have. As for mobile networks: SFR forecasts fewer than 10% of customers will be activated in mid-2021.
- Arcep notes Bouygues Telecom's deployment efforts on mobile networks, but regrets the drop in migration forecasts for fixed networks: 40% to 50% of customers are expected to be activated by mid-2021, compared to the 75% to 85% announced at the end of 2020 in the previous barometer.
- On fixed networks, the current rates of activated customers of Free and Orange are relatively high (respectively 50% and 45%), but projections on the same indicator for mid-2021 will make it impossible to complete the transition in the medium term (between 75% and 85% for both ISPs). On mobile networks, the rate of activated customers expected by Orange in mid-2021 is up but remains limited (25% to 35%); Arcep regrets that Free Mobile has not been able to communicate their forecasts.

2.3. Web hosting services

Web hosting services continue to constitute one of the main bottlenecks in the migration to IPv6: of the most popular websites in France according to Alexa rankings, only 26% are IPv6-enabled⁷. A site is considered IPv6-enabled if its domain name is mapped as being IPv6 (AAAA) in the DNS server record.

Note that the percentage of web pages that are IPv6-enabled (IPv6 content) is significantly higher than that (61%)⁸. The reason is that many of the smaller content providers operate websites (generally small number of pages viewed) that are not IPv6-compatible.

26%
of the most popular websites in France are IPv6-enabled

61%
of the most popular web pages in France are IPv6-enabled

Source: Cisco 6lab au 28/09/2018 (6lab.cisco.com). Data on Alexa's Top 731 sites in France www.alexa.com/topsites/countries

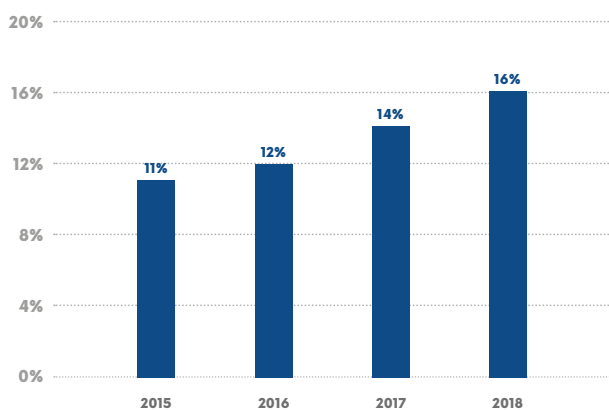
7. Cisco 6lab as of 08/10/2018 (<http://6lab.cisco.com>). Data on Alexa's Top 731 sites in France www.alexa.com/topsites/countries

8. Ibid



The percentage of IPv6-ready sites falls to a mere 16% when looking at the 3 million .fr, .re .pm .yt .tf and .wf⁹ websites. This figures has been rising since 2015, albeit at a pace that seems far from making it possible to achieve a complete transition to IPv6 by the third quarter of 2020.

PERCENTAGES OF IPv6-ENABLED WEBSITES ON .FR, .RE, .PM, .YT, .TF AND .WF DOMAIN NAMES



Source: Afnic data, July 2018.

For more information on the status of IPv6 deployment, the barometer of the transition to IPv6 is available on the Arcep website¹⁰.

Arcep Decision No. 2019-0287 of 12 March 2019 on implementing surveys of the electronic communications sector was updated, to take into account stakeholders' feedback on the information gathering mechanism that is in place. The main changes regarding the collection of information for the barometer of the transition to IPv6 were:

- The inclusion of operators that have between 5,000 and 3,000,000 active (fixed or mobile) retail market subscriptions to enable Arcep to improve its knowledge of the transition for all of the concerned operators;
- For mobile networks, specifying the number of IPv6-ready and enabled customers by technology and obtaining more information on IPv4 address-sharing, to improve the accuracy of the published information, and be able to better detect any bottlenecks;
- Simplifying the questionnaire for hosting services, to only request information that will be used for the barometer of the transition to IPv6.

These changes will help improve the quality of the information that Arcep publishes, and guarantee greater transparency on the transition's progress. The 2019 edition of this barometer will be published in the second half of 2019.

9. Afnic data, July 2018.

10. <https://www.arcep.fr/cartes-et-donnees/nos-publications-chiffrees/transition-ipv6/barometre-annuel-de-la-transition-vers-ipv6-en-france.html>

OPEN FLOOR TO ...



Nicolas Guillaume, Secretary-General, Alternative Telecoms Operators Association (AOTA)

IPv6: to enable all innovations to thrive in Europe

According to several projections, IPv4 addresses in Europe will run out in 2020. So more or less tomorrow. It is crucial that we act now to enable all innovations to develop, and not impede telecoms market competition between those that will have sufficient IPv4 resources and new entrants.

The situation has reached such a critical point that, already back in the summer of 2016, Apple reminded its community of developers that any apps that did not support IPv6-only networking would not be carried on the App Store.

Once leader in terms of IPv6 penetration, thanks in particular to ISP Free's large-scale push and, on a smaller scale, the Nerim transition, France today appears to be falling behind when it comes to actual adoption.

If the transition to IPv6 has been underway for some time on fixed networks, mobile networks has a great deal of catching up to do.

Hosting services and content and applications providers still do not seem to have fully grasped the issues. Major cloud platforms still do not provide satisfactory IPv6 solutions, for instance. One example is Twitter, which does not provide an IPv6 interface for its services. And France's federal government is not really setting an example here: the online tax service can still only be accessed in IPv4.

The situation is such that, in many cases, IPv4 networks switch subscribers back over, even though they are IPv6-enabled, to allow them to connect to online services, perform

administrative procedures, or dialogue with end users whose infrastructures are unable to manage IPv6.

We are seeing severe inertia in the hosting sector. The reason: a wait-and-see attitude amongst their business customers who have no incentive to switch to IPv6. The epitome of the snake eating its own tail: operators are well aware that, even though IPv6 products exist, their subscribers' traffic is still largely IPv4. Hosting companies explain that there is no reason to encourage their customers to switch over to IPv6 because they are mainly processing IPv4 traffic.

“What is needed then is a paradigm shift, driven by a concerted approach between several players with theoretically disparate interests.”

Clearly, without a concerted approach involving all of the stakeholders, any purely sector-driven action is bound to only partially succeed... or partially fail.

The “business market” is key to the success of a massive and true migration to

IPv6. It is only because the services layer will be capable of managing IPv6 natively and efficiently that hosting services will be able to switch over to IPv6, and that ISPs' traffic can become mostly IPv6. The final recalcitrant players, notably in the mobile market, will therefore have an incentive at last to migrate to IPv6.

What is needed then is a paradigm shift, driven by a concerted approach between several players with theoretically disparate interests.

If the legislator can intervene to create some forms of “incentivising constraints”, Arcep could set out the nominal technical conditions for IP interconnection, delivering economic signals that encourage having IPv6 for the main connection.

The Government could lead by example when awarding public procurement contracts – favouring players capable of providing an IPv6 connection for access and IPv6-only solutions for (cloud, hosting, app development) services – switching over to IPv4 only as a temporary measure.

More than ever before, local players who are AOTA members want to play an essential role, to assist government authorities and Arcep in this collective effort to make a proper transition to native IPv6. How? By assisting their customers locally – including many local authorities who also need to lead by example – and by helping them to improve their expertise through concrete actions.

OPEN FLOOR TO ...



Cédric Schroerer, Head of infrastructures, Orne THD

Deploying IPv6 to accelerate growth

Deploying IPv6 solves two major issues we are facing today: the technical restrictions of CGNAT¹ due to the insufficient number of IPv4 addresses to satisfy all of our subscribers, and the proliferation of digital devices in the home.

While awaiting IPv6 deployment, war was being waged on our CGNAT routers where new connections from some were disconnecting others, which affected every service equally. In addition to tarnishing our image, our technical team was overwhelmed by NAT-related issues. Resigned subscribers went back to ADSL connections, preferring stability over speed. So all of these issues had to be eliminated quickly and definitively.

The problem lay with the provisioning² of our cable modems. Because they are a disparate bunch, with a mix of Cisco and Technicolor hardware, itself subdivided into several models... telling all of our cable modems to “go find your /56” was a complicated affair. We needed help from both our equipment suppliers and the provider of our provisioning solution.

On a positive note, we did keep the manufacturer’s original firmware. Our modems have thus been IPv6-ready from the start... without even knowing. Our provisioning with the DOCSIS standard nevertheless meant we had to know all of the right parameters to be able to tell the modem to initiate its DHCPv6-PD and SLAAC configurations automatically, after start up. The problem was the lack of documentation: IPv6 is managed on the modem... but nobody knows how to control it.

Once the right parameters were obtained, all of our modems began to send requests to obtain IPv6 connectivity. With the help of a dhcp6-relay on our CMTS, we reroute these requests to our provisioning servers. But nothing happens. It turns out that, even though it was changed only a few months ago, our provisioning software solution cannot manage IPv6 (or only in a very messy way) and its publisher does not seem terribly concerned about it.

“We were therefore able to offset our IS’s deficiencies with open source software, and divert our DHCPv6 requests to it. The solution is stable and transparent.”

So the idea came to me... to simply install a well-known open source (ISC) DHCPv6 server. A few lines of code later, our CMTS returns the requests to this little server, and it works! The modems all take a /56 block for home equipment, and 3 IPv6 /128 (the provisioning stack, MTA/SIP and WAN) in barely a few minutes, and traffic surges in no time. The entire base was switched over in a matter of minutes! We were therefore able to offset our IS’s deficiencies with open

source software, and divert our DHCPv6 requests to it. The solution is stable and transparent.

The effect on our clientele was apparent the next day: our customers who are the most demand in terms of QoS confirmed the fluidity and stability of the connections. At the same time, subscriptions are increasing.

On the tech support side of things, there were far fewer calls and e-mails, which allowed our technicians, at last, to resolve a cable network’s issues efficiently and with precision. Before, it was hard to know if the failures were coming from a router that cut off the session, or from the trundling cable modem, despite excellent values at the end of the line. Our agents in charge also have IPv6 to reach any modem without a single proxy or NAT. It is now the firewalls that govern the security that the old private IPv4 ranges provided, as much inside each of our subscriber’s homes, as on our operator’s network.

OrneTHD achieved its IPv6 deployment with all of its consumer and business subscribers. We hope that other, similar deployments will follow.

1. See lexicon.

2. See lexicon.

3. CO-CONSTRUCTION WITH THE ECOSYSTEM TO ACCELERATE THE TRANSITION TO IPv6

3.1. IPv6 Workshop

On 10 October of last year, Arcep hosted a workshop in partnership with Internet Society France, dedicated to experience and best practices for the transition to IPv6 sharing. Targeting the ecosystem's stakeholders – ISPs, hosting services, academia, public sector bodies, businesses, etc. – the workshop was part of the Internet Governance Forum (IGF), organised around one central event and several workshops (GDPR, cybersecurity, IPv6, etc.).

Thanks to an original format – midway between a multilateral meeting and a conference – the IPv6 workshop resulted in multi-stakeholder working groups, who discussed a range of concrete topics related to the transition from IPv4 to IPv6. This event was structured around two sessions of three parallel workshops:

- The first session explored the transition to IPv6 from the different stakeholders' perspective²: ISPs and device manufacturers, hosting companies as well as public bodies and enterprises. The workshops provided an opportunity to identify each type of player's specific challenges, as well as the courses of action to take to prevent or resolve these issues.
- The second session offered a chance to deal with more cross-cutting issues that are intrinsically linked to the transition to IPv6: IPv6 quality of service and security, IPv6 training and preparing for the end of IPv4. Discussions served to highlight those problems shared by every link along the technical chain, as well as the possible solutions.



3.2. Workshop findings¹¹

The findings of these workshops are summarised in the following table¹²:

Main issues at stake	Courses of action emerging in the ecosystem
<ul style="list-style-type: none"> - Operational problems tied to CGN, or to non-compatible websites, applications and connected objects; - Lack of short-term profitability for IPv6 and lack of clarity on longer-term Rol (the cost of transition vs. do not transition unclear); - Lack of staff training and IPv6 support skills; - Lack of interest in IPv6 and weak demand from customers; - Quality of service issues tied to traffic degradation on some hardware, and IPv6 interconnection problems; - Lack of knowledge about IPv6 security and low maturity of technical solutions; - Lack of feedback and perspective on the transition to IPv6; - Dual-Stack¹³ maintenance complexity. 	<ul style="list-style-type: none"> - Create an IPv6 Task Force and an online platform to enable an ongoing dialogue on stakeholders' experience in deploying IPv6, and the problems that arise; - Promote players who offer IPv6 (e.g.; via Arcep's IPv6 barometer) and encourage players to communicate with consumers about their IPv6 solutions (ISPs' obligation to inform end users of fixed IPv6 and IPv4/v6-readiness and the presence of CGN); - Run awareness campaigns aimed at the Internet ecosystem's stakeholders, and at information system managers and management boards, to include IPv6 in calls to tender; - Improve available IPv6 training courses and issue recommendations on IPv6 architectures and deployments; - Set a national timetable for the transition: national transition roadmap and strategy; - Create an IPv6-ready approval logo for equipment and devices to guarantee they are IPv6 compatible and operate properly, and standardise a set of IPv6 indicators to be able to track the progress of the protocol's deployment, and assess the impact of IPv6 on quality of service; - Establish a Code of conduct, limiting IPv4 address sharing to the CGN level; - Create incentives to encourage players to choose IPv6; - Issue common recommendations/plan coercive measures to accelerate the transition to IPv6.

3.3. Workshop follow-up: creation of an IPv6 Task Force and an online platform

Following through on the IPv6 workshop, Arcep decided to create an IPv6 Task Force, steered jointly by the Internet Society, whose members include any interested parties (operators, hosting companies, businesses, public sector, etc.). The goals: to give participants an opportunity to address specific issues and share best practices to accelerate the transition to IPv6.

The Task Force will meet twice a year, starting in the second half of 2019. People who have experiences to share, or who are planning on deploying IPv6 are invited to make their interest know to Arcep, by completing the following form: www.arcep.fr/IPv6_Form. Alongside these biannual meetings, Arcep and the Internet Society are studying the creation of an online platform that would allow an ongoing dialogue between the different stakeholders, which would help fuel the work being done by the Task Force.

The priorities of the actions to be implemented will be set in concert with all of the Task Force participants.

11. https://www.arcep.fr/uploads/tx_gspublication/compte_rendu-atelier-IPv6-fev2019.pdf

12. This summary does not constitute Arcep's position on the actions' relevance, feasibility or priority. It only describes the information provided by the ecosystem's different players who participated in the workshops. Arcep may work in concert with the community of participants on prioritising the actions to be taken.

13. Dual stack IP: consists of assigning network equipment an IPv4 address an IPv6 address.

OPEN FLOOR TO ...



Franck Pflieger, president of IPv6 Council Martinique, manager of GALACTUS Technologie and founder of the ASPIK association

IPv6 in Antilles-Guiana: a key ingredient in the digital transformation, propelling economic growth

IPv6 is a way to guarantee that innovation on the Internet will thrive. It is thus a vital ingredient in a new economic boom.

IPv6 is also an essential building block for the Internet of Things (IoT), which is the basis of industries', enterprises' and government services' digital transformation.

For more than 15 years, GALACTUS Technologie has been hosting workshops on issues surrounding avant-garde technologies like IPv6, in Antilles Guiana. One outcome of these meetings was the creation of ASPIK, which is an industry association with more than 40 members (telecoms carriers, manufacturers and service providers). Active in the departments of Martinique, Guadeloupe and Guiana, the association's aim is threefold:

- to foster the sharing of expertise in areas such as cybersecurity, the digital transformation, and any profession tied to technological innovations in the Caribbean;
- develop cooperation amongst ICT stakeholders in the Caribbean;
- and to promote women working in the tech sector.

In June 2016, ASPIK hosted the first IPv6 event in Martinique. It was real milestone as the seminar, the different participants, fixed and mobile operators and service providers

“Saint-Barthélemy has been among the Top 5 countries where IPv6 is the most widely deployed; Saint-Martin is in the Top 30.”

all have concrete objectives when it comes to developing IPv6 technology within their company.

In addition, IPv6 Forum has welcomed Martinique since 2016, which is when the IPv6 Council Martinique was formed. IPv6 Forum's goal: to promote the deployment and adoption of the new Internet with the help of IPv6.

To quote Latif Ladid, the President of IPv6 Forum, «IPv6 Council Martinique was created to build a vocal Internet community. It will work to promote equal access to knowledge and education on new generation Internet technologies, and spur the IPv6 deployment momentum».

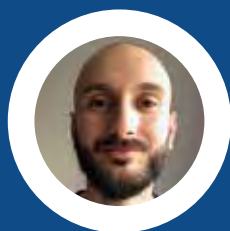
These initiatives are paying off. For several months, Saint-Barthélemy – and especially on the Akamai site¹ – has been among the Top 5 countries where IPv6 is the most widely deployed; Saint-Martin is in the Top 30... Sweet revenge on hurricane IRMA!

To further accelerate the pace of the transition to IPv6 in the region, there will be a workshop² dedicated to IPv6 in Guadeloupe from 18 to 22 November 2019, with Arcep and Internet Society France teams in attendance.

1. <https://www.akamai.com/us/en/resources/our-thinking/state-of-the-internet-report/state-of-the-internet-ipv6-adoption-visualization.jsp>

2. https://galactus.fr/ipv6_event/

OPEN FLOOR TO ...



François Contat, Head of the network and protocols security lab, ANSSI
Arnaud Ebalard, Expert at the network and protocols security lab, ANSSI

IPv6: a paradigm shift that users need to understand and prepare for

IS THE TRANSITION TO IPv6 INEVITABLE?

Yes. And in fact most of the major Internet players are now fully IPv6-compatible. IPv6 has managed to last this long thanks to stopgap measures that are reaching their limits. The growing prominence of connected objects, and the dearth of IPv4 addresses are driving the imperative to take IPv6 on board quickly, and to contribute to its adoption.

WHAT DOES IPv6 ACTUALLY CHANGE FOR CITIZENS' RESIDENTIAL INTERNET ACCESS?

For end users, the advent of IPv6 on their residential connection constitutes a paradigm shift, which must absolutely be understood and prepared for. Up until now, the technical solutions used to limit the exhaustion of IPv4 addresses, such as network address translation (NAT), made it hard to access connected equipment from outside the home. When IPv6 is enabled, addresses that are accessible from the Internet are supplied automatically, to every piece of networked equipment (TV, camera, smart light bulb or switch, game console, etc.), which exposes them to the outside world. If the operator and the user do not take any special precautions, the private IPv4 home network becomes a place that is exposed to the public in IPv6.

WHAT ARE THE CHANGES FOR A COMPANY OR AN ISP?

Large companies will reap greater benefits from the transition to IPv6. They need to work with a limited private IP address space. This aspect of private IPv4, along with the associated circumvention measures (notably NAT) carry substantial human and hardware costs, particularly when upgrading the network, incorporating new subsidiaries, etc. The advent of virtually unlimited unique local areas (ULA) with IPv6 constitutes a tool that makes it possible to maintain a stable, and especially scalable, internal infrastructure.

For ISPs, the transition from their network to IPv6 is already complete. The main challenge they are facing today is the temporary technical measures that were put into place – such as large-scale carrier-grade NAT (CG-NAT) – whose purpose was to allow IPv4 customers to continue to grow despite the actual dearth of public addresses. Another important aspect is the fact of maintaining transitional mechanisms between the two versions of the protocol for a long time. From a security standpoint, customers will need their operator to shepherd them through this paradigm shift, to avoid suffering the effects of opening residential networks and increasing the number of unsupervised equipment. And this at a time of never ending Denial of Service (DoS) attacks, for which these equipment can be used as an attack vector.

DOES IPv6 IMPROVE THE INTERNET?

IPv6 was designed to erase IPv4's visible defects (limited addressing space, aspects tied to fragmentation, size of the routing tables, etc.) and should therefore help support the internet's growth. The IPv6 routing table, for instance, is currently ten times smaller than the IPv4 table. Among other things, the need for address translation becomes marginal with IPv6, and makes it possible to lighten resource consumption on the equipment and infrastructure that use them, such as mobile networks. Ultimately, the growing number of equipment on the networks, and the ease in accessing them that IPv6 provides, constitute major security challenges that are tied to the protocol's deployment, all the more so when a sizeable portion of this new equipment is not supervised. So, even if scans become more complicated to implement for those attacking IPv6 networks, due to the expanded addressing space or address randomisation mechanisms, it may not be enough to fully protect the network.

WHAT POINTS REQUIRE SPECIAL ATTENTION WHEN MAKING THE TRANSITION TO IPv6?

When switching over to IPv6, protection systems (firewall, IDS) and network, service and equipment monitoring (syslog, SNMP, etc.) mechanisms put into place previously for IPv4 will need to be adapted. The protocol's specificities will also need to be taken into account. For local networks on which an administrator deployed DHCP snooping or anti-spoofing mechanisms, for instance, a dedicated solution must be implemented.



Ensuring internet openness

4.
GUARANTEEING
NET NEUTRALITY

5.
FOSTERING THE OPENNESS
OF DEVICES

Guaranteeing net neutrality



“The patient is in good health, but must stick to its regimen to avoid a relapse”

56,000
tests have been performed to date in France using the Wehe app



The European legislator has been protecting net neutrality since 2016, by recognising the following points in particular in its Open Internet¹ regulation:

- users' right “to access and distribute information and content, use and provide applications and services, and use terminal equipment of their choice, irrespective of the end-user's or provider's location or the location, origin or destination of the information, content, application or service, via their internet access service”;
- and internet service providers' duty to “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”.

In France, Arcep is the body responsible for implementing net neutrality and ensuring that internet service providers (ISPs) comply with it.

1. ARCEP'S COMMITMENT AT THE EUROPEAN LEVEL

In 2018, an assessment of the application of Open Internet regulation No. 2015/2120, and the implementation of BEREC guidelines for national regulatory authorities (NRA) on monitoring the regulation's application was completed. This evaluation, whose publication was made possible by constant cooperation between NRAs, drew on the contributions to a consultation with the sectors' stakeholders. It was also the subject of a BEREC opinion for the European Commission, published in December 2018². This opinion delivers an assessment of net neutrality's application in Europe, and identifies a list of possible changes to the current legislative framework. The goal is to minimise the risk of having divergent interpretations of the current legislation by stakeholders involved in the internet's operation in France and Europe. Arcep is an active contributor to

the discussions within BEREC on the possible clarifications to be brought to the Open Internet regulation guidelines.

One key point for Arcep and the other NRAs concerns the application of net neutrality rules to zero-rating offers³. The zero-rating offers found in the different Member States apply chiefly to music, online video and popular social media applications or categories of application. These practices are not prohibited by the European regulation, per se, but they can lead to discriminatory behaviour that benefits certain applications or categories of application. Being able to use an application for free (and not have the traffic it generates deducted from one's data allowance) creates an economic incentive to use that app, which could well be to the detriment of competing applications. It would therefore seem advisable to clarify the methods that NRAs use to assess these offers, and the impact they have on the market and on end users' rights. Zero-rating is in fact being investigated for the first time by the Court of Justice of the European Union (CJEU), following the prejudicial issues raised by the Hungarian court. The Court's response to these questions will help clarify the assessment methodology for zero-rating offers set out in the guidelines.

BEREC's opinion also addresses the question of differentiating quality of service classes. The guidelines allow ISPs to provide several distinct internet access plans that are tiered by technical properties such as data allowance and connection speed, under certain conditions. Arcep is keeping a close watch over this issue, to be able to foster innovation on the networks without running the risk of creating a two-speed internet.

1. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R2120&from=EN>

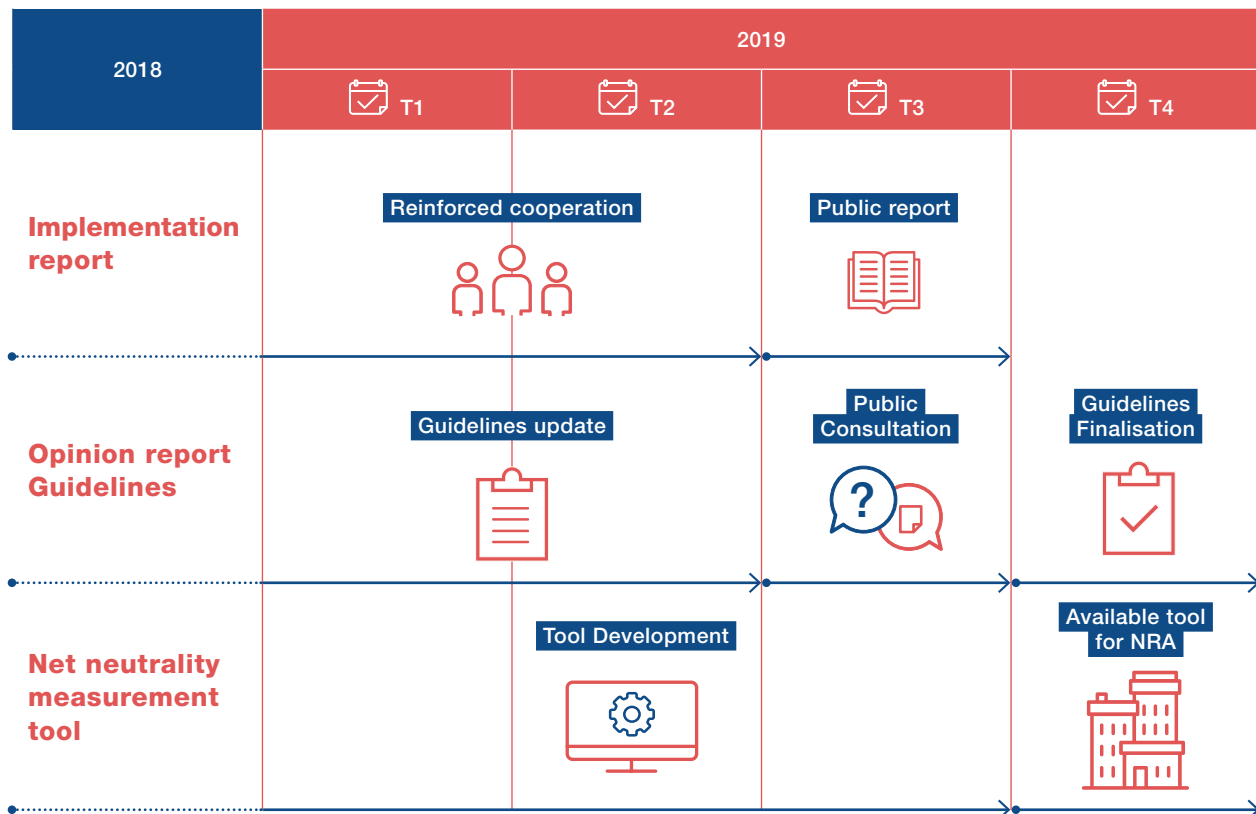
2. BEREC opinion of 6 December 2018 on the evaluation of the application of European regulation No. 2015/2120 and BEREC net neutrality guidelines: https://berec.europa.eu/eng/document_register/subject_matter/berec/opinions/8317-berec-opinion-for-the-evaluation-of-the-application-of-regulation-eu-20152120-and-the-berec-net-neutrality-guidelines

3. See lexicon

Lastly, BEREC’s evaluation looks at reconciling net neutrality and the technological advancements brought by 5G. The sector’s players have regularly raised the question of how compatible net neutrality is with the advent of 5G. In its opinion, BEREC concludes that the Open Internet regulation is technologically neutral, and therefore applies without consequence to 5G technology, in the

same way it applies to earlier 2G, 3G and 4G technologies. It notes that the regulation “seems to be leaving considerable room for the implementation of 5G technologies, such as network slicing, 5QI and Mobile Edge Computing.” And states that it is not aware of any concrete example where the implementation of 5G technology would be impeded by the Open Internet regulation.

BEREC NET NEUTRALITY WORK PROGRAMME



2. WORK IN PROGRESS

2.1. A new diagnostic tool

Following through on what was announced in the 2018 report on the state of the internet in France, Arcep committed to improving the ability to detect online practices by supporting the development of a tool that was the fruit of university research, and capable of detecting traffic management practices. Difficult to implement from a technical standpoint, this feature has been absent up until now from the other tools that are available in the marketplace.

This new tool is called Wehe. It was developed by Northeastern University and can be accessed by any consumer through an Android or iOS application. The testing tool compares the time it takes for traffic generated by certain services to be relayed. It measures the difference between the traffic stream’s actual travel time through the network layers and the travel time for a similar but encrypted traffic stream. If the results for a given source are significantly different in a repeated and matching fashion, and the problem is not situational but rather structural, it is possible to suspect that the operator has implemented measures that affect traffic. Users can then decide to inform Arcep, which will be in position to investigate these reports. This new distributed tool is part of Arcep’s crowdsourcing initiatives. They are designed to empower consumers, making each and every one an integral participant in the regulatory process, with the ability to contribute to the evidence that triggers the Authority’s actions.

OPEN FLOOR TO ...



Dave Choffnes, Assistant professor, Northeastern University

Wehe: the crowdsourcing-based throttling detection tool

In a constant struggle that pits business interests of network providers against those of content providers, and against the freedom of users to access Internet content without artificial restrictions, *net neutrality* has become the rallying cry to ensure a free and open Internet for generations to come.

While laws are an important step toward ensuring net neutrality, they are not enough alone. This is because regulations *without auditing* cannot be enforced. Traditionally, regulators and average users have lacked scientifically sound, independently developed tools to reliably detect such net neutrality violations, meaning existing laws lacked teeth and users lacked transparency about their network provider's policies. With the Wehe project, and our partnership with Arcep, we aim to fill this void by providing software that any user can run to detect net neutrality violations, and regularly updated dashboards where users and regulators can view statistics and other data concerning net neutrality violations worldwide.

Our Wehe app has been installed by more than 125,000 users worldwide. Since January, 2018 Wehe users collectively have run more than 1,000,000 net neutrality tests in more than 2,700 networks in 183 countries. We officially launched our product in France in November, 2018. To date, French residents have run more than 56,000 tests, second in number only to the United States. We regularly update our findings globally at <https://dd.meddle.mobi/globalStats.html> and for France at <https://dd.meddle.mobi/StatsFrance.html>.

SUMMARY OF FINDINGS

As of January 26, 2019, Wehe detected throttling or blocking in 30 ISPs in 7 countries. Nearly all cases of detected throttling affect video streaming services, with YouTube being throttled the most often (25 cases), and Vimeo being throttled the least (3 cases). Wehe detected throttling of Skype video tests in only two ISPs, both in the US: Sprint and Boost Mobile (which is also owned by Sprint). Wehe *did not* detect any ISP throttling of Spotify tests.

“Wehe did not detect any throttling in France.”

The most common detected throttling rate is 1.5 Mbps (12 cases). These rates typically correspond to ISPs that disclose data plans offering low-resolution video streaming.

For the vast majority of networks tested via WiFi (which are commonly connected to a fixed-line access technology such as cable, DSL, or fiber), Wehe did not detect differentiation.

Nearly all *detected throttling* occurred in cellular networks, and the vast majority of these cases came from ISPs in the US, where net neutrality violations are legal (at the time of writing).¹

Wehe did not detect any throttling in France. This indicates that French ISPs are compliant with local net neutrality regulations, at least when it comes to content-based differentiation for popular apps.

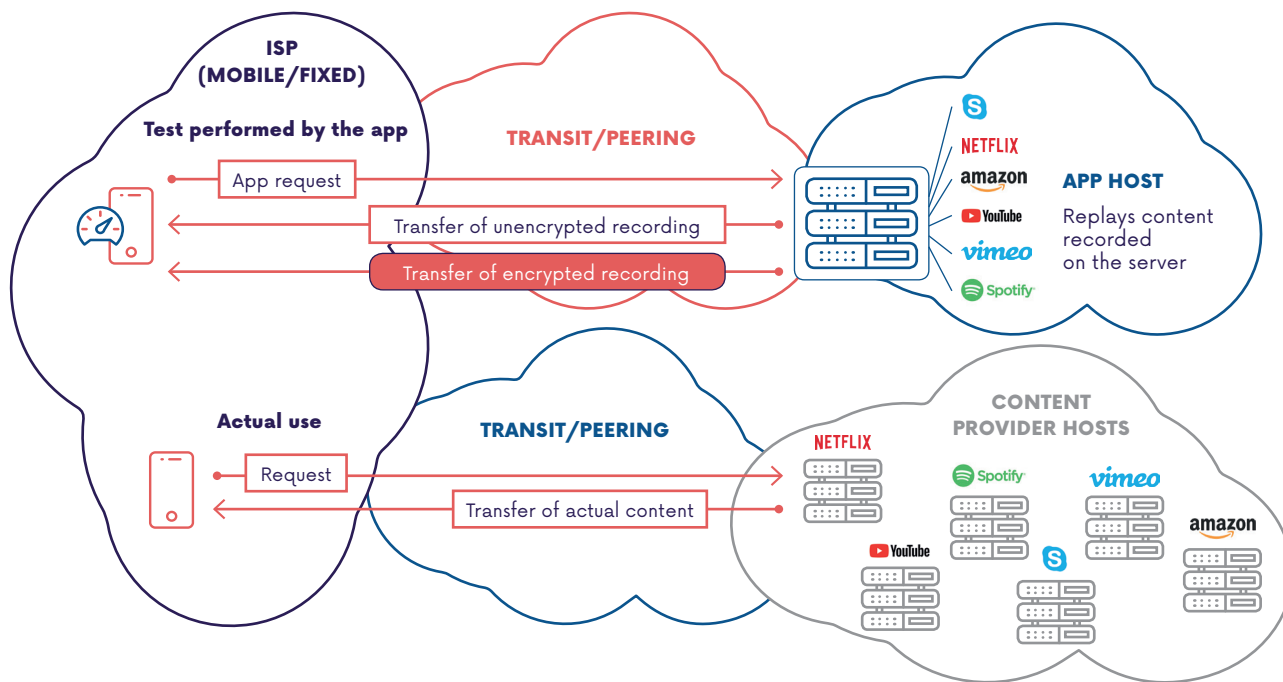
Wehe also detected a phenomenon called delayed throttling, where an ISP (T-Mobile US in this case) gives unthrottled bandwidth to an application for the first few megabytes of the data transfer, then throttles the rest of the connection. While this may improve video startup delays when streaming video, we also found it led to inefficiency later in the transfer because the ISP dropped substantial amounts of data once throttling started.

FUTURE OF WEHE

Work on the Wehe project continues. We are expanding our infrastructure to provide more global reach, adding more apps to test for content differentiation, and conducting research to better understand the impact of net neutrality violations on application performance metrics (e.g., video streaming performance). We are also seeking collaborations with additional regulators in other jurisdictions, building upon our successful work with Arcep.

1. The rules governing net neutrality in the US have changed considerably over the past few years, and may change again due to legislative action pending in Congress.

HOW THE WEHE APP WORKS



Source: Arcep

In concrete terms, the partnership between Northeastern University and Arcep resulted in major progress being made on the tool's main building blocks: increasing the accuracy of the detection of false positives, developing the automatic detection of Deep Packet Inspection (DPI) rules when throttling is detected, ability to report positive tests to Arcep through a «J'alerte l'Arcep» button, creation of an online dashboard for monitoring tests in France, diversification of the servers that host the application (notably with

two server in France, hosted by Arcep and by K-net, to whom we extend our thanks), redesign the application for Android and iOS, translating the interface into French, etc.

As yet, none of the results provided by the application have made it possible to suspect that any traffic management practices that violate net neutrality rules have been found on the traffic streams observed in France.

2.2. Paving the way for 5G

Arcep is responsible for enforcing net neutrality in France. It is also in charge of overseeing the development and deployment of 5G nationwide. Some believe that 5G and net neutrality are incompatible. But is that really the case? To challenge certain assumptions, Arcep summarised the different sides of the debate in an ad hoc document⁴.

Arcep also hosted a dedicated workshop on the issue, as part of the Internet Governance Forum in November 2018 in Paris.

Lastly, Arcep a contributed to the work that BEREC did on this topic that concluded, among other things, that the Open Internet regulation leaves considerable room for the implementation of 5G technologies such as network slicing and mobile edge computing.

4. https://www.arcep.fr/uploads/tx_gspublication/ARCEP_BD_5G_nov2018.pdf

5G AND NET NEUTRALITY DU NET, FRIENDS OR FOES?

Some believe that 5G and net neutrality are incompatible. But is that really the case? To challenge certain assumptions, Arcep summarised the different sides of the debate in an ad hoc document.



5G AND NET NEUTRALITY,
FRIENDS OR FOES ?



Arcep, French regulator of telecoms, is responsible for both net neutrality and the spread of 5G.
Arcep is dedicated to a pro-innovation regulation: ensure permission-less innovation thanks to net neutrality, and promote innovative services thanks to 5G.
But some say they are not compatible.

THE PROMISES OF 5G, THE NEXT GENERATION OF MOBILE NETWORK

Capacity



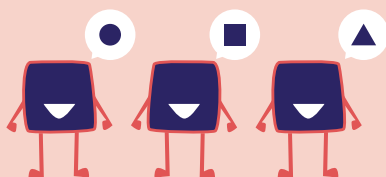
5G will deliver unparalleled speeds for increasingly bandwidth-hungry applications.

Instantaneousness



5G will reduce latency for real-time services.

Specialisation



5G will make it possible to tailor traffic streams' properties to certain applications.

Virtualisation



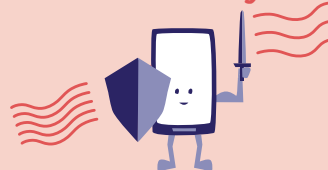
5G will rely more heavily on software-defined networking to deliver more features.

Energy efficiency



5G will make it possible to adjust transmissions to the objects' needs, which can also increase their lifespan.

Reliability



5G will provide greater security for certain data streams, notably on public networks.

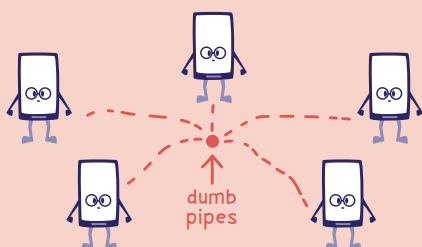
WHAT DOES THE REGULATOR DO?

- It encourages innovation and investment in the sector;
- It authorises trials and delivers frequency licences, which carry obligations.

NET NEUTRALITY :

ENSURING NON-DISCRIMINATION ON THE INTERNET

The Internet's core values



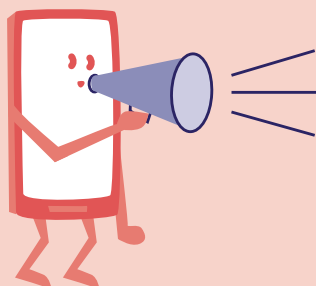
Net neutrality compliance with the end-to-end principle, with the understanding that intelligence is located on the network's edge, with no central control.

User rights



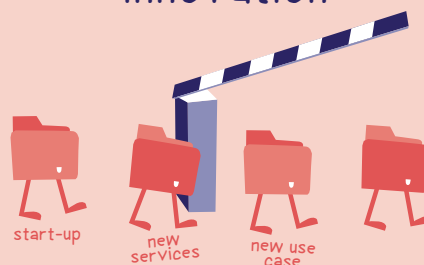
Net neutrality guarantees that every user can access any online content or service using the device of their choice.

Freedom of expression and information



Net neutrality guarantees users' freedoms, with due consideration to others.

Permissionless innovation




Net neutrality allows content providers to offer their online services without ISPs acting as gatekeepers.

WHAT DOES THE REGULATOR DO?

- It enforces net neutrality rules and imposes penalties on those that breach it;
- It co-develops diagnostic tools: reporting platforms, apps for detecting traffic throttling, etc.

INNOVATION AND NON-DISCRIMINATION IN PRACTICE :

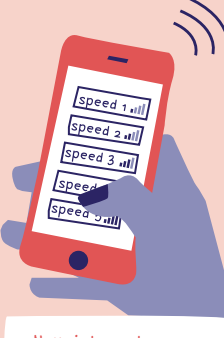
5G opens the way for
innovative applications...



Remote surgery, via ultra-reliable real time virtual reality



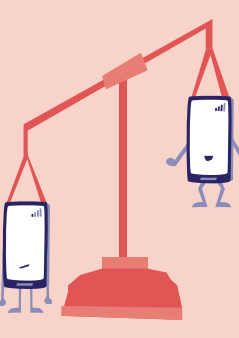
Smart farming, its drones and ground-based sensors



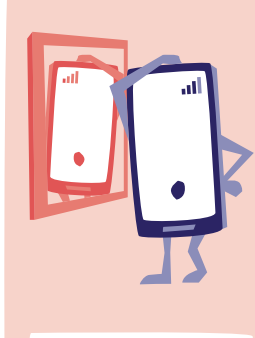
New internet access services with plans tiered by quality, allowing users to choose the speed that matches their needs

⊕
and many more use cases

... and new cooperations to design



How to provide different QoS levels without discriminating?



How to be transparent with customers on the different achievable connection speeds?



How to optimise the transmission of certain services without harming the overall quality of internet access?

⊕
and many more questions

WHO SAID WHAT ?

Dividing lines,
in a selection of quotes:

BEREC

(Body of European Regulators for Electronic Communications)

BEREC considers that the Regulation leaves considerable room for the implementation of 5G technologies, such as network slicing, 5QI and Mobile Edge Computing. To date, BEREC is not aware of any concrete example where the implementation of 5G technology as such would be impeded by the Regulation.

FCC

(American Regulator)

An other negative consumer impact from the [previous] FCC's heavy-handed regulations [on net neutrality] has been less innovation. We shifted from a wildly successful framework of permission-less innovation to a mother-may-I approach that has had a chilling effect.

GSMA (GSM Association) and ETNO

(European Telecommunications Network Operators)

The EU and Member States must reconcile the need for Open Internet with pragmatic rules that foster innovation. The telecom industry warns that the current Net Neutrality guidelines, as put forward by BEREC, create significant uncertainties around 5G return on investment.

EDRI

(European Digital Rights)

We are deeply concerned that the ongoing technological standardisation of new telecommunications technologies [5G, NFV, SDN] may undermine the current net neutrality protections in the European Union (EU).

TRAI (Indian Regulator)

Network performance optimization aligned to net neutrality concepts offers a blueprint for how IoT devices and its communication capabilities should be planned, architected, and deployed to minimize burden on the network, by being proactive about improving the efficiency and speed of their data, and also pose it as a source of competitive advantages.

OPEN FLOOR TO ...



Pieter Nooren, senior scientist, TNO

5G & Net neutrality - A functional analysis to feed the policy discussion

TNO¹ has made an independent study² into 5G and net neutrality to provide a factual underpinning for the policy debate on this topic. The main outcome is an analytical framework that helps to structure the discussions between policy makers, regulators and mobile operators. The starting point for the study are three use cases that introduce challenging requirements for the connectivity to be delivered by 5G. The use cases are taken from Virtual Reality in media and entertainment, Critical Communications in public safety and Automated Driving. Together, the three use cases present different combinations of challenging requirements for 5G networks: short delays (latencies), high bandwidth and high reliability of the connectivity.

5G BUILDS ON NEW AND EXISTING TECHNOLOGY INGREDIENTS

5G aims for the support of higher data rates, larger network capacities and a (much) higher number of devices than 4G. Another important goal is to introduce the technical capability for mobile operators to provide tailored connectivity to specific sectors, user groups and applications. This is reflected in key 5G technology ingredients, such as network slicing, local access to data networks, edge computing and QoS differentiation.

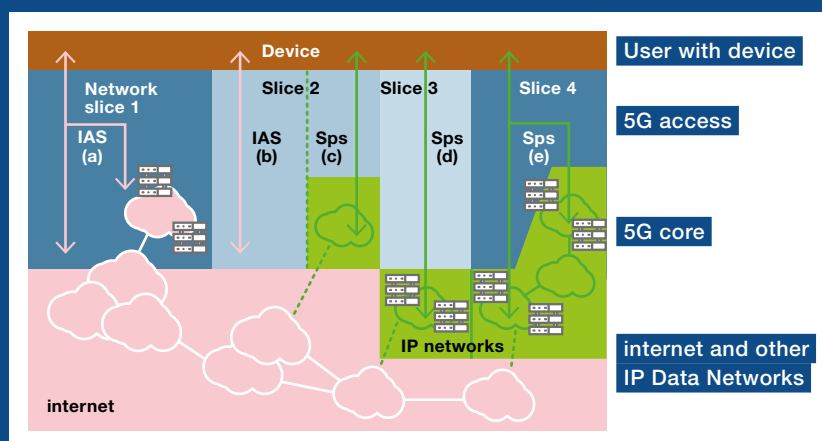
OUR ANALYSIS UNDERLINES THE IMPORTANCE OF TECHNOLOGICAL NEUTRALITY

Technological neutrality is a well-established principle that is adhered to in the Regulation and the Guidelines that lay down the rules for net neutrality. What matters for the compliance

with these rules is how the 5G technologies are used to support services and applications, rather than the technologies themselves. Therefore, the European net neutrality rules do not introduce a ban on any 5G technology ingredient, also not on the technologies that are being developed with the aim to differentiate between traffic flows and applications.

The central question in the assessment of the compliance with net neutrality rules is whether the services and applications supported by the 5G technology components adhere to the conditions and rules for Internet Access Services and Specialised Services, whichever are applicable. It is these conditions and rules that determine the room for mobile operators and content and application providers (including those from vertical sectors) in their use of 5G technology. In our analysis, network slicing provides a relevant illustration of this point. The use of slicing will vary, as illustrated in the 5G architecture figure below.

In 5G architectures that use slicing, an Internet Access Service is always in a slice. A slice can be used exclusively to provide an Internet Access Service (slice 1), a Specialised Service (slices 3 and 4) or both (slice 2). Thus, the use of slicing technology in a mobile operator network can bring in the rules for Internet Access Service, for Specialised Services or both, depending on the services and applications that are supported. It is not possible to come to an overall assessment with a single outcome on the alignment of slicing with net neutrality rules. This is because the topics that are encountered in the assessment and the outcome depend not only on the 5G technology, but also on the specific combination of services, applications and network architecture. This is true for network slicing, but also for other key 5G technologies such as QoS differentiation. A consequence is that mobile operators, content and application providers and national regulatory authorities will need to do further analysis to evaluate whether a particular type of (tailored) connectivity complies with the net neutrality rules.



1. <https://www.tno.nl/en/about-tno/organisation/>

2. 5G and Net Neutrality: a functional analysis to feed the policy discussion, P.A. Nooren, N.W. Keesmaat, A.H. van den Ende, A.H.J. Norp, TNO 2018 R10394, 13 April 2018.

3. ANALYSING OBSERVED PRACTICES

In response to the practices that were identified last year, Arcep focused first on freedom of choice and device use in ISPs' mobile plans. Several potential restrictions had been identified since 2017, and particularly the inability to tether (either completely prohibited or data capped), and the inability to use certain categories of device with certain internet access plans.

After Arcep took action, operators removed the clauses that limited the use of tethering and prohibited the use of SIM cards in other mobile devices. Arcep continues to monitor the situation very closely.

In early 2018, following a number of public requests and numerous user reports posted to the "J'alerte l'Arcep" platform, Arcep wanted to obtain additional information on the reasons for the poor quality of certain consumer service on ISP Free's network. These recurring speed and accessibility issues appear to affect several popular online services, starting with Netflix. In light of the elements gathered by the competent Arcep body early in the year, it did appear that the Free network's interconnection with the rest of the internet could be one of the reasons. Unlike other major ISPs, Free's access to the bulk of global traffic relies heavily on a single transit provider, some of whose links are saturated on a very regular basis. As a result, although it cannot be called a traffic management issue, the most bandwidth-hungry services, such as video streaming, could encounter quality issues when the links were saturated, regardless of the end user's advertised speed. The quality of service that customers actually experience depends on all of the parties involved along the technical chain, between the end users and the content she consumes (ISP, transit providers, content providers, etc.). The media in fact picked up on the direct interconnection between Free and Netflix, in spring 2018. Today, Arcep has noted a decline in the reports it is receiving from users, which is a sign that the situation has improved. As stated in Chapter 2, interconnection methods between the different stakeholders do vary (transit but also direction relationships such as free or paid peering) and are designed to meet different needs.

Arcep also focused its attention on the in-flight Wi-Fi services that airlines offer. This interaction provided Arcep with an opportunity to issue a reminder that the regulation applies not only to traditional ISPs' products, but also to this type of access product that Arcep considers "publicly available". Because in-flight Wi-Fi service is transnational by nature, on Arcep's initiative, the issue was also addressed in the work being done by several BEREC expert working groups. They confirmed that this type of service can be defined as being publicly available, and therefore subject to the provisions of Europe's Open Internet regulation.

Finally, in response to several reports made through the "J'alerte l'Arcep" platform, Arcep departments examined the matter of port blocking. Because online services and apps are accessed through a port, blocking that port will prevent access to said service or app. This restriction on access is a practice that could be incompatible with the Open Internet regulation if it cannot be justified by one of the exceptions stipulated in the regulation.

Arcep has made a script available to end users to enable them to check whether a TCP port's output is operational, blocked or available but throttled. The script is available here: <https://github.com/ARCEP-dev/disPorts>

The purpose is to better inform users on port blocking implemented by their ISP, and to further Arcep's investigations into this issue.

FYI

WHICH "PORTS" ARE USED DURING A CONNECTION?

TCP and UDP are the two main protocols used on the internet to transport traffic over IP. Every internet connection generated by an application is associated with a UDP or TCP session that is identified with a "port number". This means that at each end of a TCP connection (transmitting or receiving) a 16-bit port number (from 1 to 65535) is assigned to the sender or receiver application, referred to, respectively, as the source and destination ports.

If the source ports are usually chosen in a random fashion, on a server handling multiple applications it is the destination ports that ensure the streams are routed to the right application. They are therefore relatively standardised.

To guarantee that a service is accessible, the corresponding port must be "open", in other words the equipment involved in relaying the traffic must not block the routing of the network packets associated with this port. Any blocking or throttling on this port could therefore affect the service in question.

OPEN FLOOR TO ...



Benjamin Bayart and Oriane Piquer-Louis,
Co-presidents of the French Data Network (FDN) Federation

Net neutrality as a personal freedom

The European texts that protect net neutrality define it as giving end users the freedom to do a number of things: access and distribute content, use and provide applications, etc. Ensuring this freedom means prohibiting technical intermediaries, and particularly network operators, from impeding its exercise. And somewhat curiously, the protector of this freedom is the sector's economic regulator.

The most widely understood aspect of this issue today is the one that involves the business squabbles between the network's economic stakeholders: ISPs that want to favour their video sales platform over others, or their own sales and advertising contracts, at the expense of the free market and competition, and so at the expense of citizens' freedom to access the content of their choice. Although national regulators have successfully analysed this aspect, protecting users' freedoms still leaves something to be desired (zero rating is still tolerated in far too many cases).

Another aspect that is still completely overlooked: the right to a symmetric connection. This symmetry is, literally, in every word that European legislators use to describe net neutrality. Every word that puts internet users in a (let's say, consumer) situation has its (ergo, producer) counterpart. The intention is clear: not only freedom of choice over what we consume but also, and especially, as an internet user, the right to provide everything that can be provided.

The wording does not say that internet users can subscribe to whatever plan they want, and that Netflix has the right to distribute whatever plans it wants. The wording is clear: internet users have the right to distribute.

This is not a right that is limited to certain economic stakeholders. It is a basic, protected right of every European citizen, which is the logical corollary of fundamental freedoms in Europe.

This key element – namely, the symmetry in the relationship to the network – is still compromised far too often, however. One need only offer a quick parallel with other networks to fully gauge and understand the problem.

“Net neutrality thus ensures the freedom to access but also to distribute, which is intrinsically symmetric.”

First example: addressing. Without a fixed, public IP address, an internet connection would be like a telephone line without a phone number: we could make calls but not receive them. The limitations are obvious. Not only is this a common practice with fixed internet access, but it is the norm when it comes to mobile access. Here, the deployment of IPv6 that Arcep is helping drive forward is a step in the right direction (to provide every access line with a public address), but everybody still needs to understand that IP addresses should

be as fixed as telephone numbers are, or should be able to be.

Second example: ports and services. A great many ports are blocked at input, if not at output, by a sizeable number of operators. The oldest example is email (SMTP) ports, which are required to host a messaging server. The pretext for blocking is rather sound, in fact: a substantial number of computers run on poorly secured operating systems, and are used as botnet zombies either to flood the planet with spam or to carry out cyberattacks. It nevertheless remains that operators block ports without discernment, taking it upon themselves to decide what content their subscribers can or cannot transport. Assuming that people are incapable of doing something, we take steps to make sure of it: they are never given a chance to do otherwise. Forbidding someone to stand because you're afraid they might fall, guarantees that they will never learn to walk.

Net neutrality thus ensures the freedom to access but also to distribute, which is intrinsically symmetric. It is vital that European regulators travel a bit outside of their economic regulation shell, and take up their mantle of protector of these fundamental freedoms in the 21st century.

Some may view the call to protect these freedoms as the whim of a few overly idealistic hippies. But it is in fact the only known tool to counter the toxicity of hyper-centralised platforms whose behaviour has been so roundly condemned, but also fully enabled by our public policies.

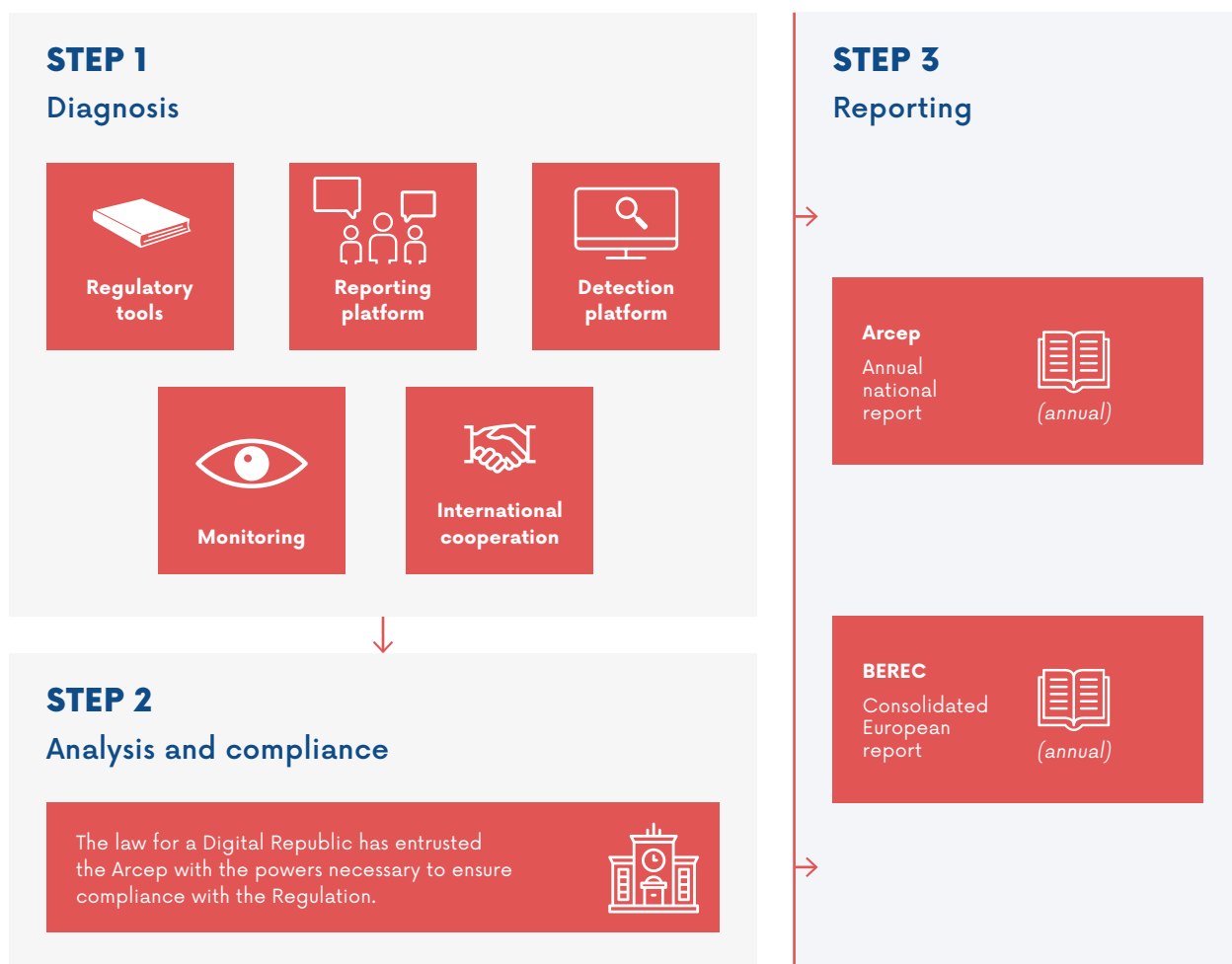
4. EUROPEAN COOPERATION FOR A COHERENT APPLICATION OF THE REGULATION

During the year gone by, European NRAs discussed their various national findings. 2018 was especially marked by the number of zero-rating offers that were reported to national regulatory authorities (in 27 of the 28 EU countries). Added to which, several NRAs reported on restrictions to end users’ freedom of choice and

usage that could be attributed to their devices. Several regulatory authorities also discussed identified port blocking practices, along with the security arguments given by the different ISPs to justify them. And, finally, NRAs shared their analyses of specialised telephony and TV over IP services.

Arcep is very gratified to be part of this Europe-wide cooperation which contributes to the consistent application of the regulations and guidelines in a way that benefits every end user (internet users and content and application providers alike).

ARCEP ROADMAP FOR ENFORCING OPEN INTERNET RULES



OPEN FLOOR TO ...



Thomas Lohninger, executive director, epicenter.works

Towards enhanced cooperation in Europe to ensure net neutrality

Two and a half years ago the European Union enacted legislation to safeguard net neutrality. The goal was to protect the open internet as an engine for innovation and ensure a European telecom single market that truly protects the rights of end-users to use and offer services irrespective of their location. To contribute to reform discussion of Europe's net neutrality framework, our NGO epicenter.works has published a report based on a complete survey of all offers with differential pricing practices in the EEA, an analysis of 800 pages of annual reports by NRAs like this one, key net neutrality decisions by regulators and economic analysis on the impact of zero-rating on the prices of mobile data volume.

The BEREC net neutrality guidelines have contributed strongly to a harmonised approach in the enforcement and supervision by NRAs. Yet, harmonisation only took place where NRAs care to assess the situation. As becomes evident in the annual enforcement reports, NRAs have widely different priorities. Even in very simple areas like the blocking of network ports – a practice which is very easy to detect and fairly straightforward to regulate – NRAs have taken different approaches which hurt cross-border service provision. Although NRAs are mandated to publish annual reports about their enforcement work, very few actually follow BEREC's criteria on which information at a minimum has to be reported. It is particularly worrisome that only eight NRAs report figures on the continued availability of internet access services at adequate quality levels.

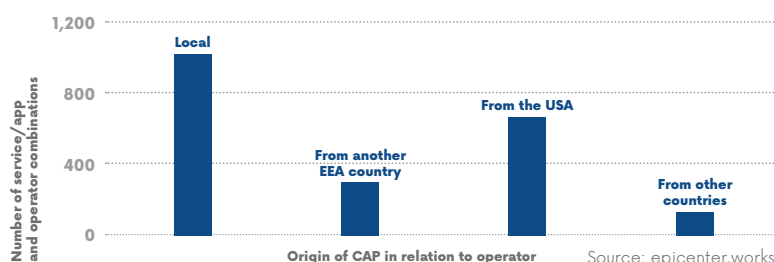
The main focus of our report¹ is differential pricing practices. Since the regulation came into force those offers have spread to all but two EU countries. We counted a total of 186 such offers in the EEA. Although the BEREC guidelines put forward a case-by-case assessment of each offer, according to the BEREC implementation reports for 2017 and 2018 only 17 NRAs have even begun formal assessments and none of them has ever decided to prohibit such a commercial practice. These assessments, for the most part, don't follow the criteria of the BEREC guidelines.

We could identify 113 such offers which fail to provide information on how the offer can be used while roaming in the EEA. 67% of differential pricing offers do not provide information for interested CAPs to join (closed offers). For those offers that did provide such information (open offers), we measured the response time to requests

of CAPs inquiring to join the program. Two answered within a day, five within a week, one within a month and 10 never came back to us. This measurement clearly shows that the fact that differential pricing practices provide contact information does not mean that they are in fact non-discriminatory about CAP participation. To our knowledge, this fact has not been assessed by NRAs at all.

In the upcoming net neutrality reform, BEREC has to ensure that the rules on commercial practices offer the guidance NRAs require to deal with these cases and also reflect the requirements the regulation bestows upon them, to intervene in cases where the rights of end-users are undermined. In this reform, Europe has not only to showcase to the world how the next mobile network standard 5G is compatible with net neutrality but also how an updated set of rules will restore consumer trust in regulators.

Geographical relationships between operators and differentially priced services and apps



1. Read the full report on the net neutrality situation in Europe and analyse the underlying data set at: <https://epicenter.works/document/1522>

5

Fostering the openness of devices



“A consensus on the diagnosis but the pathology remains challenging”



4.3 billion euros

This is the fine that the European Commission imposed on Google for abusing its dominant position in the operating systems market, by favouring its own search engine and Chrome browser.

The European Open Internet regulation enshrines users' right to access and distribute information and content online. But it applies solely to ISPs which are only one link in the internet access chain. Located at the end of this chain, smartphones, voice assistants, connected cars and other devices, along with their operating systems, have proven to be the weak link in achieving an open internet. Following through on the initial diagnosis that Arcep submitted for public debate in 2017, the year 2018 was marked by a growing awareness and commitment from institutional bodies.

1. ARCEP'S WORK

After delivering its diagnosis of the influence that devices have on internet openness, Arcep has been working to mobilise stakeholders to guarantee greater freedom of choice for users.

In February 2018, Arcep completed an analysis of devices that it began one year earlier by publishing a full report titled, “Devices, the weak link in achieving an Open Internet” – whose findings were presented at a conference on 15 February 2018. This conference provided an opportunity to challenge the entire ecosystem on the ways in which devices influence internet openness, and possible courses of action.

Arcep published two factsheets to help users handle the restrictions they might encounter when using their smartphones.

Difficulties encountered when transferring data and content to new devices, and especially when switching to a new operating system, can dissuade consumers from changing environments. This is why Arcep published a first factsheet that explains how users can keep their data when switching to a new smartphone¹.

Added to which, a smartphone's operating system will often steer users' choices, promoting certain content and services over others (apps installed by default, search engine, app store, etc.). The second factsheet was therefore designed to help users configure their smartphones to be able to take full advantage of available content and services, but also to identify any restrictions being imposed on their freedom of choice².

Arcep contributed to work being done on this issue throughout the year, notably at the *Internet Governance Forum* – a forum for dialogue under the aegis of the United Nations, which took place in November 2018 at UNESCO – by hosting a roundtable on the topic with stakeholders from civil society (Mozilla, Epicenter) and regulators from around the world (TRAI, CRTC). Arcep also continued to monitor how the market and players' practices evolved over the course of the year.

Arcep wants to pursue the work of monitoring and communicating on this issue through a collaborative device observatory, created in concert with other interested public entities.

1. <https://www.arcep.fr/demarches-et-services/consommateurs/terminaux-portabilite-donnees.html>

2. <https://www.arcep.fr/demarches-et-services/consommateurs/terminaux-personnalisation-api.html>



2. REGULATORY REVIEW

The past year marks a major regulatory milestone – laying the groundwork for the regulation of devices that Arcep had on its wishlist

Back in April 2018, the European Commission proposed its *Platform-To-Business* regulation whose purpose was to bring transparency, predictability and a level playing field to businesses whose operations depend on online platforms and search engines. The regulation stipulates that platforms, including app stores, must provide greater advance notice on any contractual changes that could have an impact on developers and, whenever their applications are suspended or removed from the app store, to give the reasons for the decision, and provide developers with a mechanism to appeal. The regulation also marks the first step towards a system of rapid resolution of disputes between developers and platforms that Arcep recommended in its February 2018 report. In addition, regarding operating systems, if the regulation does not address them, per se, it will nevertheless enable client enterprises to be informed of any differentiated treatment that the platform is likely to apply between its own services and those provided by competing companies, in terms of access to the operating system's features. A European Observatory was also set up to oversee the regulation's proper implementation. This supervision of the market is in line with what the Body of European Regulators for Electronic Communications (BEREC) recommended in its report on the impact of content and devices on the electronic communications market, which was also published in 2018. It should nonetheless be said that, although the transparency introduced by this regulation could highlight some of the issues that developers encounter, it does not provide users with the freedom of choice that "device neutrality" would.

Europe's second contribution to the issue of device openness was the DG Competition decision on the Android OS. Having ascertained that Google was abusing its dominant position in the operating systems market, to favour its own search engine and Chrome browser, the Commission fined Google for abusive practices. The company was ordered to pay a fine of €4.3 billion and put an end to these practices. As a result, Google is now required to relax the rules and allow handset suppliers to develop variants of the Android OS. It must also allow suppliers to preinstall its Play Store without having to also preinstall Chrome and Google Search. Google had announced that it would be offering this option in exchange for a licence that could cost as much as \$40 per phone. Wiko has thus been able to market an Android smartphone since April 2019 that has the Qwant search engine installed by default, instead of Google Search³. Lastly, Google will soon be required to ask its European Android users to choose the search engine and browser that will be employed by default⁴. The company Aptoide also filed a complaint against the American giant with the European Commission, accusing it of using Google Play Protect malware protection to wrongly flag its alternative app store as unsafe on Android phones. Lastly, Spotify filed a complaint with the European Commission in March 2019, this time against the Apple App Store. Spotify is accusing Apple of taking advantage of its vertical integration to favour its Apple Music service, notably by exonerating the service from having to pay the 30% tax imposed on third-party online services that sell subscriptions through the App Store.

A similar openness is being recommended by the Australian Competition and Consumer Commission which, in its preliminary "Digital Platforms Inquiry" published in December 2018, concludes that when several search engines or web browsers are available, none should be preselected by default.

3. <https://fr.wikomobile.com/shop/smartphone-view2-pro-qwant/>

4. <https://www.blog.google/around-the-globe/google-europe/supporting-choice-and-competition-europe/>

Finally, in summer 2018, application of the GDPR⁵ provided an opportunity to underscore the restrictions weighing on the choices available to users when configuring their devices, and which could, ultimately, influence the consent they give on how their personal data are used. French Deputies Eric Bothorel and Cédric Villani thus submitted an amendment that was adopted by national representatives, which made it possible to strengthen users' freedom of choice over available services and applications, particularly when first setting up their device⁶.

3. REVIEW OF MARKET PRACTICES

Despite the notable progress made since the report's publication, new practices observed in 2018 underscore the continued need for stronger regulation of devices.

Several practices observed in the operating system (OS) market illustrate the ways in which an app can be discriminated against, starting with the battery management system. To extend a device's autonomy, and limit the impact of spyware, the Android OS contains a mechanism for disabling the background activity of certain apps. Some device manufacturers went one step further by adding overlay software that selects a small number of popular apps that can continue to run in all circumstances. The remaining background apps are automatically disabled, however, as the overlay interferes with a larger number of applications than the standard Android OS does. However, when these apps are killed, users often conclude that it is because the apps themselves are malfunctioning or not well designed. This is the reason why app developers, victims of this practice, created the DontKillMyApp project which ranks mobile brands that disable background apps, and tells users how to modify their smartphone's settings when possible.

New practices from app stores have also been observed. In late 2018, for instance, the firm Kaspersky was prevented from updating its Safe Kids app (a parental control app that makes it possible to block certain applications) for iPhone. The reason given was that it needed to access Apple iPhone settings to run. Because this blocking occurred shortly after Apple had included a similar application in iOS called Screen Time, Kaspersky filed a complaint in March 2019 with Russian authorities for anticompetitive practices. Even when they can be justified for security reasons, these restrictions can have ripple effects on the diversity of the choice available to consumers. One case in point: following certain abuses, in March 2019 Google announced that it wanted to restrict access to the SMS sending functionality to only SMS apps. But this function was also employed by bodies such as the World Health Organization (WHO), which used it to relay data on the areas in Somalia that had been vaccinated for polio, as 2G coverage there was poor. App developers therefore complained about the difficulty in obtaining the appropriate case-by-case treatment for access restrictions. Some applications have, however, been able to leverage their popularity to circumvent the conditions imposed by app stores. The mobile game Fortnite is not available on the Google Play Store, for instance, which has not prevented millions of users from installing it on their Android phones since its release in 2018. Such a phenomenon is only possible on Android phones, however, as Apple does not allow apps to be downloaded from sources other than its own App Store. By the same token, even

though they are still available on the Play Store and App Store, other applications such as Netflix and Spotify are working to put an end to the fees they have to pay these app stores. Spotify thus prevents its customers from signing up through the App Store, and requires them to subscribe via the streaming service's website instead. The same is happening with Netflix to avoid having to give the App Store and Play Store a cut of transactions.

Web browsers can also be a vehicle that allows vertically integrated companies to favour their own services, at the expense of consumers' freedom of choice. Chrome, for instance, prevents users from installing extensions for downloading videos from YouTube, but does allow videos to be downloaded from rival sites, thereby reducing their per-view revenue.

Some changes in the marketplace are nevertheless in line with Arcep's recommendations. Having ascertained that voice assistants (developed chiefly by Google, Amazon and Apple) rely on speech recognition algorithms that are "taught" by large voice databases, in late 2017 Mozilla launched its Common Voice project to enable new players to develop similar algorithms. The organisation thus called on thousands of volunteers to read texts to enhance the open source dataset, and enable alternative companies to build their own voice technologies. The dataset became multilingual on 28 February 2019.

5. General Data Protection Regulation of 27 April 2016.

6. Article 28 of Act No. 2018-493 of 20 June 2018 on personal data protection: <https://www.legifrance.gouv.fr/eli/loi/2018/6/20/JUSC1732261L/jo/texte#JORFARTI000037086002>

OPEN FLOOR TO ...



Stefano Quintarelli, entrepreneur and former Italian parliamentarian

Why we do not own our devices

Imagine you own a flat. The flat is in a large building where the rules are strict and change often. One day, you are introduced to an excellent physiotherapist who specialises in exactly the type of care you need. But when she comes to you for an appointment, your doorman won't let her in. He gives several reasons for this: the physiotherapist refuses to give him a 30% cut of her fee, plus she is dressed in a way the doorman considers inappropriate. The doorman explains that you can only use one of the physiotherapists from the list that he has drawn up. There are a large number of physiotherapists on the list, but not the one you want. He insists that the rules are not there to control what you do in your own home, or to skim money from physiotherapists, but rather to keep people with malicious intent from entering your flat – even if that implies you are not free to decide who can come into your home.

Your home is, in fact, only yours under the terms dictated by the gatekeeper. You will realise this the day you try to hire a bricklayer (other than the one recommended by the doorman's company) to remove a fireplace that you are being forced to keep, and which is taking up a huge amount of space in your living room. The doorman explains that you cannot remove your fireplace because the building has an agreement with a company that sells firewood, and that you might want to use some day.

If you don't like these rules, says the doorman, you are free to move to another building, but you will lose a great deal: all of the mementos of decades spent in your home, the custom-made drapes, etc. Plus you could move to a new flat without knowing whether you'll even be able to sell the old one. Ultimately, moving will cost you too much time and money, and you resign yourself to staying put...

“Device neutrality extends the principle of net neutrality to guarantee that, like your telecoms operator, a platform cannot interfere with your decisions by restricting your freedom of choice.”

The principle of “neutrality” means that those who manage access to resources cannot use that privilege to interfere with users' choices, to alter or limit them. This principle is now enshrined in European regulation, and enforced on telecommunications networks.

But this is not yet true of devices, these tools we use to keep us informed, to create and sustain social and business ties. Over time, our devices have become our main interface with the world. But, as with the flat described earlier, we do not really “own” our devices. They do not really belong to us: our choices are restricted by technical features and disproportionate contractual commitments (have you read your smartphone's terms and conditions of use?).

Device neutrality extends the principle of net neutrality to guarantee that, like your telecoms operator, a platform cannot interfere with your decisions by restricting your freedom of choice. Of course, anyone who likes the doorman's terms will be free to adhere to them, and accept the associated restrictions. And may even pay extra for it. But someone who prefers to follow an alternative path must be able to do so, whether as a building's resident or a visiting physiotherapist.

It was to guarantee device neutrality that, in 2015, when I was a member of Parliament in Italy, I proposed a bill that would enforce network and device neutrality. This proposal was approved with unanimity by every committee in the Chamber of deputies and every Senate committee in 2017, but the final vote was postponed time and again and the legislature was dissolved. This bill was therefore never able to become law in Italy. But such a law still needs to be passed in Europe.

OPEN FLOOR TO ...



Maryant Fernández Pérez, Senior Digital Policy Officer, BEUC

Do we control our electronic devices? A European law could make it possible!

The Internet has become ubiquitous in our lives, and of course, we use devices to access it. However, we experience several restrictions when using them. For instance, can you uninstall all the apps pre-installed in your tablet? Does your device always respect your decision to use a browser that is different from the one installed by default? To solve these problems, we, The European Consumer Organisation (BEUC), are asking the European Union to enshrine device neutrality in EU law.

If Europe managed to adopt a device neutrality law, it would be a major victory for consumers. This law could, for instance, give consumers greater freedom when using their smartphones, voice assistants and connected cars and give them access to more applications and services. This law could also benefit businesses by making it easier for consumers to use their services. It could finally spur the supply of applications that better respect our privacy, for example.

Whether smartphones, tablets, smart speakers, voice assistants or any other connected devices, consumers must be able to use their devices in a neutral and non-discriminatory way.

Unfortunately, this is not always the case. Passing a law on device neutrality would be the logical next step after the adoption of the European net neutrality rules, which have demonstrated EU leadership globally. Since 2016, the EU ensures consumers have access to an open internet in which internet service providers (ISP)s must treat traffic “equally [and] without discrimination, restriction or interference”. Lawmakers must now enshrine access to the open internet at every link of the internet access chain, not just at ISP level.

A European law on device neutrality would need to establish clear definitions and obligations for the various economic actors that are behind our devices, and adequate enforcement of the rules. This law should also make sure that consumers have the right to use the software they want and access the content and services of their choice without discrimination. While protecting the device’s core functionality and security, consumers must be able to uninstall any app, service or content they do not want on their devices, amongst other things.

In addition, this law could serve to both complement Europe’s Platform-to-Business (P2B) Regulation and competition law.

First, the P2B Regulation introduces transparency obligations, new requirements regarding dispute settlement mechanisms and forbids certain unfair practices. It applies only to relationships between enterprises, but we hope that consumers will also reap its benefits.

Second, competition law can settle certain issues but it is not enough to guarantee device neutrality. Defining neutrality as a form of non-discrimination could, for instance, be a key ingredient in a remedy that ensures a competitive market, as in the European Commission’s anti-trust case against Android. However, any impediment to device neutrality can only be treated when it is linked to an abuse of dominant position. Competition law can lay down the principles, but an actual solution needs to be written into European law.

We congratulate Arcep for the work done on this issue, as well as other competent authorities for their contributions and willingness to defend consumers and promote competitive innovation in this area. This is the first step towards achieving device neutrality. BEUC already supported a similar initiative in Italy together with our Italian member, Altroconsumo. It is high time to ensure device neutrality in Europe!



Lexicon

The definitions provided below are only used in the context of this report, for the sake of clarity.

A

AES-NI (Advanced Encryption Standard New Instructions): a set of instructions that are incorporated into all of the latest microprocessors, with the goal of speeding up encryption and decryption operators using Advanced Encryption Standard (AES), and exchanges that use HTTPS.

Afnic (Association française pour le nommage Internet en coopération): France's domain name registry. A non-profit organisation (under France's law of 1901) whose mandate is to manage top-level domain names in France (.fr), Reunion (.re), France's southern and Antarctic territories (.tf), Mayotte (.yt), Saint-Pierre-et-Miquelon (.pm) and Wallis-et-Futuna (.wf).

Agent within the box: QoS and/or QoE measurement tool installed directly on an ISP's box.

Android: mobile operating system developed by Google.

ANSSI (National Information Systems Security Agency): French federal government service responsible for the security and protection of information systems.

API: Application Programming Interface that enables two systems to interoperate and talk to one another without having been initially designed for that purpose. More specifically, a standardised set of classes, methods or functions through which a software programme provides services to other software.

B

BEREC (Body of European Regulators for Electronic Communications): independent European body created by the Council of the European Union and the European Parliament, and which assembles the electronic communications regulators from the 28 European Union Member States.

C

Cable networks: electronic communications networks made up of an optical fibre network core and coaxial cable in the last mile. Originally designed to broadcast television services, these networks have also made it possible to deliver telephone and internet access services for several years, by using the bandwidth not employed by TV broadcasting.

CAP: content (web pages, blogs, videos) and/or applications (search engine, VoIP applications) providers.

CDN: Internet Content Delivery Network.

CGN (Carrier-grade NAT): Large-scale Network Address Translation (NAT) mechanism, used in particular by ISPs to diminish the quantity of IPv4 addresses used.

Cross-traffic: the traffic generated during a QoS and/or QoE test by an application other than the one being used to perform the test, either on the same device or on another device connected to the same box. Cross-traffic decreases the bandwidth available for the test.

Crowdsourcing: crowdsourcing tools refer to those instruments that centralise QoS and/or QoE tools performed by actual users.

D

DGCCRF (Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes/Directorate-General for Competition, Consumer Affairs and Fraud Repression): French government agency responsible for ensuring that markets function properly, for the benefit of consumers and businesses.

DNS (Domain Name System): mechanism for translating internet domain names into IP addresses.

DPI (Deep Packet Inspection): network infrastructure equipment that consists of analysing the content of IP packets to then prioritise or filter them, or cull statistics.

Dual-Stack: Assigning both an IPv4 address and an IPv6 address to a device on the network.

E

Ethernet (cable): common name for an RJ45 connector that supports the Ethernet packet communication protocol.

F

Ftth (Fibre to the Home) network: very high-speed electronic communications network, where fibre is pulled right into the customer's premises.

G

GDPR (General Data Protection Regulation): European Union (EU) regulation No. 2016/679 on data protection and privacy.

H

Hardware probe: tool for measuring QoS and/or QoE which typically takes the form of a box connected to an ISP's box with an Ethernet cable. A hardware probe usually tests the internet line automatically, in a passive fashion.

HTTP (Hypertext Transfer Protocol): client-server communication protocol developed for the World Wide Web.

HTTPS: HTTP Secured thanks to the use of SSL (secure socket layer) or TLS (transport layer security) protocols.

I

IAD (Integrated Access Device): a home gateway, commonly referred to as an internet box, which enables residential users to connect their telephone, computers and TV box to the Web.

ICMP: Internet Control Message Protocol used by network devices to relay error messages. It can be used to measure latency through the ping command that is built into all operating systems.

INC (Institut National de la Consommation): French National Consumer Affairs Institute. A public industry and trade establishment under the aegis of the Minister responsible for consumer affairs, representing consumers and consumer protection associations.

iOS: mobile operating system developed by Apple for its mobile devices.

IP (Internet Protocol): communication protocol that enables a single addressing service for any device used on the internet. IPv4 (IP version 4) is the protocol that has been since 1983. IPv6 (IP version 6) is its successor.

IPv6-ready: which is compatible with IPv6, but on which IPv6 is not necessarily activated by default.

IS (Information system): organised set of resources for collecting, storing, processing and disseminating information.

ISOC (Internet Society): an American non-profit association that seeks to promote and coordinate the development of the internet throughout the world.

ISP: Internet Service Provider

IXP (Internet Exchange Point) or GIX (Global Internet Exchange): physical infrastructure enabling the ISPs and CAPs connected to it to exchange internet traffic between their networks thanks to public peering agreements.

L

LAN (Local Area Network): For residential users, this is the network made up of the ISP's box and any peripheral devices connected to it, either via Ethernet or Wi-Fi.

Latency: the time it takes for a data packet to travel over the network from source to destination. Latency is expressed in milliseconds.

Linux: broadly speaking, refers to any operating system with a Linux kernel. The Linux kernel is used on hardware ranging from mobile phones (e.g. Android) to supercomputers, by way of ordinary PCs (e.g. Ubuntu).

Live-USB: a USB flash drive that makes it possible to boot up an operating system stored on a USB drive, without having to use the computer's hard drive. Any USB drive can be turned into a Live-USB.

M

mac OS: operating system developed by Apple for its computers.

Multi-thread speed test: test for measuring internet connection speed by adding together the speeds of multiple simultaneous connections, making it possible to estimate the link's capacity.

N

NRA (National Regulatory Authority): an organism or organisms that a BEREC Member State mandates to regulate electronic communications.

O

On-net CDN: CDN located directly in an ISP's network.

ONT (Optical Network Termination): FttH network equipment located on the customer's premises. An ONT can either be built-in or located outside the box.

OS (Operating System): software that runs a peripheral device, such as Windows, Mac OS, Linux, Android or iOS.

OTT (over-the-top): used to refer to electronic communications services that CAP provide over the internet.

P

Peering: the process of exchanging internet traffic between two peers. A peering link can be either free or paid (for the peer that sends more traffic than the other peer). Peering can be public, when performed at an IXP (Internet Exchange Point), or private when over a PNI (Private Network Interconnect), in other words a direct interconnection between two operators.

Peering policy: a usually publicly available document that contains an operator's interconnection strategy.

Provisioning: the automatic allocation of resources. For example, a provisioning solution can automatically allocate IPv4 and IPv6 to customers.

PLC (Powerline carrier) [adapters]: equipment for relaying internet traffic over the electrical network inside the home, instead of using an Ethernet cable or Wi-Fi.

Q

QoE (Quality of Experience): in Chapter 1, quality of the user's internet experience, for a given application. It is measured by performance indicators such as web page load time or video streaming quality.

QoS (Quality of service): in Chapter 1, quality of service on the internet as measured by "technical" indicators such as download or upload speed, latency and jitter. The term QoS is often used to refer to both technical quality and quality of experience (QoE).

R

RAM: Random Access Memory. A computing device's "working" memory through which it processes information. A lack of RAM will slow down the computer significantly forcing it to employ a slower part of the hard drive instead.

S

Single thread speed test: test for measuring the speed via a single connection, which makes it possible to have a representative flow of an Internet use.

Slow start: TCP protocol algorithm that consists of gradually increasing bitrates speeds over the course of a download.

Speed: quantity of digital data transmitted within a set period of time. Connection speeds or bitrates, are often expressed in bits per second (bit/s) and its multiples: Mbit/s, Gbit/s, Tbit/s, etc. It is useful to draw a distinction between the speed at which data can be:

- received by a piece of terminal equipment connected to the internet, such as when watching a video online or loading a web page. This is referred to as download or downlink speed;
- sent from a computer, phone or any other piece of terminal equipment connected to the internet, such as when sending photos to an online printing site. This is referred to as upload or uplink speed.

T

TCP (Transmission Control Protocol): reliable, connected mode, transport protocol developed in 1973. In 2018, most internet traffic uses TCP as an upper layer transport protocol, on top of IPv4 or IPv6.

Test server (for QoS measurement): A server that does not store data, but is able to deliver data at very high speed and allow the connection's speed to be measured.

Tier 1: a network capable of interconnecting directly with any internet network (i.e. via peering) without having to go through a transit provider. There were 18 Tier 1 operators in 2018: AT&T, CenturyLink/Level 3, Cogent Communications, Deutsche Telekom AG, Global Telecom & Technology, Hurricane Electric, KPN International, Liberty Global, NTT Communications, Orange, PCCW Global, Sprint, Tata Communications, Telecom Italia Sparkle, Telxius/Telefónica, Telia Carrier, Verizon Enterprise Solutions and Zayo Group.

TLS (Transport Layer Security): used for encrypting internet exchanges and server authentication.

Transit provider: company that provides transit services.

Transit: bandwidth that one operator sells to a client operator, that makes it possible to access the entire internet through a contractual and paid service.

U

Ubuntu: GNU / Linux operating system based on Debian Linux distribution. Ubuntu is one of the most widely used free software operating systems in France.

UDP (User Datagram Protocol): simple, connectionless (i.e. no prior communication required) transmission protocol, which makes it possible to transmit small quantities of data rapidly. The UDP protocol is used on top of IPv4 or IPv6.

UFC-Que choisir (Union Fédérale des Consommateurs): French consumer protection association whose goal is to inform, advise and protect consumers.

V

VPN (Virtual Private Network): inter-network connection for connecting two local networks using a tunnel protocol.

W

WAN (Wide Area Network): in Chapter 1, WAN refers to the internet network, as opposed to a LAN (local area network).

WebSocket: networking protocol that makes it possible to create full-duplex communication channels on top of a TCP connection for web browsers. A large number of internet speed tests use it because it enables better performances than HTTP.

Web tester: tool for measuring QoS and QoE that is accessed through a website.

Wehe: Android and iOS application, developed by Northeastern University in partnership with Arcep to detect traffic management practices that are in violation of net neutrality rules.

Wi-Fi: wireless communication protocol governed by IEEE 802.11 group standards.

Windows: proprietary operating system developed by Microsoft, which powers the majority of computers in France.

X

xDSL (Digital Subscriber Line): electronic communications technologies used on copper networks that enable ISPs to provide broadband or superfast broadband internet access. ADSL2+ and VDSL2 are the most commonly used xDSL standards in France for providing consumer access.

Z

Zero-rating: a pricing practice that allows subscribers to use one or more particular online applications without the traffic being counted against their data allowance.

#

4G box: box that provides a high-speed internet connection over a 4G network.

Annexes

Annex 1

Implementation of an Application Programming Interface (API) in boxes

1. MAIN PARAMETERS

The main parameters are sent by the Integrated Access Device (IAD) to a quality of service (QoS) measurement tool, following a single call that is sent when the user performs an internet QoS test.

PRESENCE REQUIREMENT	JSON TREE	PARAMETER NAME	UNIT	PARAMETER DETAILS	FORMAT/ACCEPTED VALUES
Mandatory	Root	ApiVersion		Version de API	64-bit signed integer
Mandatory	TimeStamp	ApiCallTime		Time stamp that corresponds to the time when the API is called	64-bit signed integer
Mandatory	Gateway	Model		Customer IAD ("box") name	text
Mandatory	Gateway	HardwareVersion		Hardware version (e.g. rev3)	text
Mandatory	Gateway	SoftwareVersion		Software version	text
Mandatory	SubscriptionSpeed	DownloadMin	Kbit/s	Minimum guaranteed download speed	64-bit signed integer
Mandatory	SubscriptionSpeed	UploadMin	Kbit/s	Minimum guaranteed upload speed	64-bit signed integer
Mandatory	SubscriptionSpeed	DownloadMax	Kbit/s	Maximum guaranteed download speed	64-bit signed integer
Mandatory	SubscriptionSpeed	UploadMax	Kbit/s	Maximum guaranteed upload speed	64-bit signed integer
Mandatory	SubscriptionSpeed	DownloadNormally	Kbit/s	Guaranteed "normally available" download speed (if it exists)	64-bit signed integer
Mandatory	SubscriptionSpeed	UploadNormally	Kbit/s	Guaranteed "normally available" upload speed (if it exists)	64-bit signed integer
Mandatory	Wan	Technology		WAN technology used by the IAD ("box")	["FTTH";"ADSL"; "VDSL";"Gfast";"cable"; "satellite";"2G/3G"; "4G";"5G"]
Mandatory if FTTH is the WAN technology	WAN/SpeedOnt	Download	Kbit/s	FTTH only: Ethernet downlink speed between the ONT and IAD. Optional: if PLC detected on the WAN port: raw speed provided by PLC.	64-bit signed integer
Mandatory if FTTH is the WAN technology	WAN/SpeedOnt	Upload	Kbit/s	FTTH only: Ethernet uplink speed between the ONT and IAD. Optional: if PLC detected on the WAN port: raw speed provided by PLC.	64-bit signed integer



PRESENCE REQUIREMENT	JSON TREE	PARAMETER NAME	UNIT	PARAMETER DETAILS	FORMAT/ACCEPTED VALUES
Mandatory if FTTH is the WAN technology	Wan/SpeedOnt	Duplex		FTTH only: Ethernet mode between the ONT and IAD	["half";"full"]
Mandatory if xDSL is the WAN technology	Wan/SpeedSynchro	Download	Kbit/s	xDSL only: downstream synchronisation speed	64-bit signed integer
Mandatory if xDSL is the WAN technology	Wan/SpeedSynchro	Upload	Kbit/s	xDSL only: upstream synchronisation speed	64-bit signed integer
Mandatory	Wan	Aggregation		Aggregation of two active WAN connections E.g.: xDSL + 4G	["yes";"no"]

N.B.: regarding customers' advertised speed:

- The "minimum speed" should only be filled in if the connection has a guaranteed minimum speed;
- The "normally available speed" should only be filled in if the connection has a guaranteed normally available speed;

- The "maximum speed" indicated for FTTH access lines must always be the customer's advertised speed. For xDSL lines, it should only be filled in if the connection has a guaranteed maximum speed.

PRESENCE REQUIREMENT	JSON TREE	PARAMETER NAME	UNIT	PARAMETER DETAILS	FORMAT/ACCEPTED VALUES
Mandatory	Lan	ConnectionType		Technology used by the API requesting device to reach the IAD. Note: PLC detection on the LAN is optional.	["wifi";"Ethernet";"cpl";"other"]
Mandatory	Lan/SpeedLan	Download	Kbit/s	LAN downlink speed (Ethernet / Wi-Fi / PLC) negotiated by the API requesting device. PLC: raw speed supplied by the PLC connected to the Ethernet port from which the API request is sent.	64-bit signed integer
Mandatory	Lan/SpeedLan	Upload	Kbit/s	LAN uplink speed (Ethernet / Wi-Fi / PLC) negotiated by the API requesting device	64-bit signed integer
Mandatory if the LAN connection is Ethernet	Lan/SpeedLan	Duplex		Half-duplex or full-duplex Ethernet	["half";"full"]
Mandatory if the LAN connection is Wi-Fi	Lan/Wifi	ieee		Wi-Fi IEEE 802.11 standard negotiated between the IAD and the API requesting device.	Positive integer (802.11a=>1 802.11b=>2 802.11g=> 3 802.11n=>4 802.11ac=>5 802.11ax=>6)
Mandatory if the LAN connection is Wi-Fi	Lan/Wifi	RadioBand		Wi-Fi radio band used by the API requesting device. 2.4 GHz frequency block or 5 GHz frequency block.	Positive integer: 2.4 GHz band => 2 5 GHz band => 5
Mandatory if the LAN connection is Wi-Fi	Lan/Wifi	Rssi	dBm	Received radio signal strength Indication. It is the API requesting device's RSSI.	64-bit signed integer

Note: Some PLC¹ adapters cannot be detected by the IAD. The same is true with Wi-Fi connections initiated at an outside access point that is connected to the IAD via Ethernet.

1. Powerline carrier: equipment for providing internet access over the electrical network inside the home, instead of an Ethernet cable or Wi-Fi connection.

2. CROSS-TRAFFIC PARAMETERS

The parameters are specific to cross-traffic. They are collected by the QoS measurement tool following **two requests** sent:

- immediately after the customer has launched the test for measuring internet quality of service;

- immediately after the measurement tool has completed the internet quality of service test.

The tool determines that cross-traffic is present if the number of bytes on the WAN interface is significantly higher than the number of bytes that the internet QoS measurement test itself has generated.

PRESENCE REQUIREMENT	JSON TREE	PARAMETER NAME	UNIT	PARAMETER DETAILS	FORMAT/ACCEPTED VALUES
Mandatory	Root	ApiVersion		Version de API	64-bit signed integer
Mandatory	ByteCounter	Download	Bytes	WAN port downstream traffic meter reading (internet => IAD)	64-bit signed integer
Mandatory	ByteCounter	Upload	Bytes	WAN port upstream traffic meter reading (IAD => internet)	64-bit signed integer
Mandatory	TimeStamp	ApiCallTime		Time stamp that corresponds to the time when the API is called	64-bit signed integer
Mandatory	TimeStamp	LastUpdate		Time stamp for the WAN port meter's latest update (meter is read in real time LastUpdate = ApiCallTime)	64-bit signed integer

In cases where the IAD cannot provide the meter reader with information on the number of bytes on the WAN port, the number of packets multiplied by the MTU (Maximum Transmission Unit) should be used instead to provide an approximation.

Test servers provided by the different quality of service measurement tools

Arcep does its utmost to ensure that this information is accurate when the document goes to press. It is nevertheless possible that changes to the test servers used have occurred in the meantime.

NPERF

SPONSOR, AS LISTED ON NPERF	CITY	REGION OR COUNTRY	IPv6	CONNECTION CAPACITY	PORT USED	HOSTING COMPANY	AS
SFR	Courbevoie	Île-de-France	IPv4 only	10 Gbit/s	443	SFR	AS15557
Orange	Paris	Île-de-France	IPv4 or IPv6	10 Gbit/s	443	Orange	AS3215
Orange	Puteaux	Île-de-France	IPv4 or IPv6	10 Gbit/s	443	Orange	AS3215
Orange	Lyon	Auvergne-Rhône-Alpes	IPv4 or IPv6	10 Gbit/s	443	Orange	AS3215
Orange	Rennes	Bretagne	IPv4 or IPv6	10 Gbit/s	443	Orange	AS3215
Bouygues Telecom	Anycast	Île-de-France (Paris)	IPv4 or IPv6	10 Gbit/s	443	Bouygues Telecom	AS5410
		Hauts-de-France (Lille)					
		Auvergne-Rhône-Alpes (Lyon)					
		Région SUD (Marseille) Nouvelle-Aquitaine (Bordeaux)					
RRT	Compiègne	Hauts-de-France	IPv4 only	10 Gbit/s	443	Renater	AS2200
OVH	Gravelines	Hauts-de-France	IPv4 or IPv6	10 Gbit/s	443	OVH	AS16276
OVH	Roubaix	Hauts-de-France	IPv4 or IPv6	10 Gbit/s	443	OVH	AS16276
OVH	Strasbourg	Grand Est	IPv4 or IPv6	10 Gbit/s	443	OVH	AS16276
DataPacket	Paris	Île-de-France	IPv4 only	10 Gbit/s	443	DataCamp	AS60068
Leonix	Paris	Île-de-France	IPv4 or IPv6	10 Gbit/s	443	Leonix Telecom	AS50628
Wibox	Saint-Denis	Île-de-France	IPv4 only	10 Gbit/s	443	Altitude Infrastructure	AS49594
Phibee Telecom	Aubervilliers	Île-de-France	IPv4 or IPv6	10 Gbit/s	8443	Phibee Telecom	AS8487
SHPV France	Toulouse	Occitanie	IPv4 or IPv6	6 Gbit/s	443	SHPV France	AS41652
Online	Vitry-sur-Seine	Île-de-France	IPv4 only	4 Gbit/s	443	Scaleway – Online	AS12876
Proceau	Paris	Île-de-France	IPv4 only	1 Gbit/s	8443	Proceau	AS43424
AppliWave	Vitry-sur-Seine	Île-de-France	IPv4 or IPv6	1 Gbit/s	443	AppliWave	AS200780



SPONSOR, AS LISTED ON NPERF	CITY	REGION OR COUNTRY	IPv6	CONNECTION CAPACITY	PORT USED	HOSTING COMPANY	AS
Ikoula	Reims	Grand Est	IPv4 or IPv6	1 Gbit/s	8443	Ikoula	AS21409
Azylis	Besançon	Bourgogne-Franche-Comté	IPv4 only	1 Gbit/s	443	Azylis	AS207151
Rezopole	Lyon	Auvergne-Rhône-Alpes	IPv4 or IPv6	1 Gbit/s	443	Rezopole	AS199422
Muona	Lyon	Auvergne-Rhône-Alpes	IPv4 only	1 Gbit/s	443	Muona	AS50818
iDruide	Limonest	Auvergne-Rhône-Alpes	IPv4 only	1 Gbit/s	443	DCforData	AS197685
AOC Telecom	Clermont-Ferrand	Auvergne-Rhône-Alpes	IPv4 only	100 Mbit/s	443	AOC Telecom	AS202328
Céliéno	Lucé	Centre-Val de Loire	IPv4 only	1 Gbit/s	443	CM'IN – Céliéno	AS39271
System-Net	Montpellier	Occitanie	IPv4 only	1 Gbit/s	443	System-Net	AS60427

UFC-QUE CHOISIR SPEEDTEST

The test uses a single target, composed of two servers running at 10 Gbit/s that share the load. They use port 443 with an encrypted connection.

CITY	REGION	IPv6	CONNECTION CAPACITY	PORT USED	HOSTING COMPANY	AS
Saint-Denis	Île-de-France	IPv4 only	20 Gbit/s	443	Zayo France	AS8218

FIXED SPEED TESTS DEVELOPED BY QOSI (DÉBITEST 60 / 4GMARK / NETMARK ZD-NET)

Below are the test servers offered by QoSi. They all use port 8443 and traffic is encrypted.

CITY	REGION	IPv6	CONNECTION CAPACITY	PORT USED	HOSTING COMPANY	AS
Roubaix	Hauts-de-France	IPv4 only	1 Gbit/s	8443	OVH	AS16276
Vitry-sur-Seine ou Saint-Ouen- l'Aumône	Île-de-France	IPv4 only	1 Gbit/s	8443	Scaleway – Online	AS12876

MOBILE SPEED TESTS DEVELOPED BY QOSI (4GMARK / DÉBITEST 60 / KICAPTE / TU CAPTES ? / GIGALIS)

SPONSOR, AS LISTED ON THE APPLICATION	CITY	REGION OR COUNTRY	IPv6	CONNECTION CAPACITY	PORT USED	HOSTING COMPANY	AS
SFR	Courbevoie	Île-de-France	IPv4 only	10 Gbit/s	80	SFR	AS15557
Orange France	Paris	Île-de-France	IPv4 only	10 Gbit/s	80	Hivane	AS34019
Bouygues Telecom	Nanterre	Île-de-France	IPv4 only	10 Gbit/s	443	Bouygues Telecom	AS540
Mediactive Network	Paris	Île-de-France	IPv4 only	10 Gbit/s	80	Mediactive Network	AS197133
OneProvider Paris	Vitry-sur-Seine	Île-de-France	IPv4 only	1 Gbit/s	443	Scaleway – Online	AS12876
OneProvider Paris2	Vitry-sur-Seine	Île-de-France	IPv4 only	1 Gbit/s	443	Scaleway – Online	AS12876
OneProvider Paris3	Vitry-sur-Seine	Île-de-France	IPv4 only	1 Gbit/s	443	Scaleway – Online	AS12876
OVH 5GMARK	Roubaix	Hauts-de-France	IPv4 only	1 Gbit/s	443	OVH	AS16276
Ikoula	Reims	Grand Est	IPv4 only	1 Gbit/s	443	Ikoula	AS21409
Adeli	Saint-Trivier-sur-Moignans	Auvergne-Rhône-Alpes	IPv4 only	1 Gbit/s	443	Adeli	AS43142

IPv6-TEST

Below are the test servers offered by the IPv6-test: migration is currently underway to port 443.

SPONSOR, AS INDICATED ON THE SPEEDTEST	CITY	REGION OR COUNTRY	IPv6	CONNECTION CAPACITY	PORT USED	HOSTING COMPANY	AS
LaFibre.info	Paris	Île-de-France	IPv4 and IPv6	10 Gbit/s	443 or 80	Bouygues Telecom	AS5410
OVH	Limbourg	Allemagne	IPv4 and IPv6	100 Mbit/s	443 or 80	OVH	AS16276
ZeelandNet	Zélande	Pays-Bas	IPv4 and IPv6	1 Gbit/s	80 only	ZeelandNet	AS15542
ServerHouse	Portsmouth	Royaume-Uni	IPv4 and IPv6	1 Gbit/s	80 only	ServerHouse	AS21472
EBOX	Longueuil	Canada	IPv4 and IPv6	1 Gbit/s	80 only	EBOX	AS174

OOKLA SPEEDTEST.NET

Below are the test servers offered by Ookla's SpeedTest.net in France: they all use port 8080 and traffic is encrypted. For mobile

applications, legacy mode makes it possible to run the test in http on port 80 if port 8080 websockets are blocked.

SPONSOR, AS INDICATED ON THE SPEEDTEST	CITY	REGION OR COUNTRY	IPv6	CONNECTION CAPACITY	PORT USED	HOSTING COMPANY	AS
Orange	Paris	Île-de-France	IPv6 only*	10 Gbit/s	8080	Hivane	AS34019
Naitways	Paris	Île-de-France	IPv4 only	10 Gbit/s	8080	Naitways	AS57119
SFR	Paris	Île-de-France	IPv4 only	10 Gbit/s	8080	SFR	AS15557
SiriusHD	Paris	Île-de-France	IPv4 only	10 Gbit/s	8080	Scaleway – Online	AS12876
fdcservers.net	Paris	Île-de-France	IPv4 only	10 Gbit/s	8080	Cogent	AS174
Interoute VDC	Paris	Île-de-France	IPv4 only	10 Gbit/s	8080	GTT – Interoute	AS8928
Cloudwatt	Paris	Île-de-France	IPv4 only	10 Gbit/s	8080	Cloudwatt	AS60940
Leonix Telecom	Paris	Île-de-France	IPv6 only*	10 Gbit/s	8080	Leonix Telecom	AS50628
Stella Telecom	Courbevoie	Île-de-France	IPv4 only	10 Gbit/s	8080	Stella Telecom	AS16211
ONLINE	Vitry-sur-Seine	Île-de-France	IPv4 only	10 Gbit/s	8080	Scaleway – Online	AS12876
TestDebit.info	Massy	Île-de-France	IPv6 only*	10 Gbit/s	8080	Bouygues Telecom	AS5410
Wibox	Val-de-Reuil	Normandie	IPv4 only	10 Gbit/s	8080	Altitude Infrastructure	AS49594
LaFibre.info	Douai	Hauts-de-France	IPv6 only*	10 Gbit/s	8080	Bouygues Telecom	AS5410
Orange	Lyon	Auvergne-Rhône-Alpes	IPv6 only*	10 Gbit/s	8080	Rezopole	AS199422
LaFibre.info	Lyon	Auvergne-Rhône-Alpes	IPv6 only*	10 Gbit/s	8080	Bouygues Telecom	AS5410
Via Numérica	Archamps	Auvergne-Rhône-Alpes	IPv4 only	10 Gbit/s	8080	Via Numérica	AS44494
LaFibre.info	Bordeaux	Nouvelle-Aquitaine	IPv6 only*	10 Gbit/s	8080	Bouygues Telecom	AS5410
TestDebit.info	Marseille	Région Sud	IPv6 only*	10 Gbit/s	8080	Bouygues Telecom	AS5410
CCleaner	Paris	Île-de-France	IPv4 only	1 Gbit/s	8080	Scaleway	AS12876
HarryLafranc	Paris	Île-de-France	IPv4 only	1 Gbit/s	8080	Hexatom	AS51269
Télécom ParisTech	Paris	Île-de-France	IPv6 only*	1 Gbit/s	8080	Renater	AS1712
Host-Heberg	Paris	Île-de-France	IPv4 only	1 Gbit/s	8080	OVH	AS16276
Ozone	Courbevoie	Île-de-France	IPv4 only	1 Gbit/s	8080	Nomotech – Ozone	AS39886
Vianet	Le Havre	Normandie	IPv4 only	1 Gbit/s	8080	velia.net	AS29066
Eurafibre	Lille	Hauts-de-France	IPv4 only	1 Gbit/s	8080	Eurafibre	AS35625

...

SPONSOR, AS INDICATED ON THE SPEEDTEST	CITY	REGION OR COUNTRY	IPv6	CONNECTION CAPACITY	PORT USED	HOSTING COMPANY	AS
ePlay TV	Roubaix	Hauts-de-France	IPv6 only*	1 Gbit/s	8080	OVH	AS16276
Techplus.europe	Roubaix	Hauts-de-France	IPv4 only	1 Gbit/s	8080	OVH	AS16276
Ikoula	Reims	Grand Est	IPv6 only*	1 Gbit/s	8080	Ikoula	AS21409
Hexanet	Reims	Grand Est	IPv4 only	1 Gbit/s	8080	Hexanet	AS34863
RIV54	Saulnes	Grand Est	IPv4 only	1 Gbit/s	8080	Vialis	AS42487
Orne THD	Rombas	Grand Est	IPv6 only*	1 Gbit/s	8080	Orne THD	AS41114
Vialis	Woippy	Grand Est	IPv4 only	1 Gbit/s	8080	Vialis	AS42487
Regie Talange	Talange	Grand Est	IPv4 only	1 Gbit/s	8080	Vialis	AS42487
REFO Falck	Falck	Grand Est	IPv4 only	1 Gbit/s	8080	Vialis	AS42487
Enes	Hombourg-Haut	Grand Est	IPv4 only	1 Gbit/s	8080	Vialis	AS42487
Fibragglo	Forbach	Grand Est	IPv4 only	1 Gbit/s	8080	Vialis	AS42487
La Regie	Reichshoffen	Grand Est	IPv4 only	1 Gbit/s	8080	SFR	AS15557
AS Dienstleistungen	Strasbourg	Grand Est	IPv4 only	1 Gbit/s	8080	OVH	AS16276
Rocho DataCenter	Chambéry	Auvergne-Rhône-Alpes	IPv6 only*	1 Gbit/s	8080	OVH	AS16276
Axione	Pau	Nouvelle-Aquitaine	IPv4 only	1 Gbit/s	8080	Axione	AS31167
Orange	Marseille	Région Sud	IPv4 only	1 Gbit/s	8080	Jaguar Network	AS30781
SEACOM	Marseille	Région Sud	IPv6 only*	1 Gbit/s	8080	SEACOM	AS37100
DFOX	Nice	Région Sud	IPv4 only	1 Gbit/s	8080	Scaleway – Online	AS12876
VistaWAN.com	Nice	Région Sud	IPv4 only	1 Gbit/s	8080	Scaleway – Online	AS12876

* The test is performed with IPv6 for all customers that are IPv6-enabled. IPv4 cannot be forced on these test servers. Customers who have an IPv4 connection and are not IPv6-enabled will perform their test in IPv4.

Annex 3

Increasing the accuracy of QoS testing

The purpose of this annex is to provide users with details on the parameters to be taken into account to improve the accuracy of quality of service measurement. The information contained in this annex is for information purposes only and is not intended to be exhaustive. Some quality of service measurement tools may have different prerequisites. Readers are also invited to refer to the instructions given by the different tools themselves.

Speeds below 100 Mbit/s: almost any machine that has 4 GB or more of RAM appears able to run tests at below 100 Mbit/s. Avoiding the use of Windows XP seems to be the only proviso.

For speeds between 100 and 300 Mbit/s, the minimum recommended configuration includes:

- Windows 10 and Linux Live-USB: 6 GB of RAM minimum. MacOS and Linux: 4 GB of RAM minimum;
- Network card capable of managing 1 Gbit/s;
- 4-pair Ethernet cable, i.e. eight wires (four-wire Ethernet cables are limited to 100 Mbit/s);
- CPU equipped with a set of AES hardware instructions: AES-NI (Advanced Encryption Standard New Instructions). Intel Core-i7 PC s since 2011, Intel Core-i5 PCs since 2012, AMD PCs since 2013, Intel Core-i3 PCs since 2014, Intel Pentium PCs and Intel Celeron PCs since 2016 are all equipped, in theory, with AES-NI;
- Antivirus software that does not inspect https traffic. Some antivirus software allows users to untick a box to disable https traffic inspection;
- Deactivate the web browser extensions that can slow the connection. Some extensions limit connection speed either directly or indirectly by increasing the load on the CPU;
- For single-thread tests, it is recommended that the latest version of the device's OS be used, whenever possible (e.g. Windows 7 or older can limit connection speed due to a TCP receive window² that can be too small in some instances).

For speeds between 300 Mbit/s and 1 Gbit/s, in addition to the prerequisites listed in the above section for connections of 100 to 300 Mbit/s, the minimum recommended configuration includes:

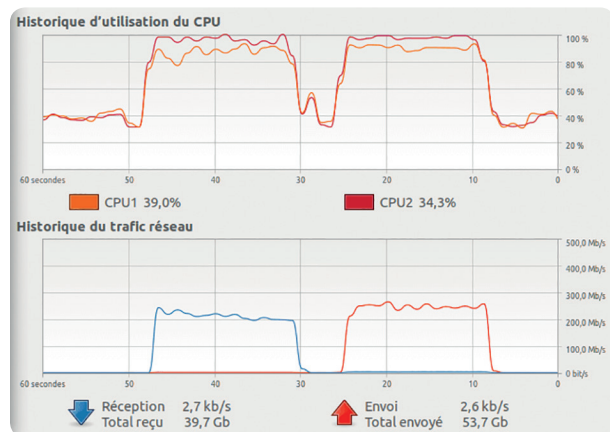
- Windows 10 and Linux Live-USB: 8 GB of RAM minimum. MacOS and Linux: 6 GB of RAM minimum;
- A recent 64-bit operating system:
 - Windows: Windows 8.1 minimum;
 - Mac OS: Mac OS 10.9 minimum;
 - Ubuntu: Ubuntu 14.04 minimum.
- Select a test server connected to the Internet at 10 Gbit/s;
- Display the CPU load during the test and check that it is running at less than 70% capacity during the test.

For speeds higher than 1 Gbit/s: performing reliable tests on 10 Gbit/s lines on a web browser currently appears to be a complicated affair. Added to which, as far as Arcep is able to ascertain, virtually no test server is connected to the internet with a link in excess of 10 Gbit/s.

Procedure for running a CPU stress test during the quality of service test:

- Windows: click on the button on the right-hand side of the taskbar, and click on Task Manager in the "Performance" tab, then choose "CPU";
- macOS: launch "Activity monitor" in Utilities. In the "CPU" tab, the idle rate must be at least 30%;
- Ubuntu: launch the "System monitor" app and click on the "Resources" tab.

The following graph depicts the CPU's average load over a period of time. To guarantee that QoS tests are not restricted, the CPU must not be using more than 70% of its capacity during the test.



2. Quantity of received data that is likely to be transferred in a single go over a connection. The sender can only send this amount of data, and must wait for an acknowledgement and a window update from the host receiver.

Example of a procedure for checking whether the CPU is equipped with Advanced Encryption Standard New Instructions (AES-NI).

AES-NI help accelerate processing:

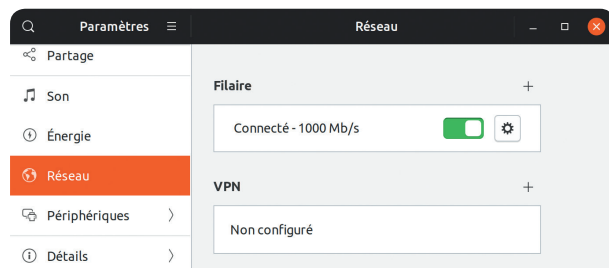
- Windows: download and launch CPU-Z (<https://www.cpuid.com/softwares/cpu-z.html>). In the "CPU" tab, the "Instructions" line must contain the letter-string "AES";
- macOS: download and launch MacCPUID (<https://software.intel.com/en-us/download/download-maccpuid>). In the "Features" tab, check that "AES" is enabled;
- Ubuntu: Launch the Terminal and type in "lscpu". The last paragraph must contain the letter-string "AES".

If the letters "AES" are not there, it means that the CPU is not equipped with the technology, which can slow the speed tests.

Spécification	Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz				
Famille	0X6	Modèle	0XE	Temp.	40°C
Famille ét.	0X6	Modèle ét.	0X8E	Stepping	10
Instructions	HT, MMX, SSE(1, 2, 3, 3S, 4.1, 4.2), AVX(1, 2), FMA(3) AES , CLMUL, RdRand, SGX, VT-x, x86-64				

Procedure for checking that Ethernet cable speed is 1 Gbit/s:

- Windows 10: in the Start Menu, launch "Settings" then click on "Network and Internet" then "View network properties". The "Connection speed" displayed must be 1 Gbit/s;
- macOS: launch "Network utility", under "Info", select the Ethernet interface. The "Link speed" displayed must be "1 Gbit/s";
- Ubuntu: launch "Settings". Under "Network", the wired speed must be "1000 Mbit/s".



This document was drafted by Arcep

DIRECTORATE FOR INTERNET AND USERS

Loïc DUFLOT, *director*

“Open Internet” unit

Pierre DUBREUIL, Vivien GUEANT, Emmanuel Leroux and Samih SOUISSI, *advisors*

DIRECTORATE FOR ECONOMY, MARKETS AND DIGITAL AFFAIRS

Stéphane LHERMITTE, *director*

“Economic analysis and digital intelligence” unit

Anaïs LE GOUGUEC, *head of unit*

Nisrynne NAHHAL and Vincent TOUBIANA, *advisors*

DIRECTORATE FOR MOBILE AND INNOVATION

Anne LAURENT, *directors*

“Mobile coverage and investments” unit

Guillaume DECORZENT, *head of unit*

Arnaud COMERZAN, *advisor*

DIRECTORATE FOR COMMUNICATIONS AND PARTNERSHIPS

Clémentine BEAUMONT, *director*

Anne-Lise LUCAS, *advisor*

DIRECTORATE FOR LEGAL AFFAIRS

Élisabeth SUEL, *director*

“Infrastructure and open networks” unit

Agate ROSSETTI, *head of unit*

Annabel GANDAR and Mélissa NOBILEAU, *advisors*

Thank you...

All of the people who were consulted, interviewed or who took part in Arcep’s co-construction efforts devoted to internet quality of service and in the IP♥6 workshop, for their energy and invaluable contribution to this report.

Publication

Arcep
14, rue Gerty Archimède - 75012 Paris
01 40 47 70 00 - com@arcep.fr

Design

Agence Luciole

Translation

Gail Armstrong

Printing

Corlet Imprimeur
ZI, rue Maximilien Vox,
Condé-sur-Noireau,
14110 Condé-en-Normandie

Photos' credits

Pages 6 and 7: Kibлинд
Pages 15, 21, 24, 35, 38
and 62: IStock/Getty Images,
Page 41: Florence Gaty /
Internet Society
Pages 52 to 55: Kibлинд

June 2019





ARCEP, NETWORKS AS COMMON GOOD

Internet, fixed and mobile telecom and postal networks constitute the “**Infrastructures of freedom**”. Freedom of expression, freedom to communicate, freedom to access knowledge and to share it, but also freedom of enterprise and innovation, which are key to the country’s ability to compete on the global stage, to grow and provide jobs. Because it is essential in all open, innovative and democratic societies to be able to enjoy these freedoms fully, national and European institutions work to ensure that these networks develop as a “**common good**”, regardless of their ownership structure, in other words that they meet high standards in terms of accessibility, universality, performance, neutrality, trustworthiness and fairness.

Democratic institutions therefore concluded that independent state intervention was needed to ensure that no power, be it economic or political, is in a position to control or hinder users’ (consumers, businesses, associations, etc.) ability to communicate with one another.

The electronic communications and postal regulatory authority (Arcep), a neutral and expert arbitrator with the status of quasi autonomous non-governmental organisation, is the **architect** and **guardian** of communication networks in France.

As network architect, Arcep creates the conditions for a plural and decentralised network organisation. It guarantees the market is open to new players and to all forms of innovation, and works to ensure the sector’s competitiveness through pro-investment competition. Arcep provides the framework for the networks’ interoperability so that users perceive them as one, despite their diversity: easy to access and seamless. It coordinates effective interaction between public and private sector stakeholders when local authorities are involved as market players.

As network guardian, Arcep enforces the principles that are essential to guaranteeing users’ ability to communicate. It oversees the provision of universal services and assists public authorities in expanding digital coverage nationwide. It ensures users’ freedom of choice and access to clear and accurate information, and protects against possible net neutrality violations. From a more general perspective, Arcep fights against any type of walled garden that could threaten the freedom to communicate on the networks, and therefore keeps a close watch over the new intermediaries that are the leading Internet platforms.