FRENCH REPUBLIC
JUNE 2018

The state of the Internet in France

2018 EDITION

arcep

Table of contents

Introduction

What was it like before? It is often difficult to remember what life was like for people and businesses before the phenomenal rise of the Internet, because it so thoroughly permeates every inch of our lives today that it has become invisible. Ubiquitous at home and at work, but also in the streets and on transportation, ever since we've been able to slip it into our pockets, the Internet has gone everywhere we do. In 2017, the smartphone became the device most commonly used to connect to the Internet in France, now outranking computers[1]. In a matter of years, this planetary network has become the "beating heart" of the economy, and of society as a whole. It has become an infrastructure that is vital to freedom of enterprise, of expression, freedom to innovate and to access knowledge. The technical, economic, social and democratic issues surrounding this by now vital global common good are colossal. And there is no guaranteed outcome.

The endless controversies over data privacy and fake news, cyberattacks, challenges to net neutrality, market concentration around a handful of digital platforms, unequal access: the steady stream of headlines are a constant reminder of the Internet's upheavals. All tantamount to a series of health scares, and reasons to consider what treatments to prescribe to maintain it over time as an engine of innovation and freedoms that upholds our values.

As architect and guardian of communication networks in France, Arcep has its share of responsibility. As such, Arcep identifies accidents and illnesses and potential future threats that fall under its purview, and takes action to heal or prevent them. A neutral and vigilant expert at the Internet's (bed)side, Arcep monitors changes over time, performing a complete annual check-up to ensure that this network of networks remains an inclusive public resource.

There are fundamental issues attached to the digital divide. In 2017, only two thirds of the people in France believed they were capable of using a computer[2]. If Arcep is not in charge of matters relating to digital technology training, it does keep a close watch over the second essential facet of the issue: infrastructure rollouts. The work it does on accessibility and coverage are available in Volume 2 of its annual report, "Arcep regulation in support of smart territories"[3].

Volume 3 of Arcep's annual report is this document on the state of the Internet in France. Beyond its main purpose of an annual report, it seeks to be a didactic presentation of the current state of networks and the work being done to best guarantee users' ability to exchange information. Arcep is devoted to keeping its finger on the Internet's pulse, and a watchful eye on its overall operation and openness: quality of service, data interconnection, the transition to IPv6, net neutrality and the openness of devices. Arcep's first line of action is to improve the instruments available to x-ray the networks and determine the symptoms, to then work on remedying the situation when necessary, by writing up the most appropriate prescription.

[1] https://www.arcep.fr/uploads/tx_gspublication/barometre_du_numerique-2017-infographie-271117.pdf
[2] https://www.arcep.fr/uploads/tx_gspublication/barometre_du_numerique-2017-infographie-271117.pdf
[3] https://www.arcep.fr/uploads/tx_gspublication/rapport-GRACO-2018_dec2017.pdf

1 QUALITY OF SERVICE

To improve quality of service on the internet, we need to be able to measure it correctly. But the comparison tools available today deliver such disparate results that it's no wonder users don't know which way to turn. It's impossible for them to use performance as a real criterion when choosing their access provider!
To "fine tune the scanner," increase its accuracy, transparency and clarity, Arcep called on all of the Web testing ecosystem's players and began a co-construction process. The goal: to publish a common code of conduct and develop an API that contains each device's "access ID card".

Key figure: **20 PLAYERS** involved in the co-construction process for measuring quality of service

Bonus: **5 TIPS** on how to improve your Wi-Fi signal

2 INTERCONNECTION

Interconnection enables all networks to talk to each other, and appear to us as a single network. But when two players do not agree on their interconnection, the quality of the user experience is threatened. Which is why Arcep keeps a close watch over the market: in late 2017, its information gathering process was further enhanced to take interconnection players' changing behaviour into account. Once consolidated, the results will be published in a dedicated annual scorecard, before the end of 2018. Arcep can also be required to "police" certain situations, and settle disputes between the players when the circumstances require.

Key figure: **+44%** increase in French ISPs' incoming traffic in a single year

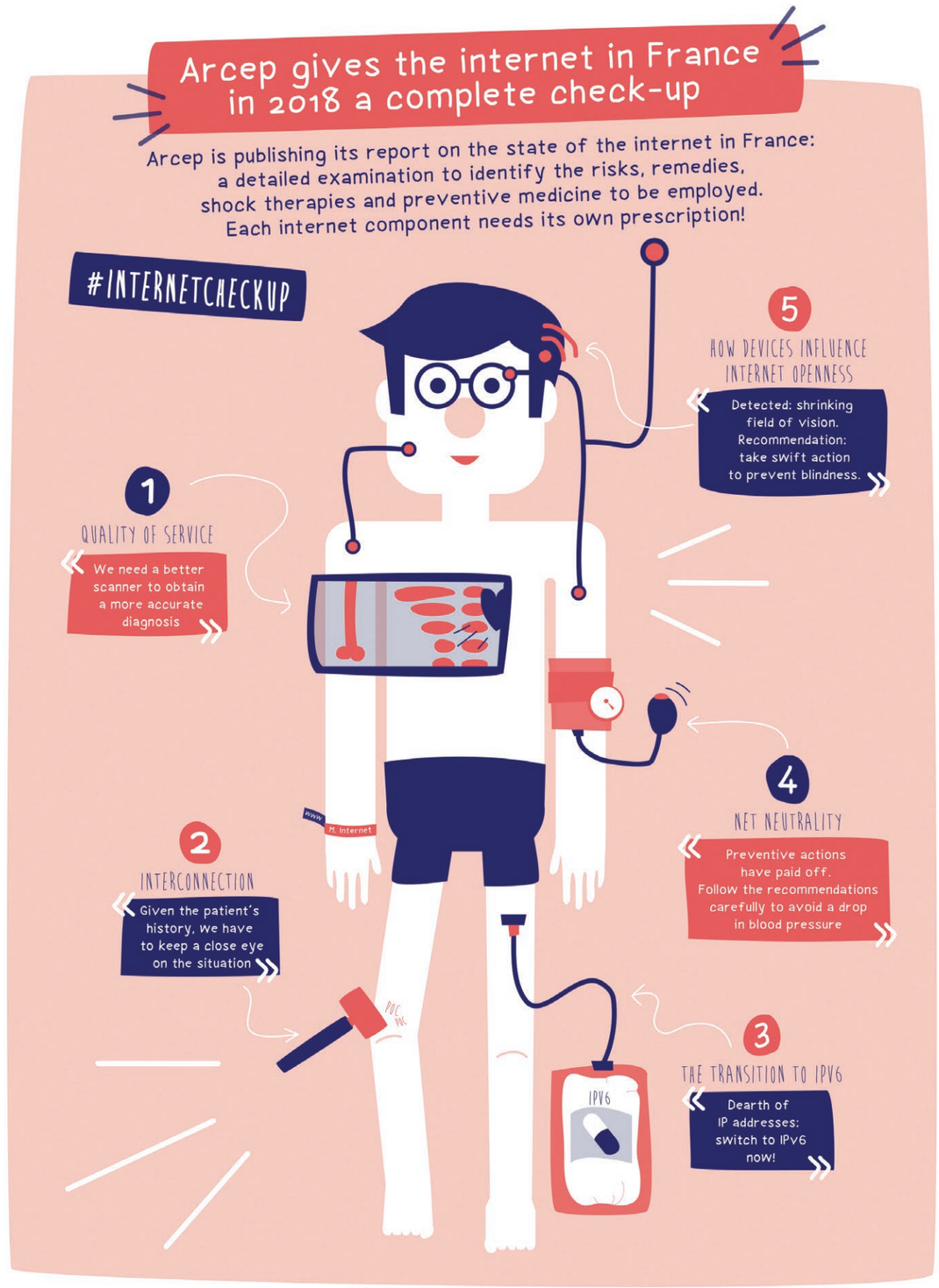
Bonus: INTERCONNECTION FOR DUMMIES

3 THE TRANSITION TO IPV6

The ongoing proliferation of connected products will drain the available stock of IPv4 addresses by 2021. Any delay in France's transition to IPv6 will erect a significant barrier to entry for market newcomers, and would split the internet's development in two - with IPv4 on the one side and IPv6 on the other - severely hampering businesses' ability to compete. Arcep is publishing a scorecard to galvanise the ecosystem: for instance, only two of the top four ISPs have a substantial number of activated IPv6 customers. Arcep will be hosting several "IPv6" workshops to give market players involved in the transition a chance to share their experiences.

Key figure: **2021** estimated year when IPv4 addresses will run out.

Bonus: ISP RANKINGS in Arcep's scorecard on the transition to IPv6



4 NET NEUTRALITY

In late 2017, the United States challenged the idea of protecting net neutrality. In Europe, in the interests of freedom of information, freedom of expression and freedom of enterprise, Arcep and its counterparts continue to implement the Open Internet regulation. France is reaping the benefits of the proactive dialogue that it began with stakeholders in 2016, while working to ensure the ecosystem keeps its eye on the ball, and access providers adjust their behaviour, through case-by-case analysis. Launched in 2017, the "J'alerte l'Arcep" user reporting platform uses crowdsourcing to keep the regulator informed. Arcep is also contributing to the development of traffic management detection tools.

Key figure: **367** neutrality-related reports from users since October 2017 on "J'alerte l'Arcep"

Bonus: EVERYTHING YOU NEED TO KNOW about the net neutrality debate

5 HOW DEVICES INFLUENCE INTERNET OPENNESS

With the introduction of European net neutrality regulation, Arcep can enforce it on the networks. But there is a weak link at the end of the chain: devices. Smartphones, voice assistants, tablets... all restrict internet openness and lock users' into their operating systems, their browsers and their app stores.
A series of meetings and workshops helped achieve a detailed analysis of these findings, and in mapping out very concrete courses of action, from improving transparency to having the regulator take direct action.

Key figure: **12** COURSES OF ACTION

Bonus: **1** COMIC STRIP SYNOPSIS of the Arcep report, "Devices: the weak link in open internet access"

PART 1

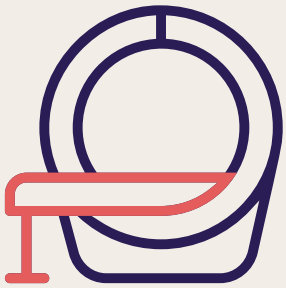
ENSURING THE INTERNET FUNCTIONS PROPERLY

Given how central the Internet has become to society, it is vital to guarantee that its constituent networks function properly.
This is why Arcep supervises the Internet ecosystem, to ensure that progress continues to be made in measuring performance and quality of service, in monitoring the data interconnection market's development, and in furthering the transition to IPv6.

1. Improving Internet quality of service measurement

ARCEP'S PRESCRIPTION

A better scanner is needed to obtain a more accurate diagnosis



How healthy is quality of service 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 are indicators required to perform this assessment, but relative measurements are more relevant than absolute ones. A connection speed [4] that may have been entirely satisfactory a few years ago no longer enables certain uses that have appeared since then. To evaluate how well France is performing on Internet service quality, an interesting first step would be to take a look at the analyses that seek to compare the situation in the different European countries.

1. A NEED TO CHARACTERISE THE MEASURED ENVIRONMENT AND FOR TRANSPARENCY ON THE ADOPTED METHODOLOGY

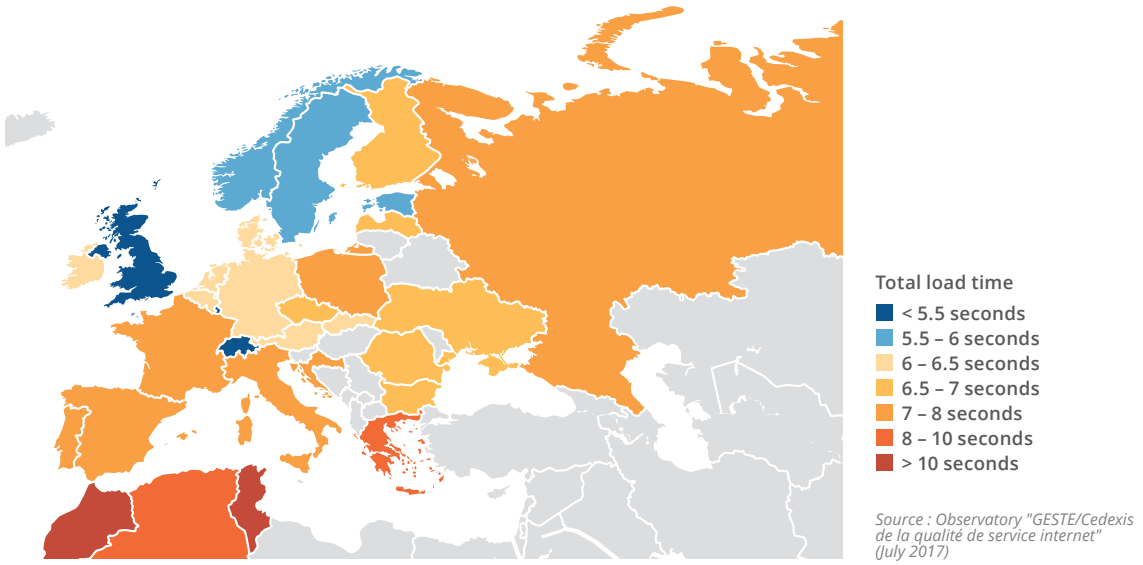
There are two main types of observatory around the world: those based on direct measurements and those based on statistics (e.g. percentage of Internet subscriptions that are broadband) such as the European Commission's *Digital Economy and Society Index*[5] or the Organization for Economic Co-operation and Development's (OECD) *Broadband Portal*Portal. Instructive in many respects, these scoreboards are devoted more to national coverage than to quality of service issues – a topic that is addressed in the Arcep report on smart territories[6], and

[4] See lexicon.
[5] *The Digital Economy and Society Index* (DESI) : https://ec.europa.eu/digital-single-market/en/desi
[6] www.arcep.fr/graco

will thus not be examined here. It should also be noted that scoreboards on Internet quality of service based on actual measurements reflect the average quality of the connections that were tested, regardless of the number of lines deployed across the country.

One such observatory is the one devoted to measuring Internet quality of service on fixed networks, run by GESTE, a consortium of content and service providers. It puts France in the bottom half of the rankings in terms of average web page load times.

GESTE OBSERVATORY[7]



Source : Observatory "GESTE/Cedexis de la qualité de service internet" (July 2017)

Two points warrant being made here. First, the web pages chosen to perform the speed tests are from GESTE members' websites. This scoreboard can therefore not provide any conclusions about quality of service for the Internet as a whole. Moreover, it is currently impossible for testing tools to qualify the fixed access technology (fibre, ADSL, etc.) on which the tests were performed. Observatories are thus forced to aggregate measurements from all of the technologies combined, which can give an idea of the technology mix in the country (and so the choices that have been made, e.g. to upgrade cable networks or give priority to fibre rollouts) but not an accurate measure of the quality of these connections for any one access technology in particular. The problem is the same when it comes to publishing a comparison of operators' findings: by way of illustration, an operator whose base is made up solely of fibre connections will top the rankings, even though its fibre products may not necessarily be of a higher quality than the access products sold by its competitors that also use cable or ADSL.

Measuring Internet quality of service on mobile networks is an easier matter. As the following 4G speed comparison scorecard from the UK's OpenSignal demonstrates, crowdsourced[8] mobile testing apps are able to identify the technology being employed. This scorecard sets itself the tasks of comparing countries from across the globe on two main metrics: the proportion of time that users have access to a 4G network (and so looking at connectivity, which is very closely bound up with coverage) and 4G download connection speeds. Here again, France fares relatively poorly in its results for Q4 2017[9]: ranking 36th out of 77, with a 4G download speed of 25 Mbit/s.

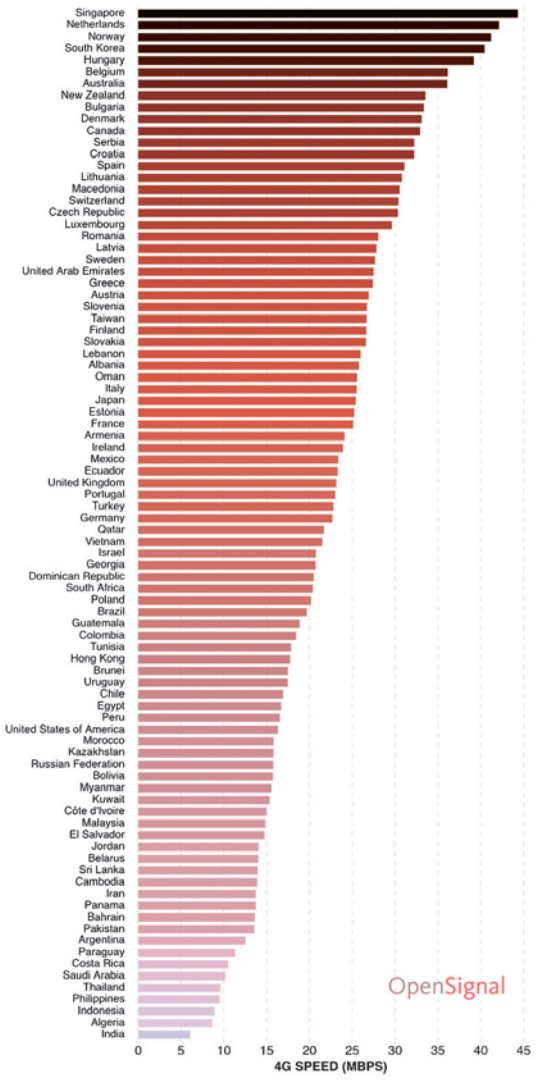
[7] The base map of the original diagram has been modified.
[8] Crowdsourcing tools are mechanisms that centralise QoS and/or QoE measurements taken by actual users.
[9] https://opensignal.com/reports/2018/02/state-of-lte#coverage-lte

We may be surprised to find that other scoreboards provide significantly different average 4G speeds for France than the one given below. One case in point is the nPerf speed test that revealed a speed of around 33 Mbit/s[10] which would put France in 11th spot in the OpenSignal rankings. This disparity is not surprising, however: studies conducted by Arcep in 2017 revealed that the choice of methodology used by the testing tools had a considerable impact on the results[11]. The location of the test server, the indicator testing protocol, as well as the number and representativeness of the measures taken all had a direct influence on the measured value.

If the diversity of the crowdsourcing ecosystem is beneficial, it nevertheless needs to be coupled with a requirement of transparency over the methodological choices made, so that any third party is able to explain the differences observed between two tools, and to question the relevance of making one choice over another. In addition, there are already plans for co-construction work to be done on characterising the fixed network access technology being used, so that the results can be delivered in more useable formats.

Testing tools could therefore be more finely tuned, to be able to obtain a more accurate assessment of Internet quality of service in France and, if necessary, to recommend the most suitable remedies.

OBSERVATORY OPEN SIGNAL



Source: Open Signal - The State of LTE (February 2018)

[10] Number calculated based on data published by nPerf in the following report: https://media.nperf.com/files/publications/FR/2018-01-16_Barometre-connections-mobiles-metropole-nPerf-2017-T4.pdf. Average 4G speed, all operators combined: 0.24 x 21.5 + 0.27 x 39 + 0.25 x 37.3 + 0.24 x 31.3 = 32.5 Mbit/s.

[11] https://www.arcep.fr/uploads/tx_gspublication/rapport-etat-internet-france-2017-mai2017.pdf, p. 28 to 40.

A HIGH QUALITY INTERNET TO SUPPORT INNOVATION

Jonathan ARDOUIN,
Country Manager, France, **KRY**

Remote medical consultations are increasingly prevalent across Europe. They are helping to overcome permanent care issues and medical deserts that France also has to deal with. This new channel of care is still only nascent in France, as the 2018 Social Security Financing Act has only just enshrined the ability to be reimbursed for remote medical consultations.

KRY is the leading provider of video medical visits in France. Now in our third year of operation, we conduct close to 3% of all first aid consultations *via* video in Sweden, a country where video consultations are already a common practice and reimbursed by national health insurance. The hindsight we have gained from our experience in Sweden proves that video is the best channel – better than the phone or sending photos – for remote consultations, and can guarantee the same quality as an in-person visit. It allows the medical practitioner to establish ties with the patient and confidently make a diagnosis.

"TO BENEFIT FULLY FROM VIDEO CONSULTATIONS, A FAST AND STABLE INTERNET CONNECTION IS CRUCIAL FOR BOTH THE PATIENTS AND THE DOCTORS. TODAY IN FRANCE, IT IS COMMON FOR THIS TYPE OF CONSULT TO END ON THE PHONE BECAUSE THE INTERNET CONNECTION IS NOT FAST ENOUGH."

The one proviso, however, is that the video needs to be of high enough quality to allow the doctor to identify the patient's visible symptoms with certainty. To benefit fully from video consultations, a fast and stable Internet connection is crucial for both the patients and the doctors. Today in France, it is common for this type of consult to end on the phone because the Internet connection is not fast enough. And this even in major cities, and with users who have a "high-speed" connection.

The implication then is that a poor quality Internet service equals lost opportunities for patients: in areas where connections are too slow, patients will be deprived of rapid access to care. Common pathologies, which can easily be diagnosed *via* video, will need to be rerouted to already overtaxed physical channels (doctors' office, clinics, A&E). Having a high quality fixed Internet service is thus vital when it comes to telemedicine.

2. AN INNOVATIVE CO-CONSTRUCTION APPROACH

On 19 January 2016, Arcep presented the conclusions of its strategic review, and announced the implementation of data-driven regulation, a greater push for co-constructed regulation, and Arcep's development around a role of neutral expert on digital issues.

The work devoted to Internet quality of service is fully in line with this new modus operandi.

In this data-driven approach to regulation, Arcep wants to use information regarding quality to stimulate competition that is not based solely on price, but also on the quality of the services being sold, with a view to monetising network investments.

To be both more efficient and more relevant, Arcep is thus seeking to co-construct this regulation:

- On the one hand, with "the crowd" by giving every citizen the power to become a mini-regulator. This was the impetus behind the launch of the "J'alerte l'Arcep" platform in October 2017, through which any consumer can report problems with their Internet access to Arcep (see inset). In addition to reporting, users can also input the results of QoS tests performed on their line using crowdsourced tools, and so contribute to the data used when publishing benchmarks of ISPs' performance;
- and, on the other, through a partner-centric approach with the ecosystem's stakeholders, for both the reporting and testing aspects referred to above. In the area of reporting, in addition to launching its own platform Arcep is examining the possibly of initiating a data-sharing scheme with consumer protection advocates[12]. This "unbundling" of the reporting process could help dismantle existing silos, and drive a better, collective understanding of the issues at hand. Arcep's partner-centric approach to crowdsourced testing is described below.

Alongside these co-construction efforts, Arcep is working to develop its own tools for collecting measurements that can enhance the data from its partners' third-party tools. These projects are detailed in Section 3 of this Chapter.

FYI

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. The platform has logged 22,500 reports since it first launched. Of these reports, 68%* concern a quality or availability issue with fixed or mobile services. And, among them, two thirds concern the fixed market, and one third the mobile market.
This valuable feedback helps fuel the work that Arcep is doing on quantifying and identifying the problems that users are encountering, to then steer its actions towards the most appropriate solutions possible. It is on issues relating to Internet quality of service that the co-construction approach, the work being done on the BEREC tool and the monréseaumobile (my mobile network) scorecard described in Chapter 1, Section 3 come fully into play.

* Percentage obtained through reports logged between October 2017 and May 2018.

2.1. Bringing together stakeholders

Up until the end of 2016, Arcep's scorecard on the quality of fixed services was based on a system operating in a controlled environment. This type of testing was abandoned in early 2017 – largely because the real-life situations encountered by users were not being properly represented – and replaced by a system that would be based on crowdsourced testing tools.

The 2017 report on the state of the Internet in France presented the findings of the two studies that initiated the co-construction approach: the map of the ecosystem of the tools available in the marketplace, and a comparison of the results of different online testing tools. This report had stressed the need for a concerted community effort on several top priority issues. Arcep has since launched six courses of action as a direct result.

[12] In accordance with existing regulation, notably regarding data privacy.

To bring them to completion, **Arcep is acting as a neutral expert that brings the community together and fosters the work being done on matters of general interest.** These initiatives were carried out in collaboration with a wide spectrum of stakeholders from the crowdsourced metrology ecosystem[13]:

- testing tools: ASSIA, Case on IT (medUX), Cedexis, Directique, Ip-label, Gemalto, 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.

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

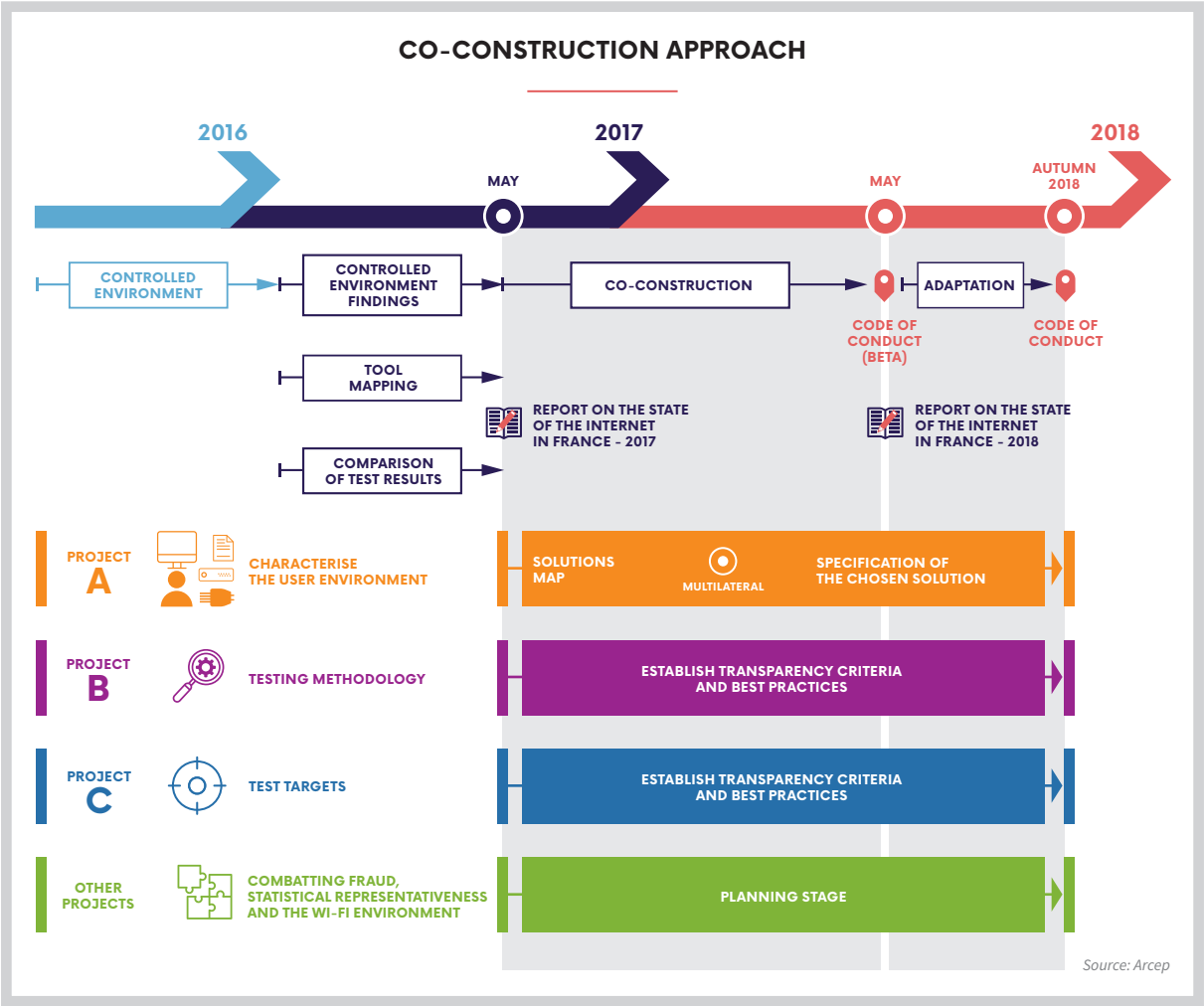
Alongside the working groups, Arcep also consulted with other national regulatory authorities (notably AGCOM, BnetzA, COMREG, Ofcom and RTR) to pool their experience in measuring the quality of fixed services.

The goal that cuts across all of these initiatives is to enable the tools to meet consumers' and the Authority's needs as fully as possible, in terms of obtaining information on quality of service on the fixed and mobile Internet.

To be more specific, Project A seeks to address the technical problem raised in the previous section, namely the lack of characterisation of the user environment when measuring the quality of fixed services. The other projects (B, C and those currently in the planning stage) address the need for greater transparency that was also identified in the previous section. In particular, they seek to establish a "code of conduct" for testing tools. This future code of conduct concerns two aspects: first, inviting the tools to back the publication of their results with a clear explanation of the methodological choices made, so that any outside party is able to understand the potential differences observed between tests performed with different tools. Second, to set out the best practices that are vital to obtaining reliable measurements. Although most of the choices that have been made have merit, some practices do seem more questionable, and warrant being modified.

The first version of the code of conduct will be published before the end of 2018. And it will evolve over time: every year, in theory, Arcep will publish successive, continually improved versions, which include not only changes to Projects A, B and C, but also the fruit of the projects that are currently in the planning stage.

A beta version of the maiden code of conduct can be found in Annex 1. Stakeholders are heartily encouraged to share any remaining feedback on the matter with Arcep before 15 July 2018.



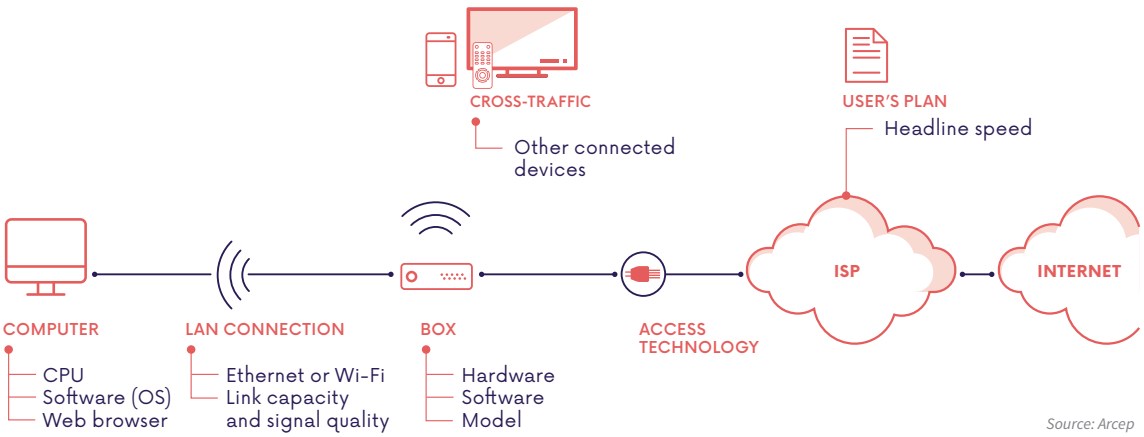
2.2. Project A: Characterising the user environment

The project dedicated to characterising the user environment on a fixed line, and notably the technology being used, has a dual purpose: first, it is vital to being able to create a truly relevant scorecard for consumers and, second, it is of significant value when establishing an accurate diagnosis of a quality of service issue. For instance, it is important to know whether a poor connection is due to the ISP's access network, the Wi-Fi network's quality or the simultaneous use of other connected devices on the local network when performing the test.

The following diagram recaps the main properties of the user environment that will influence the test results.

The current characterisation of the different elements varies depending on the type of testing tool being used. Some hardware probes[14] are, for instance, capable of testing a LAN[15] connection and even estimating cross-traffic[16] on the local network. On the flipside, while it is true that web testers[17] can be rapidly deployed on a large scale, they are only able to detail a small number of elements (web browser used, etc.).

THE USER ENVIRONMENT:
A SET OF CHARACTERISTICS WITH HIGH IMPACT ON MEASUREMENTS

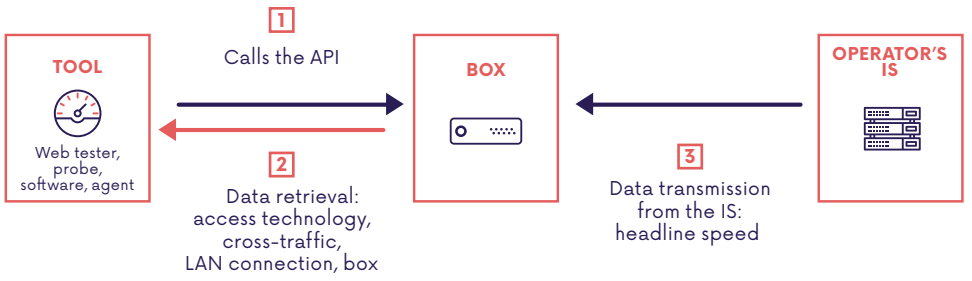


Source: Arcep

14/15/16/17 See lexicon.

This project centred around the work coordinated by Arcep involving testing tools, ISPs and academia. The community began with an exploratory phase during which seven solutions attempting to satisfy the requirements were examined. One proposed path was to characterise the measurements through a questionnaire completed by the person performing the test, and more or less guided by the information given ahead of time by the ISPs (e.g. list of plans available for a given technology) or by an API[18] deployed between the tools and ISPs' information systems (IS). At this stage in the discussions, it appears that another solution may seem to offer the best compromise between exhaustiveness, reliability, security and development costs for most stakeholders. Arcep thanks them for their dynamic and constructive contributions.

AN "ACCES ID CARD" API FOR CHARACTERISING THE USER ENVIRONMENT



Source : Arcep

A diagram of the solution is presented above. When a test is performed, the tool (whether a web tester, hardware probe, software agent on a box, software that can be installed on a device) simultaneously sends a request to the "access ID card" API located on the tester's box [1]. If the tool queries this API, the box will send it the characteristics of the line at the time of testing [2]. Most of the information is available natively on the box: access technology, information on the LAN connection and the box and — for most ISPs – a WAN[19] port traffic counter that makes it possible to detect cross-traffic. Other properties, such as headline speed, are not available locally on the box but on the operator's IS: through another API, if the ISP transmits them to the box often enough to ensure that the information is always up to date [3]. It should be noted that operators' IS – the system at the heart of their internal processes' operation which may not be very reactive – never interacts directly with the tools.

Moreover, this solution is invisible to the person performing the test, and in no way diminishes the user experience. Further details on the solution's technical features can be found in Annex 2.

This ambitious project should thus enable the tools used to test fixed networks to achieve degrees of characterisation that are virtually equivalent to those obtained natively by mobile apps – which are already capable of identifying the access network (2G, 3G or 4G), for instance, and the strength of the signal since they are tied directly to the mobile operating system (OS) and there is no intermediary between the device and the network – contrary to a fixed network where the connection is supplied through a box.

By establishing API specifications and the list of tools authorised to access them, in concert with stakeholders, Arcep will continue to create the environment of trust needed for collaboration with the different players. Taking the State-as-a-platform approach to the fullest extent, Arcep will thus fulfil its mandate to inform consumers while leaving it up to its partners to develop innovations based on the information that has been collected.

[18/19] See lexicon.

WEB TESTERS' CHARACTERISATION OF THE USER ENVIRONMENT

Renaud KERADEC,
CEO/CTO and Founder, **nPERF SAS**

The ability to characterise the user environment is an important issue for nPerf. It will be a positive thing for everyone who uses nPerf tools. Operators will benefit from having more complete data, which will enable a better diagnosis of abnormal situations. nPerf will be able to publish more detailed studies with more relevant comparisons of the performances provided by the different operators, according to the technologies available to French Internet users. End users will thus have a clearer picture of the quality of the service provided by the different ISPs. nPerf will also be able to simply tell users whether they are actually obtaining their ISP's headline speed!
At nPerf, we are certain that the solution that was co-created with Arcep, testing tool designers and operators will eventually deliver all of the elements needed to better characterise the collected data, to everyone's benefit.

Adam ALEXANDER,
VP Strategic Partnerships, **OOKLA LLC**

Ookla, the company behind Speedtest, realizes the importance for consumers, regulators and service providers to understand the performance of consumer Internet access through accurate benchmarking. As part of our efforts with Arcep, we've focused on the value in characterizing the end user's environment to ensure speed and quality benchmarking relative to the subscription offered to the end user, and the need to isolate the end user's environment to ensure the service provider is being appropriately measured based on factors within their control.
Ookla sees the value in the proposed solution of being able to call an API to reconcile the technical and the end user's subscription speed in reconciling performance of a connection relative to the consumer's expectations. While there is an investment required by both the service provider to supply the API, and by Ookla to consume the API, we believe the richness of the data and accuracy of the benchmarking to be a net positive return on investment.

Arnaud BÉCART,
Senior Solutions Engineer, **CEDEXIS (NOW PART OF CITRIX)**

Cedexis – which was recently acquired by Citrix – measures the performance of cloud and CDN platforms through over a billion user sessions a day. This actual crowdsourced data enable these platforms to improve their network connectivity. They can also be used by ISPs to measure and compare their Internet users' ability to access platforms such as Google, Amazon or Akamai.
GeoIP bases make it possible to identify the Internet user's network and region, but are not terribly precise with regard to the type of network (fixed, mobile) or the access technology (3G, 4G, FttH, xDSL, etc.). The introduction of an API that provides this information would be very useful for distinguishing access times (DNS, TCP, latency or bitrate). Although it offers a technical response to the lack of characterisation, the solution proposed by Arcep involves a number of technical constraints as it requires developments from the operator (API between its IS and the box, and API in the box) and for the testing tool (integration of the box's API).
Cedexis believes that a direct interface (API between operators' IS and the tools' IS) would be simpler to develop, maintain and reproduce in other countries as it does not require any alterations to be made to the box or to the tool. Operators would be able to implement a secured and automated exchange with our servers, that we would be able to integrate easily into our platform, given that this approach does not require any major adjustment to our tool that collects more than 14 billion measurements a day.
Alongside this project, we are examining other characterisation methods such as API Network Information and direct exchanges with ISPs.

2.3. Project B: Testing methodologies

As explained in the findings of the study on "mapping tools", every choice of protocol serves a different purpose: the current expansion is therefore a good thing for the ecosystem. To give an example: testing single thread speeds, i.e. with a single TCP connection, measures the speed one can hope to achieve when loading a web page, whereas a multithread measurement (with several parallel TCP connections) tests a saturated line and so comes closer to measuring capacity.

However, as mentioned earlier, it seems vital that, when publishing the results of a test, there needs to be transparency over the methodology used, so that any third party is able to explain the results obtained. It is also useful to seek to eradicate practices that are likely to introduce a heavy bias. To this end, Arcep has instigated work on a code of conduct for those players involved in measuring quality of service and quality of experience on the Internet, which contains two dimensions:

- a list of "transparency criteria" which should accompany all results publications;
- a list of best practices that Arcep would like to see associated with certain criteria in particular.

To define these transparency criteria and best practices for speed and latency testing methodologies, Arcep relied on the *"Net Neutrality Regulatory Assessment Methodology"*[20] report that BEREC published in October 2017 and which contains recommendations on the methodologies to be used to test these technical indicators.

Arcep plans on including transparency criteria and best practices regarding web page load times and video streaming quality in the code of conduct, even if BEREC did not issue any guidelines on the – more complex – process of measuring these usage indicators. As mentioned here, in the combined views of UFC and INC, these indicators are particularly worthwhile: first, they speak more to consumers and, second, they make it possible to monitor the actual quality of increasingly demanding new applications.

The beta versions of these two lists can be found in Annex 1.

© Fotolia/alfa27, Fotolia/Julien Eichinger

[20] http://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/methodologies/7295-berec-net-neutrality-regulatory-assessment-methodology

QUALITY OF EXPERIENCE: ESSENTIAL INFORMATION FOR CONSUMERS

Thierry MARTIN,
Study engineer at the Centre for comparative testing,
INSTITUT NATIONAL DE LA CONSOMMATION

INC, the publisher of *"60 Millions de consommateurs"* (60 million consumers), has been committed to improving the quality of Internet access services since 1990, by publishing a benchmark of ISP tests in its magazine. The INC's testing centre designed testing methodologies after having concluded in early 2000 that measurements taken in a controlled environment did not sufficiently reflect that diversity of user experiences. The slew of mail from customers who were dissatisfied with their Internet access only confirmed this conclusion. This approach led us to offer more personalised information that takes more systematic account of the "felt user experience". Our solution, which has been available since 2002, is the Internet connection tester that allows users to test the performance of their fixed Internet connection. Over time, the unique speed tester has been fleshed out with a series of performance indicators: download speed, web browsing, video streaming, etc.

Pushed by informed consumers with growing connectivity needs, INC has been working for two years on overhauling its tools to achieve more reliable data collection on performance indicators. But ensuring the reliability of the measurements is only one of the purposes of our work, whose ultimate aim is to help informed consumers choose their access products thanks to comprehensible and truly useful information.

Other ideas for services are already being explored, designed to help consumers in their connected lives – a sign that INC continues to work for and with informed consumers.

Antoine AUTIER,
Deputy head of the study department, **UFC-QUE CHOISIR**

When a consumer is choosing their Internet service provider or mobile service operator, price is naturally a major consideration. But it is far from being the only one: quality of service remains an essential criterion.

The indicators that interest consumers most are of course those relating to usage. A consumer that uses a video streaming service often will thus pay a great deal of attention to the performance offered on this type of service. But technical indicators matter as well, especially when it comes to the fixed Internet whose market is not known for its liquidity. A consumer could thus be especially mindful of speed to the extent that, a sizeable disparity between the speeds being offered today, which for now makes no real difference, will very likely have a real impact on the quality of the user experience on future bandwidth-hungry services.

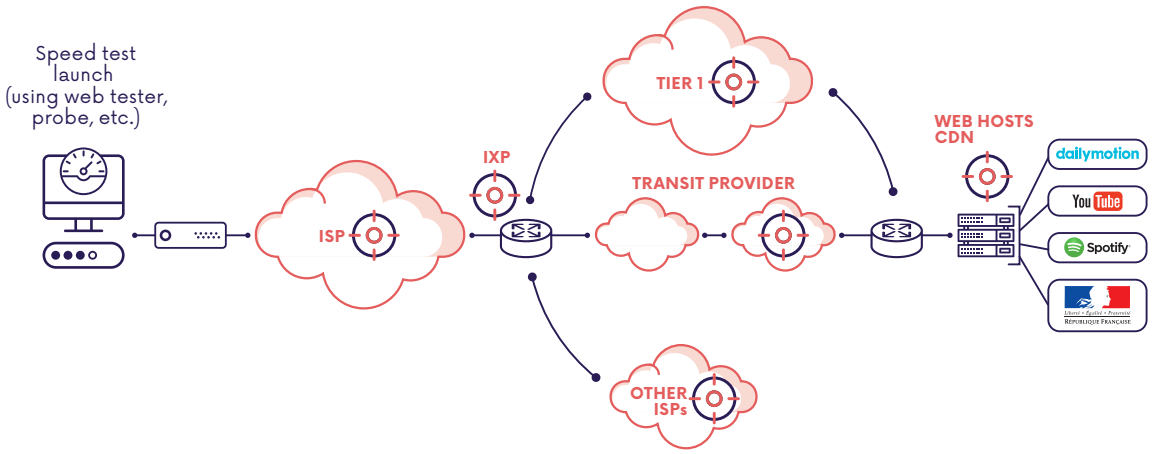
As concerns the production of indicators, and even if UFC-Que Choisir may not have always agreed with Arcep's choices of methodology, it should be emphasised that, in the current environment, Arcep's publications on mobile services are a reliable and illuminating source of reference for consumers.

The situation is very different with fixed services, where we find a relative dearth of indicators being produced, both technical and especially use-related ones. If this can be attributed to the existence of a great many biases, it must not discourage any future initiatives, given what is at stake for consumers.

This is why UFC-Que Choisir recently launched its observatory for fixed Internet quality. Based on the results collected from a panel of testers, this observatory aims to establish benchmark indicators for consumers, to enable them to make informed choices when selecting their ISP.

2.4. Project C: Test servers

THE TEST SERVERS' LOCATION: A CHOICE THAT STRONGLY IMPACTS THE RESULTS



Source: Arcep

In addition to methodologies, another factor that has a considerable impact on results is the server used to perform the test, otherwise known as the test target or target server. The bitrate being measured is therefore the bitrate available between the test device (computer, probe or other) and the target server.

As detailed in the following 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: 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 scarcely 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 1 [21] 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).

Given the potential impact of the test target's properties (location, as well as server capacity, etc.), transparency criteria have also been included in the first draft of the code of conduct (cf. Annex 1). As with project B, these criteria are accompanied by best practices for controlling the impact that test targets have on QoS measurements.

[21] Tier 1 networks are the networks that are capable of interconnecting directly with any other Internet network. See lexicon.

2.5. Other projects: combatting fraud, statistical representativeness and the Wi-Fi environment

As an adjunct to these three projects, work devoted to combatting fraud, to the statistical representativeness of tests and the impact of the Wi-Fi environment is also being undertaken.

Once they have progressed to a certain point, these three projects are also meant to enhance the code of conduct, whose beta version can be found in the annexes. The project on combatting fraud is vital to achieving reliable measurements, notably with a view to detecting and excluding automatic tests. Following through on a proposal made by several of the ecosystem's players, Arcep is examining the possibility of a charter, whereby the signatories would commit to complying with a certain code of ethics.

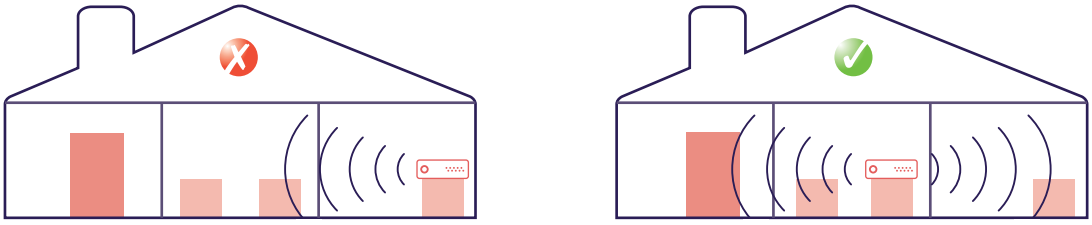
Particular attention should also be given to the number and profile of the users performing the tests, to guarantee the statistical representativeness of the resulting measurements. Several solutions have already been put into place by certain players, such as test drive campaigns that seek to make up for the lack of tests being performed in certain locations, or the creation of more advanced statistical models.

Lastly, because Wi-Fi can have a significant impact on users' actual connection speed, it is important to work on taking it into account and diminishing its impact. As a first step, Arcep believed it would be useful to list several best practices for consumers on how to optimise their Wi-Fi signal (see next page).

FIVE TIPS FOR IMPROVING YOUR WI-FI SIGNAL QUALITY

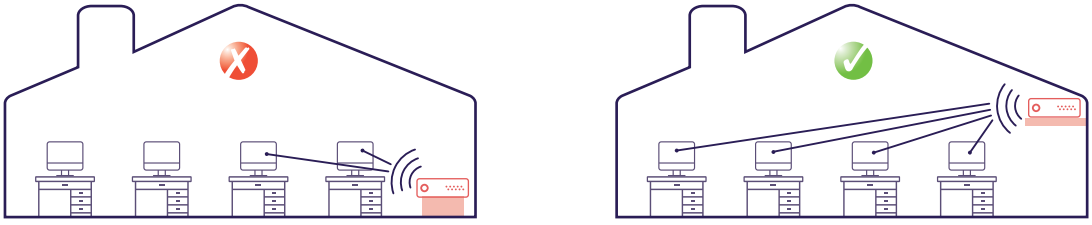
1 PLACE THE BOX IN A CENTRAL ROOM IN THE HOME

It is recommended that the box be placed in a central location in the home to limit the number of obstacles that the Wi-Fi signal encounters when connecting to devices. Walls weaken the wireless signal and substantially decrease the internet speed available to the devices located in the most distant rooms. Placing the box at one end of the home or in a closed room therefore prevents you from getting the most out of the Wi-Fi network.



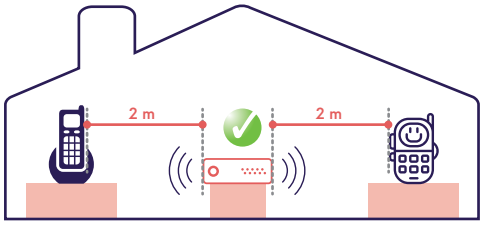
2 PUT THE BOX IN THE MOST UNCLUTTERED LOCATION POSSIBLE

For the same reasons, it is recommended to place the box in as uncluttered a location as possible, ideally high off the ground. Putting the box on the ground, between books, in a TV cabinet or close to tall furniture will diminish the Wi-Fi signal and the user experience.



3 KEEP THE BOX AWAY FROM OTHER WIRELESS EQUIPMENT

To achieve your connection's maximum capacity, it is also recommended to leave a space of around two metres between the box and any other wireless equipment, such as the base station for a wireless phone, a baby monitor, microwave oven, etc. This will limit any interference between the different radio waves and the Wi-Fi signal is optimised.



4 OPT FOR 5 GHZ WI-FI FREQUENCIES

For boxes that are capable of transmitting at frequencies of 2.4 GHz and 5 GHZ (which is the case with the latest generation of boxes), it is recommended to configure the box to transmit on 5 GHz frequencies.

5 WHEN BUYING A NEW COMPUTER, MAKE SURE IT IS WI-FI 802.11 AC COMPATIBLE

It is recommended to choose computers that are compatible with the 802.11 standard. This standard is more powerful than 802.11n, which also exists on certain new computers. Moreover, there is no risk of incompatibility with the box since it is backwards compatible with all of the older standards.

Source: Arcep

HARDWARE PROBES AND WI-FI PERFORMANCE MEASUREMENT

Luis MOLINA,
Co-founder, **CASE ON IT**

Fixed Internet networks enable Ethernet and Wi-Fi connections with technically different properties, and different quality of service potential. Wi-Fi connections are facing two main difficulties: interference between channels which are aggravated by proximity, and a weakened signal inside the home caused by walls and obstacles.

This is why MedUX designed probes equipped with both an Ethernet and a Wi-Fi 802.11 a/b/g/n/ac interface. This makes it possible to measure Ethernet and Wi-Fi quality of service concurrently, in real time.

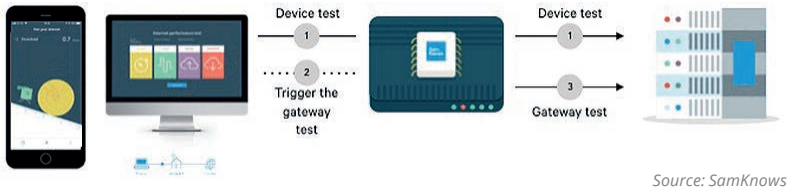
MedUX 2018 seeks to create an ecosystem that improves fixed sensors with mobile apps. The apps could thus: talk to the probe to make local adjustments, run Wi-Fi coverage checks inside the home, extract Wi-Fi performance indicators (channel and neighbouring channel use), etc.

Because most users employ Wi-Fi on their fixed network, MedUX addresses their needs with a combination of targeted Wi-Fi measurements, and additional ones provided by the ecosystem. Fully covering the end user's home, MedUX can thus obtain an exhaustive measurement of the impact of Wi-Fi quality on both technical and use-related indicators.

Sam CRAWFORD,
CTO and founder, **SamKnows**

In recent years there has been a significant rise in both Internet access speeds and the number of Wi-Fi connected devices in the home that connect to the Internet. However, the quality of in-home connectivity has not kept pace with this trend; instead factors within the home are often the cause of Internet performance or reliability issues for users. Indeed, even the latest generation Wi-Fi networks and smartphones will not be able to saturate a 1Gbps link unless under perfect lab conditions. Moreover, there is often no easy way for a user or even the ISP to reliably discern whether the issue is caused by factors inside or outside of the home.

SamKnows has developed a two-step performance test that actively measures performance from the user's device to the Internet and performance from the user's SamKnows-enabled router (or Whitebox) to the Internet.



Source: SamKnows

"FACTORS WITHIN THE HOME ARE OFTEN THE CAUSE OF INTERNET PERFORMANCE OR RELIABILITY ISSUES FOR USERS."

These two sets of results can be paired together and used to infer whether the bottleneck lies in the user's device, in the home network, or in their Internet connection. This information can be used for a number of options, including driving a support workflow, which allows the user to self-diagnose and resolve an in-home issue, without ever contacting their ISP. These performance measurements are also not constrained to just speed tests; any of the SamKnows metrics can be compared in this fashion, including the video streaming and gaming tests.

WI-FI PERFORMANCE MEASUREMENT

Dr John CIOFFI,
President and CEO, **ASSIA Inc**

Superfast access is becoming a reality for a growing number of people. Skyrocketing access speeds are going hand in hand with an increase in the number of wireless devices connected to the networks. For fixed networks, this revolution has meant new constraints on home networks that are relying more and more heavily on Wi-Fi, which has thus become a vital ingredient in the quality of the user experience.

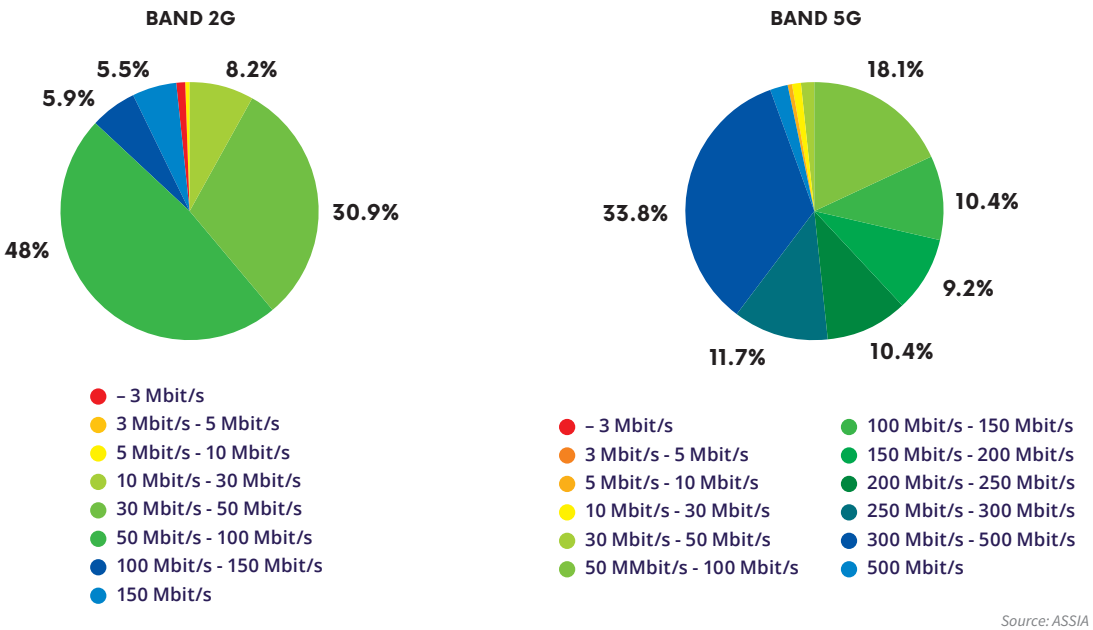
Studies that ASSIA has conducted on its customers' networks reveal that 30% of the lines on the 2.4 GHZ Wi-Fi band suffer from speed/latency issues at the Wi-Fi station/access point, which affects users. This figure drops to 10% when using the 5GHZ band. On the 2.4 GHZ band, 40% of base stations provide a bitrate of less than 50Mbit/s (1% of base stations run at below 3 Mbit/s); on the 5 GHZ band, this figure drops to 20%. At the same time, we have observed that, when employing the same Wi-Fi technology, users' devices play a key role in determining the available Wi-Fi speed, and that performances will vary considerably depending on the hardware being employed.

Over the past 15 years, the way we "consume" the Internet at home has changed dramatically: from a desktop computer connected to a modem with an Ethernet cable, we now have a plethora of connected devices, virtually all of which use Wi-Fi (an average of 12 per home in North America).

The methods used to measure quality of service based on speed also need to take these realities into account, and especially the impact that Wi-Fi has on the results.

For more information: https://www.assia-inc.com/defining-next-wi-fi-revolution/

SPEEDS MEASURED BY ASSIA ACCORDING TO WI-FI FREQUENCY BAND



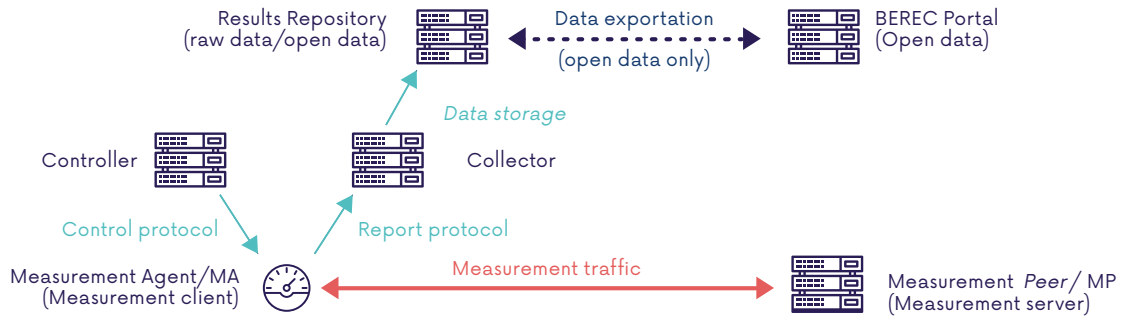
Source: ASSIA

3. WORK BEING DONE ON DEVELOPING COMPLEMENTARY TOOLS IN-HOUSE

3.1. BEREC's common tool

In October 2017, BEREC published two reports that laid the groundwork for a common tool for measuring quality of service: *"Net neutrality regulatory assessment methodology"*[22] which provides recommendations on methodologies for assessing the different QoS indicators, and *"Net neutrality measurement tool specification"*[23], which specifies the tool's architecture.

SPECIFICATION OF THE NET NEUTRALITY QoS MEASURING TOOL ARCHITECTURE



Source: Net neutrality regulatory assessment methodology

Following through on this work, in March 2018 BEREC issued a call to tender to select the service provider that would develop the tool.

The specifications include three essential components: an open source software programme for measuring the different indicators, and which could be used by national regulatory authorities (NRA) wanting to implement the tool; a reference measurement tool that would execute the open source software and deliver the results as open data (the proof of concept that will serve as the reference implementation); and a BEREC portal that will collect and process the results of the measurements, to then generate statistics, maps and reports.

The exact properties of the tool will depend on the options proposed by the selected vendor. At the very least, the BEREC tool will include a mobile application (Android and iOS) and a web tester capable of measuring the usual technical indicators (speed, latency, etc.) as well as any port blocking. If the vendor does propose to do so, the tool could also measure key performance indicators (KPI) such as web page load time and video streaming quality, along with net neutrality-related indicators such as proxy detection and DNS manipulation[24]. An installable version of the tool (Windows, Mac and/or Linux) may also be made available.

The development of all three components is due to be complete in Q3 2019, after which NRAs could, if they choose to do so, implement the tool in their country, after having adapted it to their national market (translated the user interface, installed local test servers, added additional indicators to test, etc.).

A sizeable percentage of NRAs, of which some already have a national measurement system in place, see great merit in adopting this tool. Among other things, it would guarantee a harmonised measurement methodology in the different European countries, and provide cross-border measurements that would be more representative of actual Internet connectivity (which is

[22] http://www.berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/methodologies/7295-berec-net-neutrality-regulatory-assessment-methodology
[23] http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/7296-net-neutrality-measurement-tool-specification
[24] *Domain Name System;* See lexicon.

rarely only national) across Europe. It would also facilitate knowledge and expertise sharing between the different NRAs that have adopted the tool.

However, as with existing crowdsourced tools for fixed networks, there is a real lack of characterisation of the user environment. Project A in Arcep's co-construction efforts would thus prove vital here, and serve to complement the work being done on the BEREC tool, which Arcep is also invested in.

FYI

Operators' transparency obligations

Article 4.1 d) of the European Open Internet Regulation* requires ISPs to provide a "clear and comprehensible explanation" of any upload and download speed parameters attached to their Internet access plans. In accordance with the Regulation, ISPs are thus required to include, for fixed networks: the minimum, usually available and maximum bitrates included in their contracts, and for mobile networks, maximum bitrates.
BEREC guidelines for NRAs' implementation of the European Regulation provide an initial set of details on defining each type of bitrate. To achieve harmonised commitments from ISPs, Arcep and France's Directorate-General for Competition, Consumer Affairs and Fraud Repression (DGCCRF) are working on the practical implementation of these provisions. At the same time, Arcep is examining the possibility of an oversight mechanism for assessing disparities between actual performances and the performances advertised in the contract.**

* https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32015R2120&from=FR

** https://www.arcep.fr/fileadmin/uploads/tx_gspublication/2016-10-21-Lignes-directrices-NN-version-francaise.pdf

3.2. Arcep's monitoring of mobile QoS

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 the city, in rural areas, on different forms of transport, etc.), and for the most popular services (calling, texting, web browsing, video streaming, file downloads, etc..). In 2017, 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).

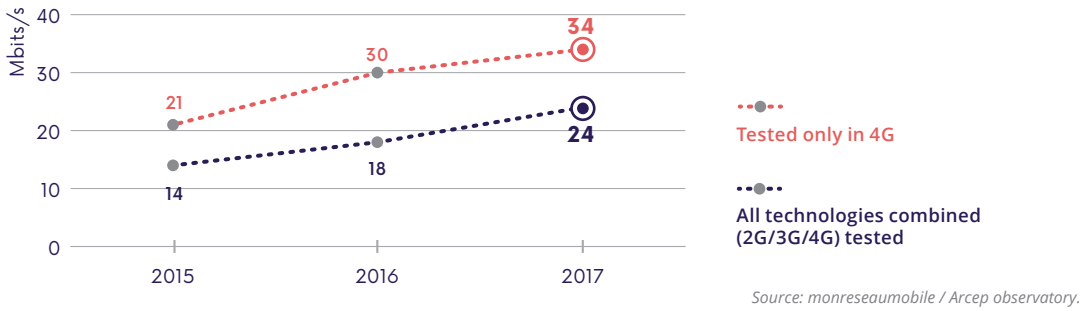
To make the most of these findings, in 2017 Arcep launched a new, interactive mapping tool called monreseaumobile.fr (my mobile network), which allows users to view all of the data collected through this QoS audit, as well as data on operators' coverage. If operators' coverage maps – which are produced based on digital simulations – provide necessary information for the country as a whole, they only provide very basic information on the actual availability of mobile services in France. These maps are completed by QoS data obtained under real life conditions: they do not provide an exhaustive picture of the country, but do make it possible to obtain an accurate view of the level of service provide by each operator in the tested locations.

Arcep's annual audit also makes it possible to track the progress that each of the operators' networks has made in improving service quality. Arcep's monitoring of 4G performance has proven especially vital here: at the end of 2017, 4G users accounted for around 90%[25] of total mobile data traffic. To keep pace with the explosion of mobile traffic, 4G has indeed become the lynchpin of operators' investments.

[25] Data taken from the scorecard on electronic communications in France for Q4 2017: https://www.arcep.fr/index.php?id=13921

The average download speeds measured on mobile networks have been increasing steadily over time. In 2017, they stood at 24 Mbit/s all technologies (2G, 3G, 4G) and all operators combined. 4G speeds are considerably faster: 34 Mbit/s, and also increasing steadily. In 2017, 78% of the web pages that Arcep tested, from among a sampling of the 30 most popular sites in France, loaded in less than 10 seconds. 4G also delivers sizeable gains on this indicator as 95% of web pages loaded in less than 10 seconds when using a 4G connection[26].

DATA OBTAINED FROM ARCEP'S MOBILE QUALITY OF SERVICE AUDITS



Source: monreseaumobile / Arcep observatory.

To flesh out Arcep's vision and bring it increasingly in line with users' expectations, in addition to taking its own measurements, the Authority wanted to increase its interaction with third parties involved in measuring performance, whether crowdsourced mobile solutions or other players, such as rail and public transport companies SNCF and RATP. The ties that have already been forged, and those yet to be fully developed, will help create a shared understanding of data collection methodologies, while seeking to achieve a high standard of quality, transparency and representativeness. It is to this end that, in January 2018, Arcep and QoSi announced the incorporation of data on mobile calling and texting service coverage into the Qosbee comparison engine, in addition to mobile quality of service data.

Qosi will also provide Arcep with the data it has obtained through its crowdsourcing apps and its own field surveys. Not only will these data enable Arcep to deepen its knowledge of the quality of operators' services, but they will also be published on monreseaumobile.fr, alongside Arcep's own measurements, to further enrich the information available to users. This partner-centric approach is fully in sync with the co-construction projects described above, as much for fixed as mobile networks.

[26] Testing methodology available at: https://www.arcep.fr/fileadmin/reprise/observatoire/qsmobile/2017-06-21_Report_QoS_Data.pdf

CO-CONSTRUCTION AND PUBLIC-PRIVATE DATA SHARING

Fabien RENAUDINEAU,
CEO, **QoSi**

Arcep has adopted a data-driven approach to regulation: a new form of action that leverages crowdsourcing, and so makes every citizen a micro-regulator thanks to exact and personalised information.

The services provided by Qosi are entirely in line with the nudge[27] that Arcep wants to give. We have thus elected to work closely with Arcep by taking part in discussion groups and the co-construction of forthcoming regulatory frameworks for mobile services but also, more recently, fixed ones as well.

More significantly, in the area of mobile service quality, we have formed a partnership focused in particular or reciprocal data sharing between the regulator and our Qosbee app. By providing Qosbee mobile coverage data (voice and SMS), Arcep gives every users the ability to know which is the best mobile operator for them, according to their consumption habits and where they live.

Over the past several months, this new regulatory momentum *"à la française"* has attracted the clear and growing attention of regulators in Africa and certain countries in Asia. Yet another sign that this vision is paving the way for tremendous opportunities in our markets.

"THIS NEW REGULATORY MOMENTUM *"À LA FRANÇAISE"* [...] IS PAVING THE WAY FOR TREMENDOUS OPPORTUNITIES IN OUR MARKETS"

[27] Nudge is a behavioural sciences theory that posits that indirect suggestions can influence people's decision-making, as, if not more, efficiently that direct instructions or legislation.

2. Monitoring Data interconnection market

Keeping a close eye on the situation is needed, given the patient's history

1. A VARIETY OF STAKEHOLDERS IN AN EVOLVING ECOSYSTEM

Several stakeholders interact in the Internet ecosystem:

- content and application providers (CAPs): content owners that employ several intermediaries to deliver their content to end users;
- web hosts[28]: owners of the servers that host the content managed by third parties (CAPs or individuals);
- Transit providers: managers of international networks that act as intermediaries between CAPs and ISPs for relaying traffic;
- Internet Exchange Points (IXPs): infrastructures that enable the different players to interconnect directly, through an exchange point, rather than going through one or several transit providers;
- Content Delivery Networks (CDNs): networks that specialise in relaying large volumes of traffic to several ISPs, in various geographical locations and thanks to cache servers installed in proximity to end users;
- Internet service providers (ISPs): network operators that are responsible for relaying traffic to end customers;
- End customers: individuals who use their own equipment and subscribe to an ISP's plan to be able to access content online.

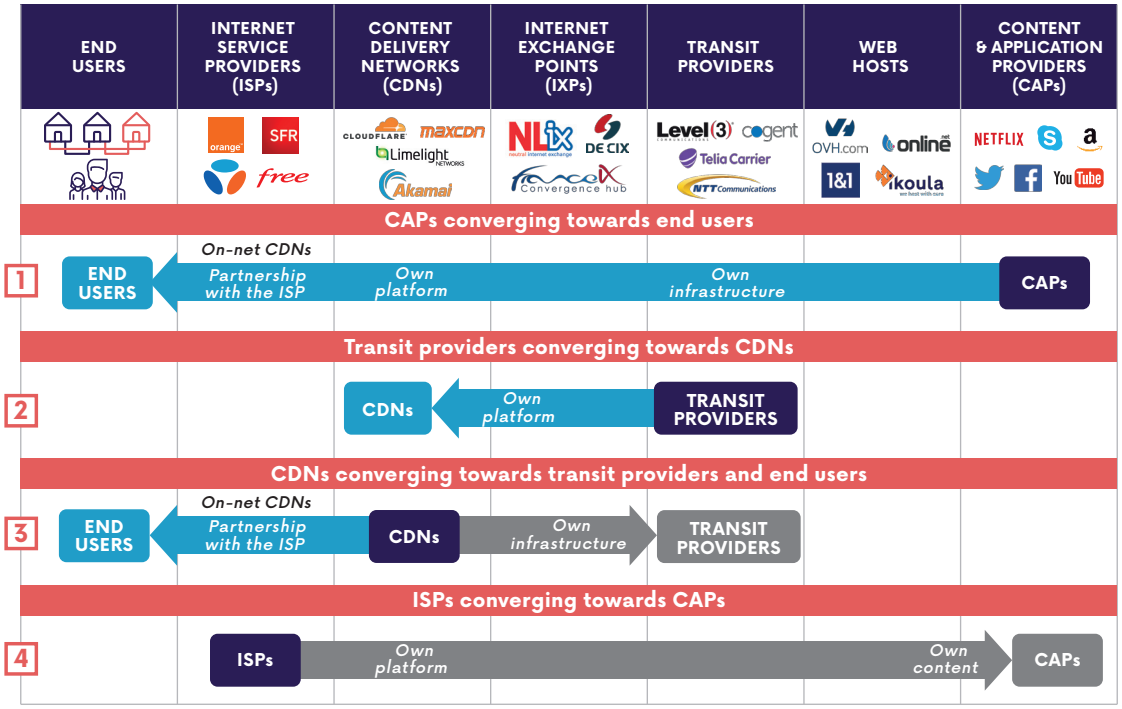
[28] More specifically: Article 6-1 Par. 2 of the Act of 2004-575 of 21 June 2004 on confidence in the digital economy, which defines web hosting companies as physical or legal entities that store, on behalf public online communication services, signals, writings, images, sounds and messages of any kind, provided by the recipients of those services, for the purposes of making them available to the public, even for free.

As the following diagram illustrates, the current market trend is one of convergence between the different players. Several vertical integration scenarios are occurring, both in the top and bottom half of the value chain:

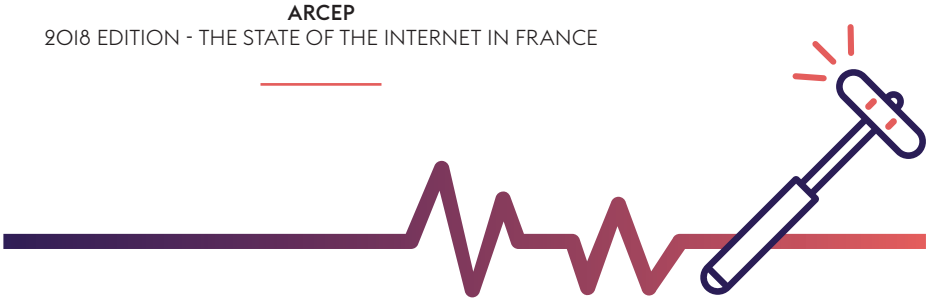
1. In order to get closer to end customers and to improve the resilience and quality of their services, CAPs are deploying their own network infrastructure and their own CDN platforms;
2. In addition to their transit solutions, transit providers employ their existing infrastructure to develop CDN products and host third-party content;
3. On the one hand, CDNs are behaving more and more like network operators by deploying their own infrastructure around the globe. On the other hand, they are establishing partnerships with ISPs to deploy their servers on the latter's network, and so be as close to end customers as possible;
4. ISPs are diversifying their businesses by creating their own content, and distributing it themselves through their own platforms.

NB. for further details on the technical terms employed below, Arcep invites readers to refer to Annex 6 of the Report to Parliament and the Government on net neutrality, published in September 2012.

INTERNET ECOSYSTEM STAKEHOLDERS CONVERGENCE [29]



[29] Inspired by a diagram from the Detecon Consulting presentation: "The value of Network Neutrality to European consumers".



DATA INTERCONNECTION FOR DUMMIES

Stéphane BORTZMEYER, Internet expert,

answers the most frequently asked questions on data interconnection.

What does interconnection do?

A customer of SFR obviously doesn't want to interact only with other SFR customers. They want access to the entire Internet. So operators need to interact with one another, i.e. to interconnect, and it is these interconnections that create the Internet, this network of networks.

What does an interconnection look like, physically?

It is an optical fibre that runs between the two operators' machines. To streamline the process, operators typically take advantage of being in the same data-centre where what are called meet-me rooms, dedicated to interconnection, are located. Or they interconnect at an Internet exchange point (IXP), those dedicated interconnection services where a new connection no longer has to even pass through a new fibre.

When two players want to interconnect, how do they go about it?

Connecting to one another physically is only part of the process. There needs to be an agreement between the two operators, so that each one can send the other their data, and relay the data they receive. Such an agreement is above all a business decision, rather than a technical one. Aside from a few countries, there are no national or international laws governing these agreements. Although the term "agreement" makes one think of a written and signed contract, many interconnection agreements are informal agreements, sealed with a handshake.
There are two main types of agreement: peering and transit. As the name suggests, peering occurs between two peers, i.e. two players of comparable size, no money changes hands and each only gives access to its own network, so not to any third party's network. Every operator has a peering policy (which is often formalised in a, possibly publicly available, text) that defines the players it agrees to consider its peers. This policy may, for instance, indicate a minimum bitrate threshold (large operators do not like peering with small ones).
But peering is not enough to cover everything, as two operators may simply be too far from one another for it to be possible. If a Free customer in France wants to visit Colombia's national university's website, for instance, it is likely that Free and the network that connects the university to the Web do not have a way to interconnect physically. Here is where what are called transit providers, which have a much broader global footprint, come in. When an operator connects to the transit provider, it is the one who is "buying transit" by paying the transit provider. Here, the contract is almost always a formal one, and the transit provider gives the operator access to the entire Internet. The different transit providers interconnect with one another through peering agreements, and it all comes full circle. So anyone can visit the Colombian university's website.

How do they choose between peering and transit?

Remember, this is above all a business decision. Let's take the example of a small ISP. It is in its best interest to negotiate a maximum number of free peering agreements, to secure advantageous interconnection possibilities. But this will not give the ISP access to either the biggest operators' networks (they will refuse to peer with this small player, and will demand it become a paying customer) or to far-off networks in other countries (the transit provider will not do it a favour for free). So our little ISP will need to pay one or several transit providers.
In some instances, the big operators charge their peers while only providing access to their own network (contrary to transit provider). This is referred to as paid peering, and depends entirely on the balance of power.
Peering policies may include a symmetry criterion, i.e. approximately the same number of bits going in and coming out. And they may require the agreement switch to a paid peering if traffic becomes too asymmetrical.
Generally speaking, asymmetry creates negative pressure on the relationship, hence the importance of peer-to-peer exchanges, to increase symmetry.
It is worth mentioning that there is no official equalisation mechanism between operators, as was the case with telephony.

And do CDNs change the situation in any way?

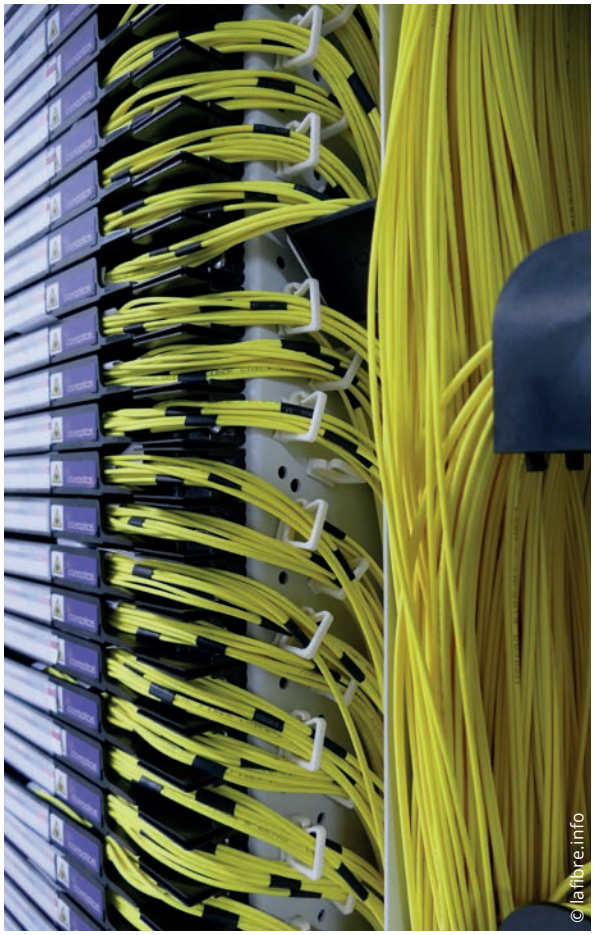
A CDN (Content Delivery Network) is a service that delivers content in advance to many locations close to future customers. The closest one is of course on their ISP's own premises, which are referred to as on-net CDNs. These servers, which are managed by the company that owns the CDN but installed on the ISP's network, are beneficial for the content provider (since located closer to its customers) and for the ISP (as they decrease the need for interconnection). However, they also lead to tough negotiations to determine whether one of the two parties will pay to host the service.

2. AN EXTENSION OF COLLECTED DATA FOR BETTER SUPERVISION AND SUPPORT

Given the occasional tensions that may appear on the interconnection market[30], continuous monitoring is necessary so that Arcep can encourage stakeholders to behave virtuously and react quickly in if any problem happens. At this stage, it does not appear necessary for Arcep to intervene directly through an *ex ante* regulatory decision. However, the Authority has the powers to act if difficulties arise[31].To improve its knowledge of interconnection and data routing markets on the Internet, through Decision No. 2012-0366, in 2012 Arcep implemented the periodic collection of information on the technical and pricing terms and conditions governing interconnection and data routing.

Decision No. 2012-0366 was amended for the first time in 2014 (Decision No. 2014-0433-RDPI). In 2017, after having drawn conclusions from several rounds of this new data collection campaign and from responses to an ad-hoc questionnaire[32] that was sent to operators in March, on the new interconnection systems and the make-up of traffic in France, the competent Arcep body adopted Decision No. 2017-1492-RDPI on 12 December 2017, following a public consultation. This purpose of this update to the decision was, first, to relax its scheme and simplify capacity indicators and, second, to request information on on-net CDN servers traffic (also referred to as on-net CDNs or internal cache servers). The competent Arcep body believed that there needed to be an indicator that enabled it to determine the technical and financial conditions of internal cache servers traffic, to be able to factor in their growing use alongside traditional interconnection methods. In particular, these adjustments will make it possible for Arcep to fine tune its understanding of the technical-economic relationship between Internet service providers and content and application providers, when it comes to relaying their traffic.

The results and findings of this updated information gathering process are being presented for the first time in this report. Arcep has also decided to publish information on data interconnection on a regular basis going forward, through the creation of a dedicated observatory in late 2018, which will be updated annually.



[30] See the dispute between Cogent and Orange before the French Competition Authorities, concluded in 2012, or the administrative investigation on several companies, including Free and Google, regarding the technical and financial conditions of traffic routing, run by Arcep in 2012-2013.
[31] For more information on the regulatory framework applicable to interconnection, the reader may refer to the insert on page 45 of the 2017 report on the state of the Internet in France.
[32] Send on the basis of the decision on the collection of information on the technical and pricing terms and conditions governing interconnection and data routing.

BOUYGUES TELECOM AND ORANGE FRANCE INTERCONNECTION POLICIES

Benoît PLESSY,
Head of IP/optical backbone architecture, peering manager,
BOUYGUES TELECOM

For our customers, the ability to access the Internet is indispensable to their daily lives. And they want to have a high quality Internet access service.

In addition to the access service provided, interconnection agreements between Bouygues Telecom and Internet companies need to be put into place to enable end customers to consume certain services and/or applications that are available on the Internet.

This is why Bouygues Telecom opted for an open interconnection policy that can be summed up as follows:

- Enable Internet players to relay their services and applications on our network through direct interconnection as part of peering agreements, or using a public Internet exchange point;
- Regionalise (Marseille, Lyon, Lille) the exchange points and introduce third-party cache servers onto our networks, to bring content closer to customers and reduce the risks should incidents occur;
- Ensure sufficiently well provisioned interconnections to avoid interconnection links from being overloaded, including with our transit providers.

We believe this approach helps further the Internet's sound development in France. It should nevertheless be emphasised that the ongoing increase in traffic, spurred by major Internet players, is having a significant impact on our network infrastructure.

Aurore CROCHOT,
Head of IP interconnection and peering,
ORANGE FRANCE

To provide Internet content with a better quality of service, every player along the supply chain needs to be involved.

As an Internet player, Orange has seen a massive increase in traffic from the biggest online content providers. This handful of heavyweights singlehandedly account for more than half of all Internet traffic going to Orange customers in France.

Faced with this exponential growth, Orange is adapting its networks' capacities and reinforcing its many access points, to obtain a robust and reliable network to provide the best quality of service to its customers.

This quality of service, which is vital for Orange, nevertheless also depends on content providers. They make their own choice of service and/or transit providers for relaying their traffic to the users of their services.

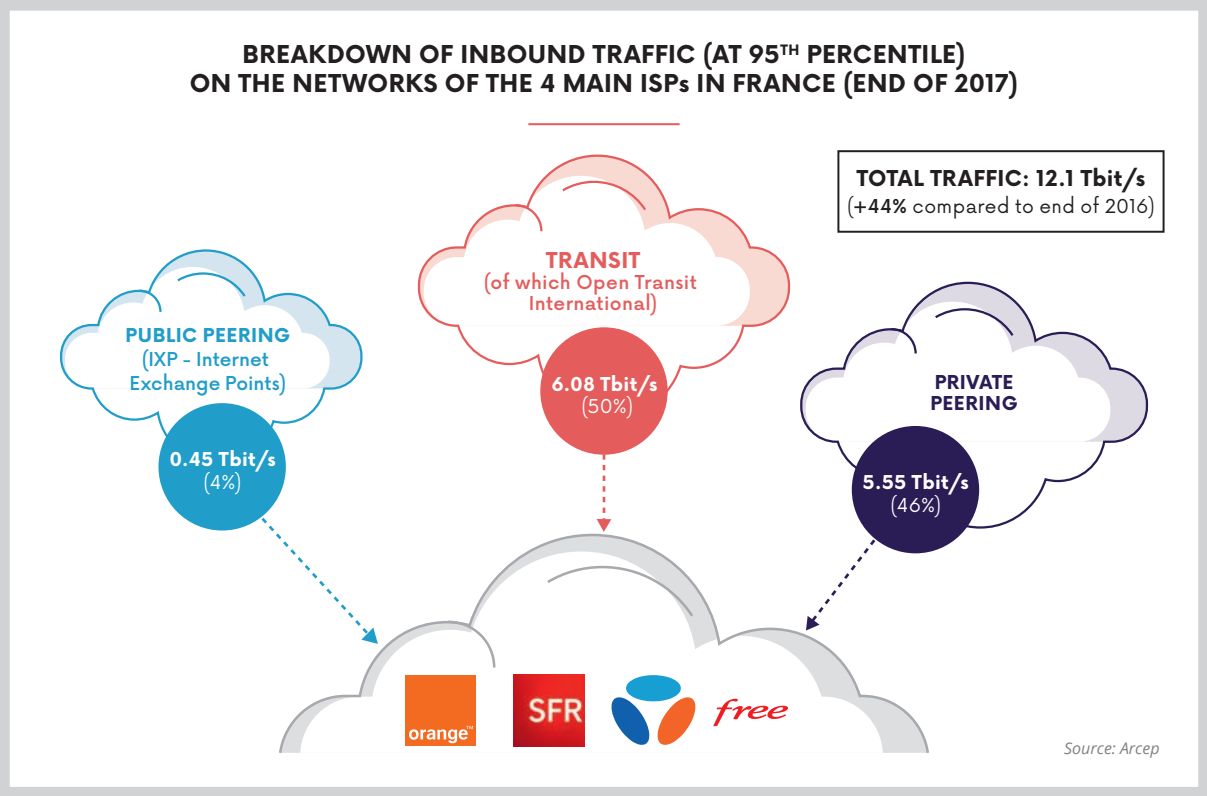
Orange has thus also made the choice to continue to exchange traffic with these transit providers and content providers to optimise the quality of service experienced by its own customers and end users (resilience in case of network failures, managing traffic surges, converging towards processing routing between IPv4 and IPv6 in a uniform fashion). Orange attaches a great deal of importance to fostering dialogue with these various players, to achieve a balanced business model, and one that favours direct interconnections on its networks.

Free and SFR chose not to respond to Arcep's invitation to contribute to this section.

3. RESULTS THAT CONFIRM MARKET TRENDS

For confidentiality reasons, only aggregate results[33] are published.

3.1. Inbound traffic



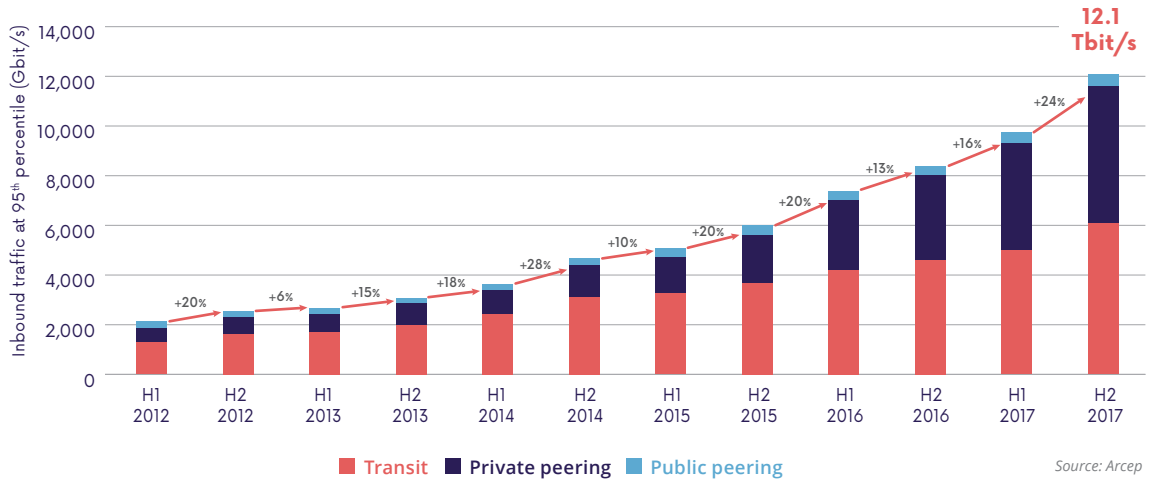
Inbound traffic to the four main ISPs in France has increased from 8.4 Tbit/s at the end of 2016 to 12.1 Tbit/s at the end of 2017, which translates into a 44% increase in a single year. Half of this traffic comes from transit links.

This relatively high rate of transit is due in large part to transit traffic between Open transit international (OTI), a Tier 1[34] 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. This rate of transit is much lower for other ISPs which do not have a transit provider business, and so make much greater use of peering.

Inbound traffic thus continues to grow at a considerable rate: by an average 40% a year[35].

[33] Results obtained from operators' response to the information gathering campaigns on the technical and financial conditions of data interconnection and routing, which scope is described within the decision 2017-1492-RDPI: https://www.arcep.fr/uploads/tx_gsavis/17-1492-RDPI.pdf
[34] See lexicon.
[35] At the end of 2016, total inbound traffic increased by 36% compared to the end of 2015.

INBOUND TRAFFIC TO THE MAIN ISPs IN FRANCE BETWEEN 2012 AND 2017

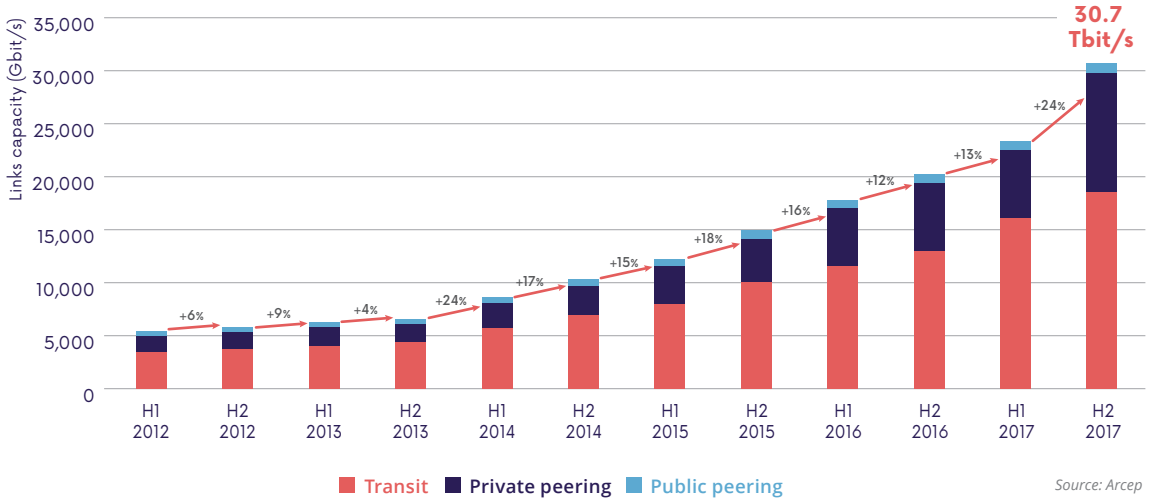


3.2. Installed capacity

Installed Interconnection capacities have increased at the same pace as inbound traffic. Installed capacity at the end of 2017 is estimated at 30.7 Tbit/s, or 2.5 times the inbound traffic.

This ratio does not exclude congestion incidents, which can occur between two players or on a particular link, depending on their status at a given moment in time.

INTERCONNECTION LINKS CAPACITIES OF MAIN ISPs IN FRANCE BETWEEN 2012 AND 2017



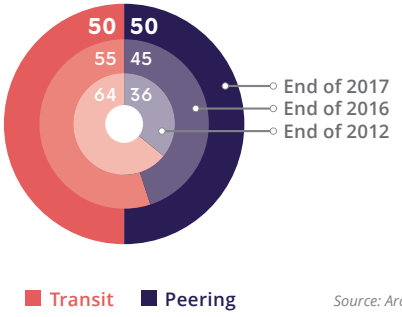
3.3. Evolution of Interconnection methods

Peering vs. Transit

As mentioned earlier[36], there are two kinds of interconnection: peering and transit[37]. Peering's share of interconnection links has been increasing steadily – due mainly to the increase in installed private peering capacity between ISPs and the main content providers. Public peering traffic is also increasing, albeit more slowly: its relative share (5% at the end of 2016 vs. 4% at the end of 2017) is decreasing in favour of private peering (41% at the end of 2016 vs. 46% at the end of 2017).

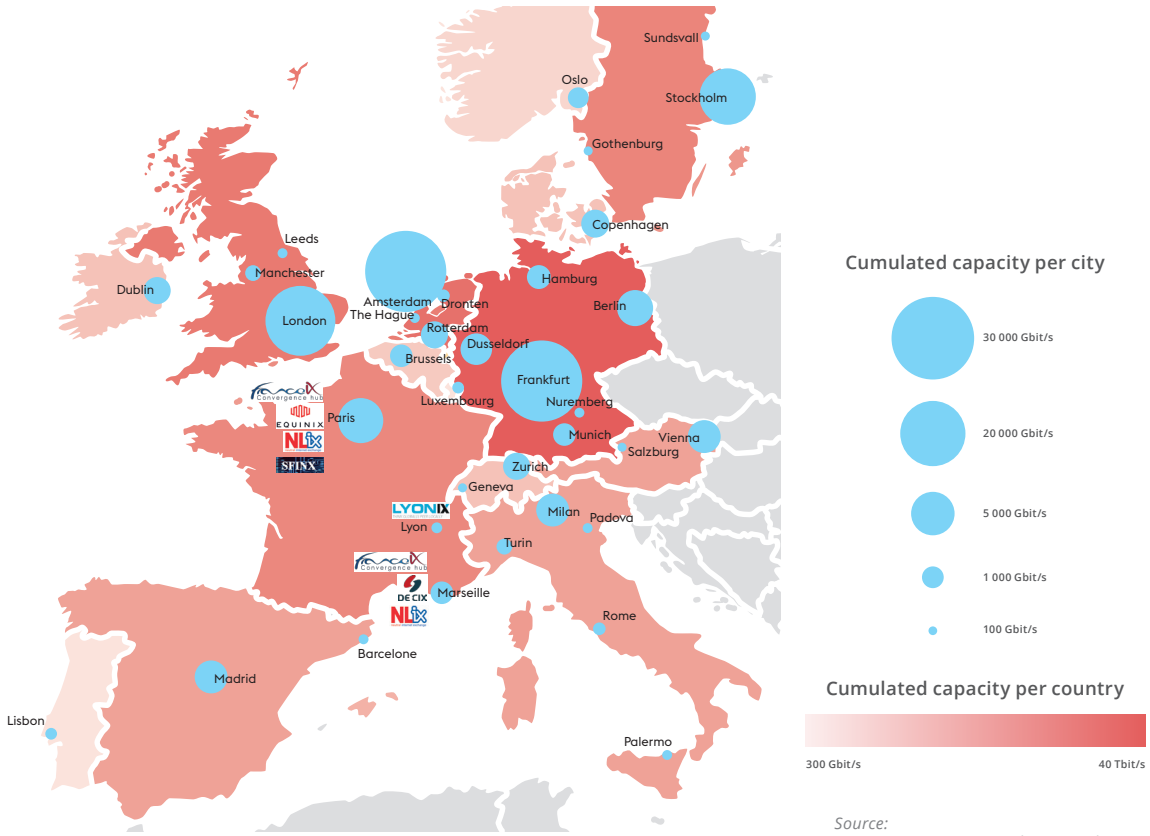
Reminder: private peering occurs between two peers through dedicated interconnection, while public peering takes place at Internet Exchange Points (IXP). As indicated at the start of this section, these infrastructures enable the different players to interconnect by sharing installed capacity, without having to go through transit providers, for instance, which is more cost effective and improves traffic routing.

EVOLUTION OF PEERING AND TRANSIT FOR THE MAIN ISPs IN FRANCE
(In proportion of inbound traffic volume)



Source: Arcep

MAP OF IXPs* IN FRANCE AND NEIGHBORING COUNTRIES



* IXPs with an installed capacity higher than 100 Gbit/s

Source:
Data: Ripe, PeeringDB, TeleGeography
Consolidation Arcep

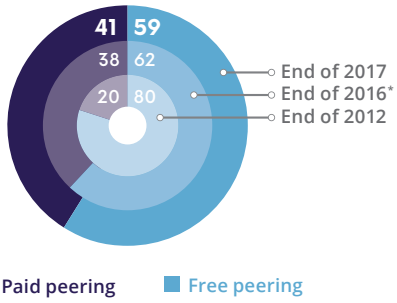
[36] Contribution: Interconnection for dummies, page 32.
[37] See lexicon.

The map reveals that France ranks fifth[38] in the number of Internet exchange points installed in the country, behind Germany, the Netherlands, England and Sweden. In France, IXPs are largely concentrated in Paris and Marseille. France-IX Paris, with a capacity of 2.9 Tbit/s and its ten clients of more than 100 Gbit/s, is positioned as the French market leader.

Free vs. paid peering

Both public and private peering can be paid peering. The percentage of peering that is paid for has changed since the end of 2016, rising from 38% to 41%. This change is due primarily to the increase in private peering traffic, of which a sizeable share is paid, notably when there is a considerable asymmetry in traffic. 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)



* The figures for end of 2016 have been updated since the 2017 report, after having obtained more detailed data from certain operators.

Source: Arcep

3.4. Breakdown of traffic by type of interconnection

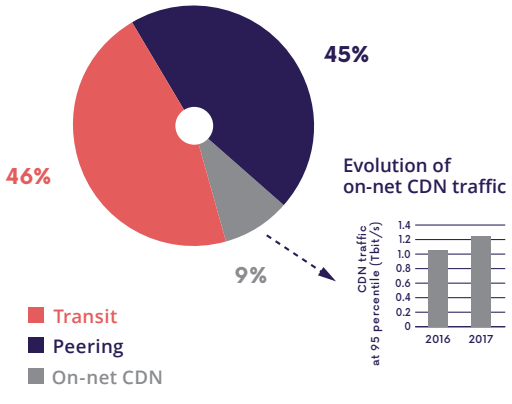
As explained at the top of the section, CAPs are working more and more to forge closer ties with end customers. To this end, they are creating partnerships with ISPs to host their content in cache servers in operators' networks. These on-net CDNs can either belong to the operator that hosts them or to a third party. In France, Google and Netflix are the two main players that incorporate servers in certain operators' network.

Thanks to the *ad hoc* questionnaire on the breakdown of traffic and on-net injection on ISPs' networks, which was sent to the top four ISPs in early 2017, Arcep was able to observe that, at the end of 2016, the traffic coming from on-net CDNs stood at 1 Tbit/s and accounted for 11% of these top ISPs' traffic, although percentages vary considerably from one ISP to another.

As mentioned earlier, to be able to monitor this trend more closely, Arcep updated its decision on information gathering, to be able to assess how traffic coming from on-net CDN evolves over time. By the end of 2017, traffic coming from these servers had increased to reach 1.2 Tbit/s, or 9% of those four ISPs' total traffic. Again, this percentage, which is lower than the previous year, varies considerably from one ISP to the next: some operators have no on-net CDN while, for others, it accounts for more than a quarter of the inbound traffic being injected into their networks.

In addition, the ratio of inbound to outbound traffic varies between 1:4 and 1:11 depending on the operator. In other words, data stored in the cache servers are viewed between four and 11 times.

BREAKDOWN OF TRAFFIC IN FRANCE BY INTERCONNECTION TYPE (END OF 2017)



Source: Arcep

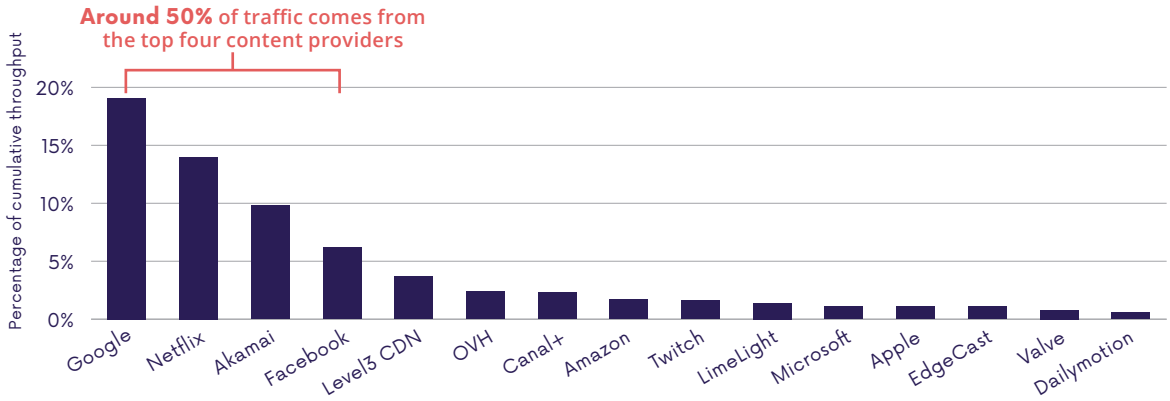
[38] Rankings include the following countries: Austria, Belgium, Denmark, England, France, Germany, Ireland, Italy, Luxemburg, Norway, the Netherlands, Portugal, Spain, Sweden and Switzerland.

3.5. Traffic breakdown by origin

Like last year, the information gathering campaign made it possible to estimate the breakdown of traffic by origin.

The four biggest providers (Google, Netflix, Akamai[39], Facebook) together account for around half of inbound traffic on the networks of the top ISPs in France, which confirms the conclusion contained in the 2017 report indicating an increasingly clear concentration of traffic amongst a small number of players whose position in the content market is more and more entrenched.

BREAKDOWN OF TRAFFIC IN FRANCE BY ORIGIN (END OF 2017)



Source: Arcep

3.6. Evolution of costs

The range of transit and peering fees has not changed since last year. According to the latest data, the negotiated price of transit services is still between €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/s.

On-net CDNs are free in most cases. They can be charged for, however, either by the Gbit/s that the CDN pushes to the ISP client, or as part of a broader paid peering solution that the CAP has contracted with the ISP.

[39] Akamai is a CDN that distributes content for several CAPs.

FRnOG IN THE SERVICE OF THE INTERNET COMMUNITY IN FRANCE

Philippe BOURCIER,
Founder, **FRnOG (FRench Network Operators Group)**

FRnOG was created in 2001, modelled on NANOG and SwiNOG, to enable more meaningful dialogue between operators on technical issues (outages, attacks, security, peering, etc.). The ultimate goal is to have companies and their staff shift from being rivals to being fellow workers who aren't afraid to talk to each other.

More than fifteen years later, it appears to have paid off, as there are now more than 5,000 members on the mailing list and over 350 members in attendance at every one of the free biannual meetings.

In addition to these actions, the group was one of the key elements in the emergence and success of the third generation of Internet exchange points in France (France-IX and Equinix Paris) by enabling a dialogue between the initiators of these projects and future customers. At a time of growing concern about data and our digital sovereignty, but also as France is poised to become THE "start-up nation" in Europe, it would have been a veritable strategic error not to have a global-scale exchange point in France.

"THE ULTIMATE GOAL IS TO HAVE COMPANIES AND THEIR STAFF SHIFT FROM BEING RIVALS TO BEING FELLOW WORKERS WHO AREN'T AFRAID TO TALK TO EACH OTHER."

In more recent news, the community was able to come together around a noble cause: operation IRMA.

At the 29th meeting of FRnOG, the Association of Alternative Telecom Operators (AOTA), which was describing its activities to our members, issued a call for donations to help save one of its members: a small independent operator in the Antilles that has lost everything to hurricane Irma, called Dauphin Telecom. In concert with AOTA, we decided to hold a large drive to collect hardware, based on the list provided by the operator. More than €100K of used hardware was thus collected and sent, allowing Dauphin Telecom to start getting back on its feet while waiting for its insurance to come through.

© FRnOG

3. Accelerating the transition to IPv6

Lack of IP addresses: switch to IPv6 now.

1. THE TRANSITION TO IPv6: 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 addresses[40], of which a substantial portion cannot be used for Internet addressing: not only are 593 million IPv4 destined for particular uses (private networks, etc.), but the way that addresses were assigned back in the Internet's early days – in the late 1980s – was not efficient, and some companies were assigned blocks of 18 million IPv4 were neither ISPs nor web hosts.

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 IPv6 for each square millimetre of the earth's surface[41] (!). In this era of increasingly diverse applications and the proliferation of connected products, making the transition to this new protocol has become key to ensuring competitiveness and innovation.

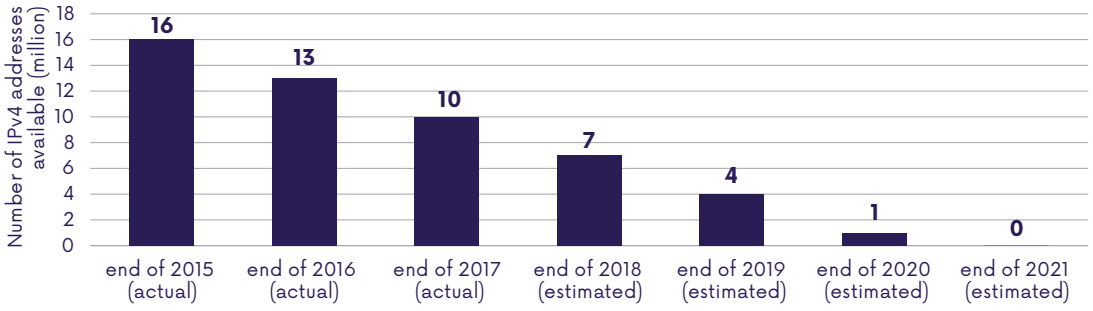
This transition also represents the most important evolution since the Internet's creation. Contrary to software upgrades that are backwards compatible with earlier version (e.g. software developed for Windows 7 can work in Windows 10), IPv6 is completely incompatible with IPv4. As was the case on 1 January 1983 for the migration to IPv4, one might think that the transition to IPv6 could be performed in one fell swoop, in a single day – i.e. flag day. But the size, disparity and complexity of today's Internet make it impossible to do so. The transition to IPv6 is therefore taking place gradually, starting with a period of cohabitation with IPv4 then, when every player has migrated, IPv4 will be fully replaced (switch-off phase).

The transition to the IPv6 protocol began in 2003. In 2018, however, the Internet is still only in the early part of the cohabitation phase. As explained above, IPv4 will continue to be necessary for as long as the entire technical chain has not fully switched over to IPv6. Otherwise, a site that is not able to have an IPv4 address could not be accessed by users who subscribe

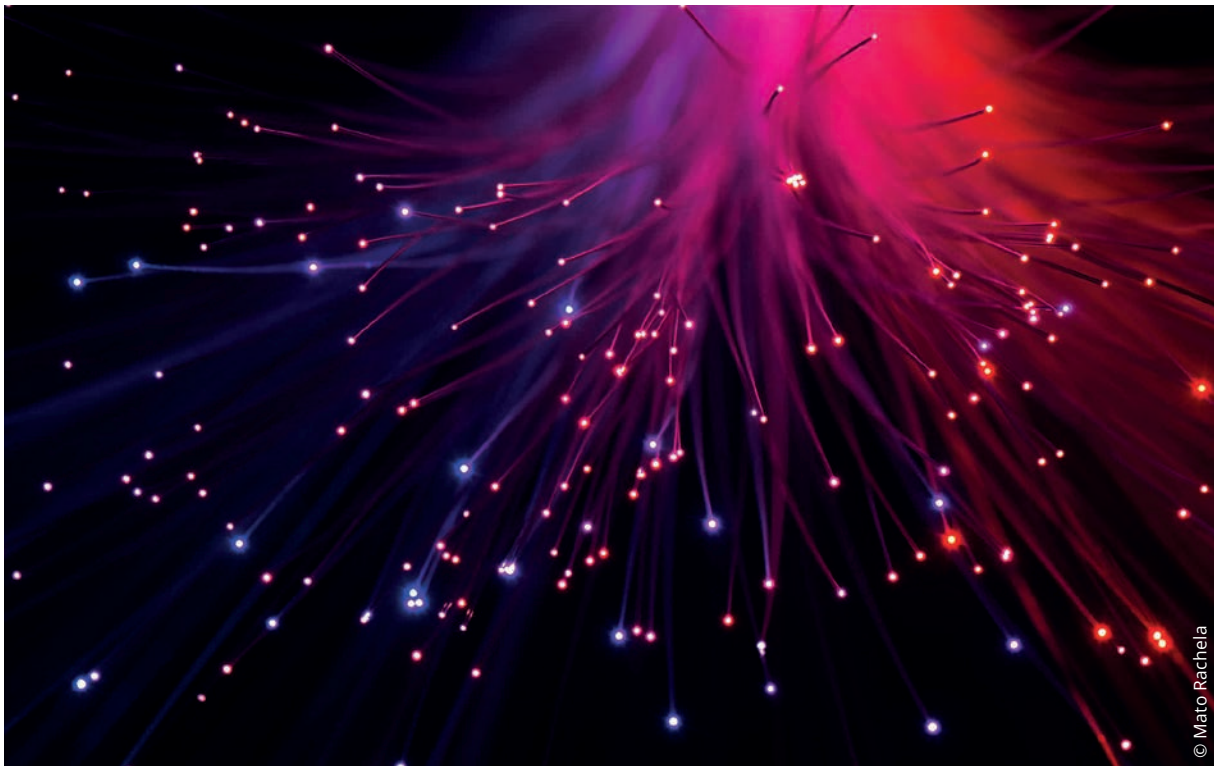
[40] IPv4 addresses use a 32-bit code. A maximum 2^{32}, or 4,294,967,296 addresses can theoretically be assigned simultaneously.
[41] IPv6 addresses use a 128-bit code. A maximum 2^{128} (i.e. around 3.4×10^{38}) addresses can theoretically be assigned simultaneously.

to an ISP that does not provide IPv6 addresses. So IPv4 is still needed to be able to communicate with the IPv4 Internet. But the shut-off date for IPv4's availability in Europe is fast approaching. Estimated to be in late 2021[42], it is already driving a significant increase in the price of IPv4 addresses, which have become the scarce resources of the 21st century Internet. This high price creates a sizeable barrier to entry for newcomers to the market, and increases the risk of seeing the Internet split in two, with IPv4 on the one side and IPv6 on the other.

ASSESSMENT AND ESTIMATE OF THE REMAINING STOCK OF IPv4 ADDRESSES



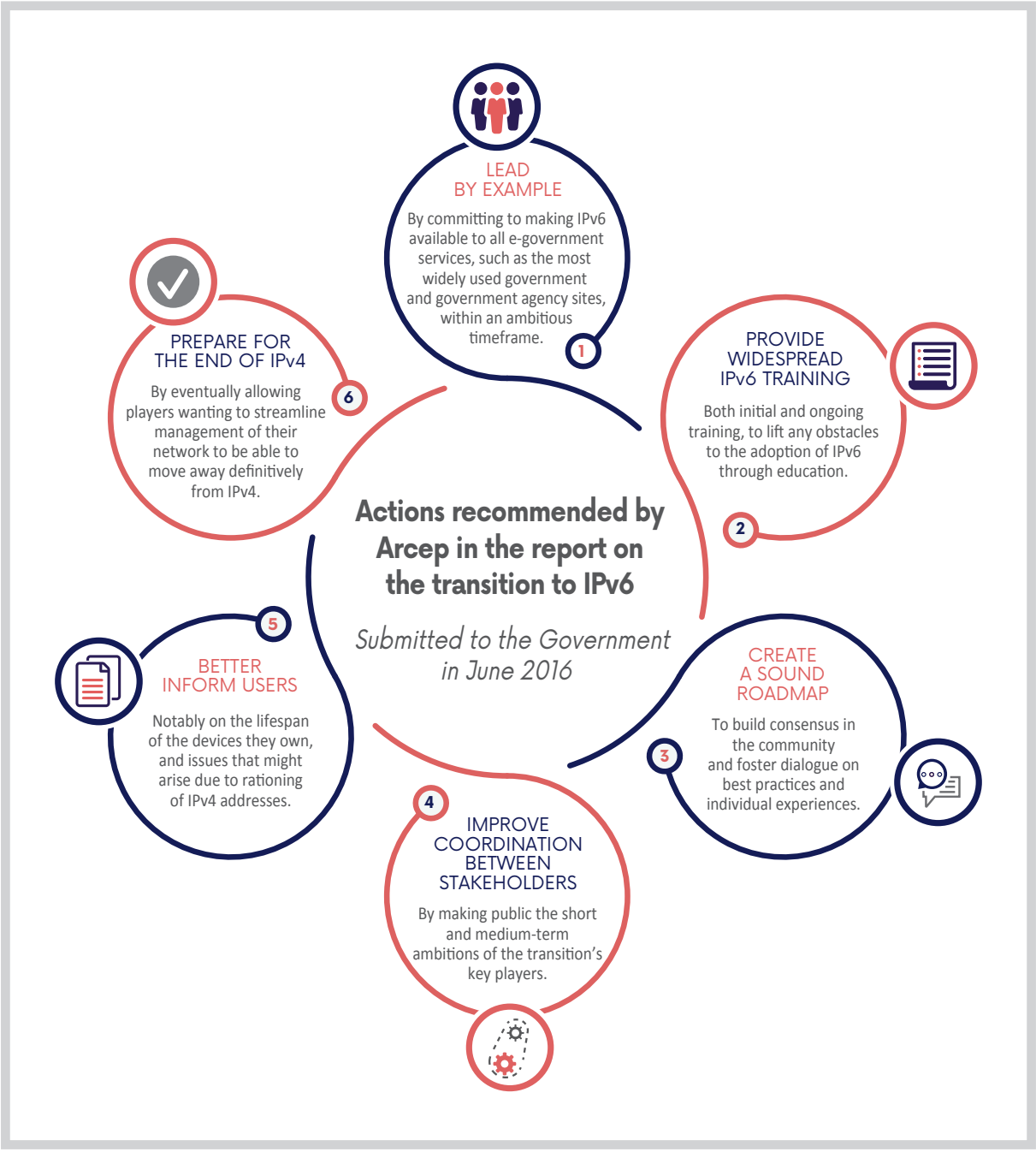
Source 2015-2017: RIPE-NCC (march 2018)
Source 2018-2021: Arcep projection (march 2018)



[42] See diagram below.

ISPs have introduced certain substitution measures to handle this dearth of IPv4 addresses. Carrier-grade NAT (CGN) equipment, for instance, makes it possible to have several customers share an IPv4 address. This can, however, have several negative effects that make maintaining IPv4 a complex affair, and virtually impossible for certain applications such as peer-to-peer, remote access to shared files on an NAS[43] or to a smart home's control system, certain online games, etc.

In June 2016 Arcep delivered a report to the Government, produced in concert with Afnic, which contained several courses of action designed to support and accelerate the transition to IPv6. They are listed in the diagram below.



[43] Network Attached Storage, a networked storage server.

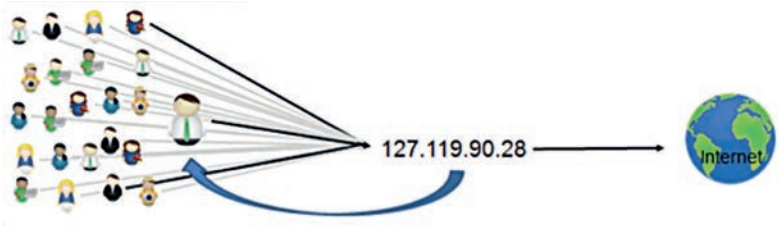
LIMITING THE USE OF CGN AND THE TRANSITION TO IPv6: THE BELGIAN EXAMPLE

Gregory MOUNIER,
European Cybercrime Centre (EC3), **EUROPOL**[44]

Commissioner Adeline CHAMPAGNAT,
Councillor to the anti-cybercrime delegation,
CENTRAL MANAGEMENT OF THE JUDICIARY POLICE

CGN stands for carrier-grade network address translation. It is a mechanism for translating a private internal IP address into an external public address that is visible on the Internet. ISPs can thus have thousands of users share a public IP address simultaneously, and so countervail the dearth of IPv4 resources.

In addition to this practice, which is employed by more than 90% of mobile operators, there are certain technical issues that can have sizeable negative effects on public security. When investigative agencies are probing a crime or offence enabled by the Internet, one of the fist digital traces available is an IP address. ISPs are legally required to provide investigators with the identity of the subscriber who uses this address. When it is behind a CGN, ISPs will need to know not only the date, time and the source and destination IP addresses, but also the source port number. Unfortunately, service providers rarely keep a record of the source port.



CGN therefore make investigations more difficult as it will take a lot of time to identify a subscriber: an ISP can provide investigators with a list of all of the subscribers who were using the same IP address, but this list could contain thousands of names. ISPs' failure to obey the law thus violates the privacy of a great many people who could be named in the procedure, even though investigators are only interested in a single suspect. Here, only the virtually complete transition to IPv6 can provide a lasting solution to this problem.

CGN techniques were meant to be temporary solutions, while waiting for the transition to IPv6 to reach a critical threshold, and for all Internet traffic to switch to IPv6. Unfortunately, the transition has been very slow since it began in the 2000s. One might even wonder whether, for certain operators, CGN technology has not gradually become a substitute for IPv6, and a way to prolong the life of IPv4 indefinitely and so avoid the need to invest in upgrading their networks. The European Parliament adopted two reports in 2017 criticising operators' misuse of CGN, and condemning the negative impact these practices are having on the security of European citizens.

To offset the fact that Internet platforms do not keep a record of source ports, Belgium invited ISPs based in the country to sign a voluntary code of conduct in 2012, in which they commit to reducing the overall ratio of subscribers to IP addresses to 16:1. Five years on, Belgium's enforcement services receive an average of only four subscribers using the same IP address, which hugely reduces the negative impact that CGN have on criminal investigations.

Another unexpected consequence: Belgium has the highest rate of IPv6 adoption in the world, with over 52% of users now in IPv6, and this since 2013, soon after the code of conduct was adopted. It is therefore entirely reasonable to think that the decision to voluntarily limit the number of subscribers attached to a public IP address pushed operators based in Belgium to only use CGN as a last resort, but also to invest more heavily in the transition to IPv6.

European institutions have drawn inspiration from the example set by Belgium, and in late 2017[45] asked EU Member States to propose having ISPs adopt a code of conduct to limit the use of CGN and the number of subscribers per public IP address. This measure is based on the supposition that CGN technology is hampering the adoption of IPv6.

[44] Europol and its European Cybercrime Centre (EC3) is collaborating with the competent authorities in European Union (EU) Member States, European institutions and RIPE NCC to accelerate the transition to IPv6.
[45] http://data.consilium.europa.eu/doc/document/ST-15748-2017-INIT/en/pdf, p. 14 et 15.

2. ARCEP OBSERVATORY, OR A HEAVY DOSE OF TRANSPARENCY TO ACCELERATE THE TRANSITION

As part of the actions recommended in its June 2016 report, Arcep has been delivering an annual scorecard on the transition to IPv6 since December 2016. The purpose is to better inform users about this topic, in keeping with a data-driven approach to regulation. This scorecard, whose results are detailed in Part 2.1, provides a snapshot of the progress being made in France, along with one-year and three-year deployment forecasts for ISPs with more than a million subscribers[46]. The next edition will include several new additions (cf. section 2.2).

2.1. Results at the end of 2017

On 18 December last, Arcep published the 2017 edition of its scorecard on the transition to IPv6 in France. This edition contained two major additions:

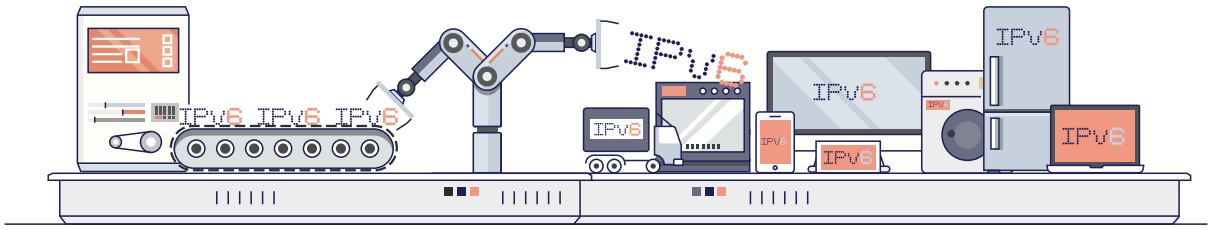
- alongside the data produced and provided by third parties (Cisco, Google, ANSSI, World IPv6 Launch), the scorecard is now enhanced with data that Arcep collected directly from the main operators in France;
- the current status and past developments in IPv6 adoption are now completed with operator's expected short and medium-term deployment forecasts.

The scorecard provides three types of IPv6-related information: the percentage of IPv6-ready customers, the percentage of activated customers and the rate of use for IPv6. Diagram below indicates the location in the network where these rates are measured or calculated. For further information about the meaning of these indicators, readers can refer to the explanatory graphic contained in the Arcep scorecard[47].

The results confirm the progress being made in IPv6 use in France, which stood at 20.4% at the end of 2017. Free is the ISP that is the most advanced on the transition front, with a 35% rate of use at the end of 2017 (compared to 24% at the end of 2016). The greatest progress has been made by Orange, however, whose rate of use doubled in a year, going from 16% at the end of 2016 to 33% at the end of 2017.

Regarding the transition on fixed networks by the different operators in France:

- end of 2018: Free plans on activating IPv6 for all of its customers. Orange plans on activating IPv6 for 50% to 60% of its customers within a year. Bouygues Telecom plans on carrying out a widespread transition, to have 25% to 35% of its customers activated. While SFR is projecting that fewer than 10% of its customers will have been switched over by the end of the year;
- end of 2020: Orange forecasts that 70% to 80% of its customers will have been switched to IPv6. Bouygues Telecom plans on having activated 75% to 85% of its customers, while SFR forecasts that it will have reached between 10% and 20% activated customers.

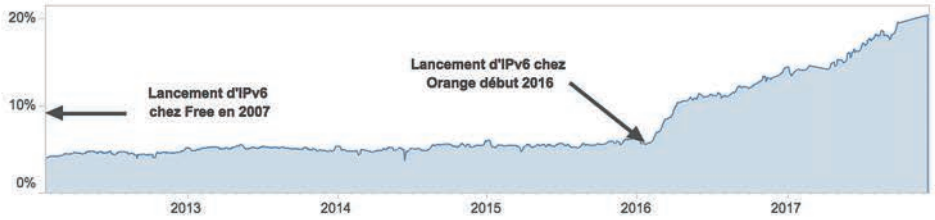


[46] To be more precise, ISPs with more than a million subscribers that manage their IP address plan.
[47] https://www.arcep.fr/index.php?id=13726

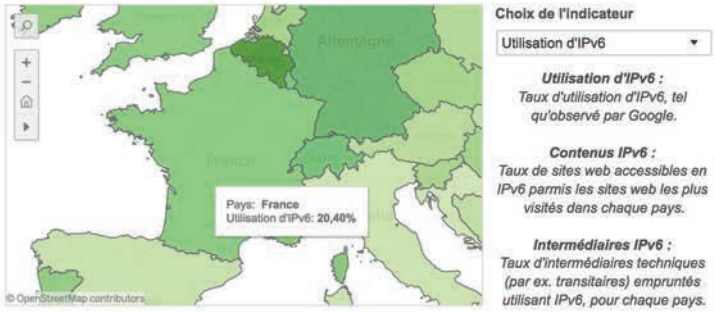
TRANSITION TO IPv6: ARCEP OBSERVATORY

18 december 2017

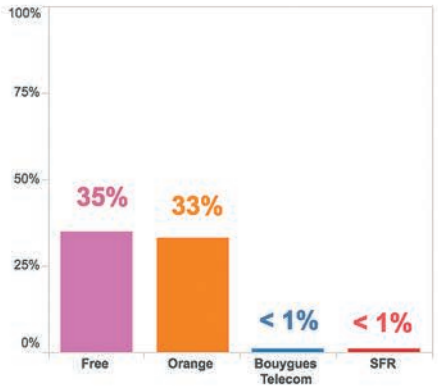
Evolution du taux d'utilisation d'IPv6 en France, tel qu'observé par Google
Source : Cisco - 6Lab



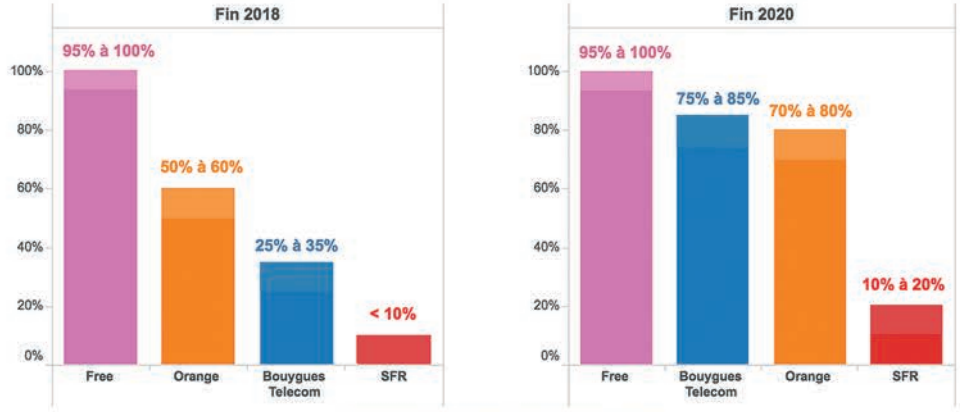
Etat de la transition IPv6 dans le monde au 07/12/2017
Source: Cisco - 6Lab



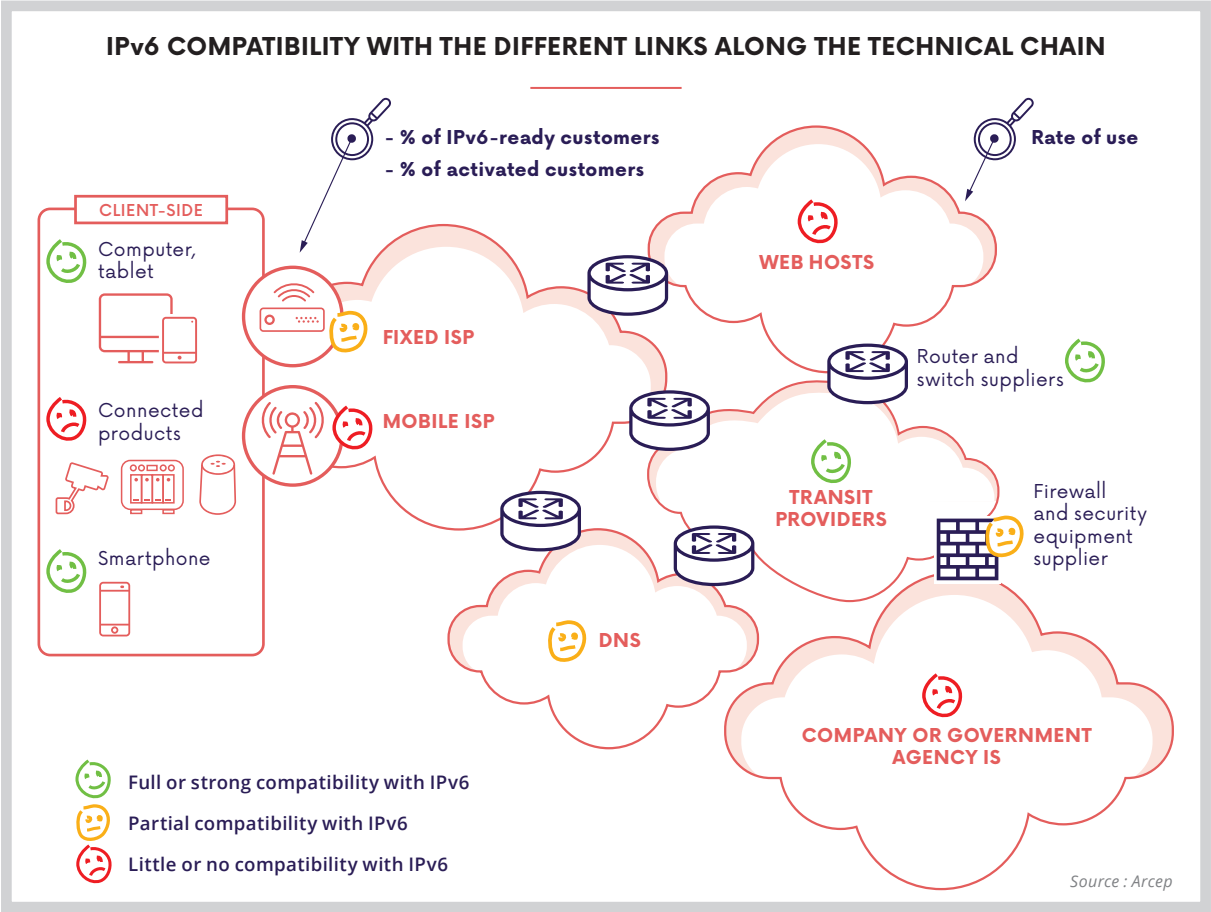
Taux d'utilisation d'IPv6 sur les principaux réseaux en France au 08/11/2017
Source: World IPv6 Launch / Apnic



Prévisions des taux de clients du réseau fixe activés en IPv6 pour les principaux opérateurs en France*
Source: Données recueillies par l'Arcep auprès des opérateurs



**Projections, chiffres susceptibles d'évoluer.*



2.2. Forthcoming enhancements

In early 2018, Arcep Decision No. 2018-0268 of 15 March 2018 on the introduction of surveys of the electronic communications sector was amended to:

- Establish a questionnaire that further clarifies the difference between IPv6-ready customers and activated IPv6 customers, and provide detailed figures for each access technology and type of network;
- Expand the scope of the information gathering to include – in addition to operators that manage their IP address plan and which have more than a million subscribers – web hosting companies and operators that manage their IP address plan and have between 10,000 and a million subscribers who have agreed to help enhance the observatory.

Web hosting companies have a crucial role to play in the transition. To ensure the IPv6 protocol functions from end to end, it needs to cover all of the links along the Internet value chain simultaneously. As depicted in the above graphic, web hosting companies remain one of the chief bottlenecks.

At the same time, other data will come to enhance future publications of the scorecard. From hereon in, Arcep will track the percentage of the top 50 sites[48] that are IPv6-compatible. Over the course of two years, from March 2016 to March 2018, this percentage rose from 22% to 34%[49]. By way of comparison, the percentage of the top 50 sites that are https-compatible rose from 22% to 76% during that same period[50]: i.e. a much higher increase that can be attributed, among other things to the pressure that several players have put on these sites, including search engines that downgrade http site's rankings, web browsers that flash security warnings on an http site, etc.

[48] Source listing the top 50 sites: Médiamétrie rankings.
[49] According to tests conducted by Arcep departments in March 2016 and March 2018.
[50] According to tests conducted by Arcep departments in March 2016 and March 2018.

A WEB HOST'S POINT OF VIEW

Jérémy MARTIN,
CTO,
FIRSTHEBERG.COM/TECH CRÉA SOLUTIONS

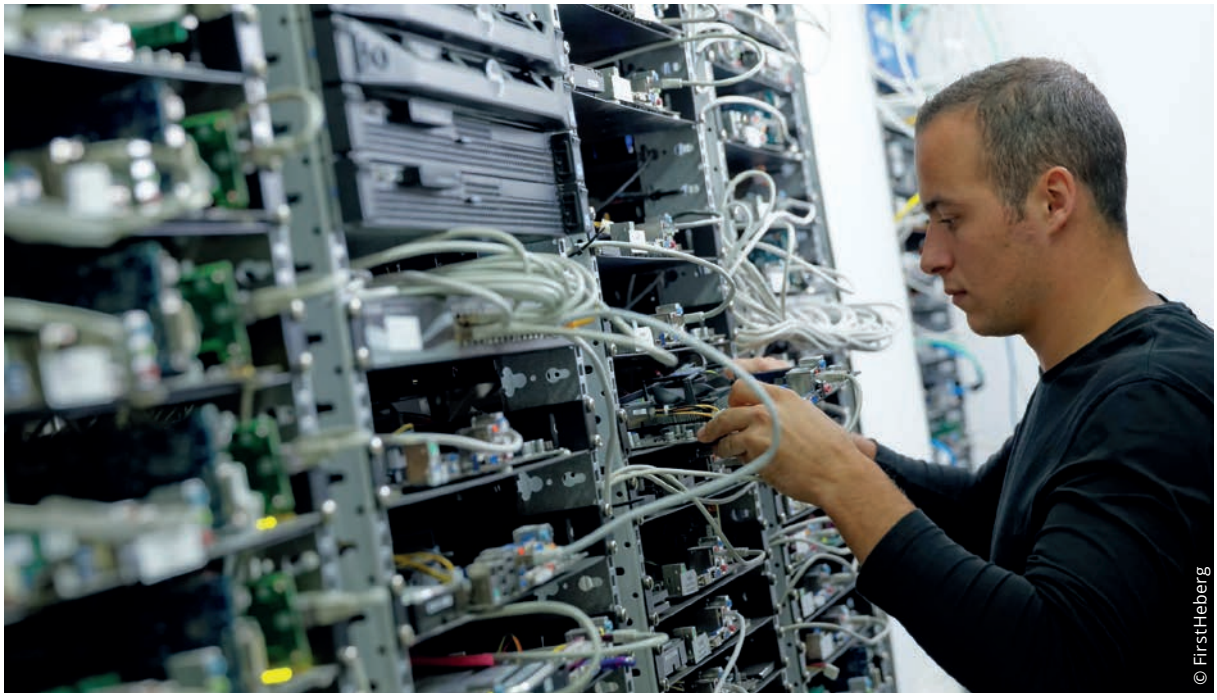
On 17 April 2018, RIPE NCC, the regional Internet registry for Europe, allocated its last block of new IPv4 addresses. RIPE is now allocating returned IPv4 addresses, but they are expected to run out in early 2021. With the growing demand for fixed IPv4 addresses, the price of leasing an IPv4 address will double over the next two years.

Today, FirstHeberg offers an IPv4 address and a block of dedicated IPv6 addresses for each server being leased. By 2020, FirstHeberg will be marketing a more affordable solution, with no dedicated IPv4 resources. FirstHeberg believes that, for financial reasons, starting in 2020 a small website may be forced to have only an IPv6 address. So if all of the boxes are not IPv6 activated by then, or if a great many companies continue to refuse to migrate there IS to IPv6, the Internet will unfortunately be split in two: customers that do not have an IPv6 address will not be able to access these small websites. This is why FirstHeberg will continue to offer a paid "dedicated IPv4 address" option, at least up until 2030. This will be especially crucial to those that absolutely need a site that can be accessed by both IPv6 and IPv4 customers.

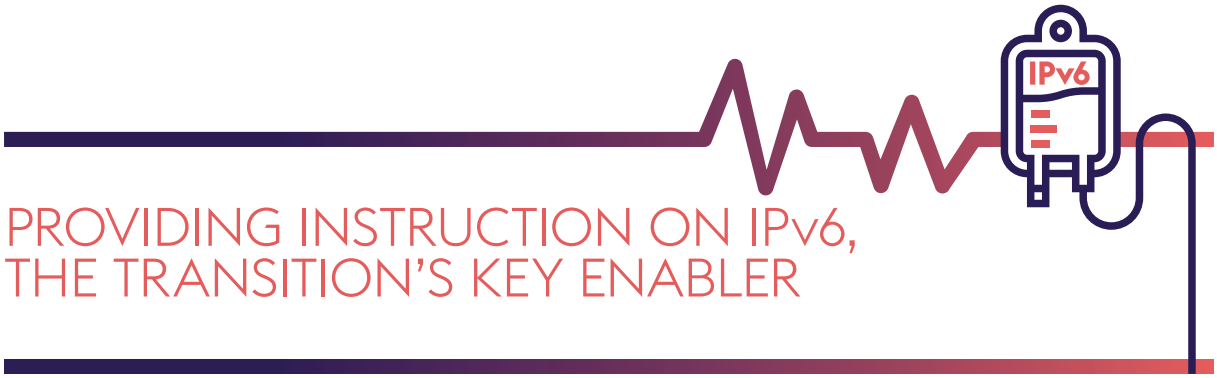
"THE IMPLEMENTATION OF IPv6 NEEDS TO BE UNDERGIRDED BY A POLITICAL VISION."

Clearly, the implementation of IPv6 needs to be undergirded by a political vision, to encourage stakeholders to implement the protocol in a very concrete way and to use it, possibly in exchange for financial incentives.

A deadline for the mandatory and legal implementation of IPv6 may be an effective measure, provided the State supports smaller businesses in the transition. A 2023 deadline is entirely feasible for achieving 100% coverage. And Europe could help by setting a far-off date for putting an end to IPv4, which would force the final holdouts to migrate. Policy constraints will indeed prove vital in the transition to IPv6, to prevent SME and SoHos from failing to make the move, especially those whose business model is based on providing network services, due to a lack of IPv4 addresses.



© FirstHeberg



PROVIDING INSTRUCTION ON IPv6, THE TRANSITION'S KEY ENABLER

Bruno STEVANT,
Teacher-researcher and head of G6 association training activities,
INSTITUT MINES-TÉLÉCOM

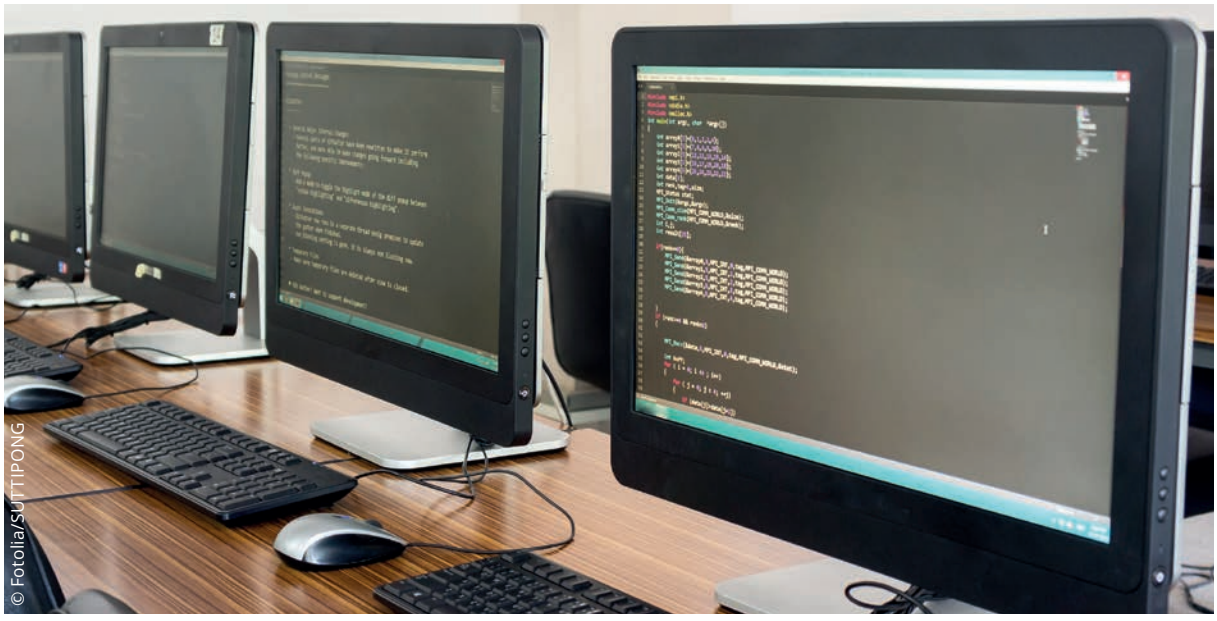
IPv6 is being deployed more and more by operators and on enterprise networks. Twenty percent of Internet traffic today is over IPv6. To be operational, newly graduated network engineers need to be skilled in implementing the new IP protocol and in managing a dual stack IPv4/IPv6 network.

The teaching of networks in universities and engineering schools needs to cover the theoretical aspects of IPv6, but also and especially allow students to practice IPv6. Today, however, far too few universities have IPv6 on their network, and fewer still offer instruction tailored to the new protocol.

At IMT, IPv6 has been a topic of research for more than 15 years. As the technology has gone from R&D to the production stage, we chose to integrate IPv6 into our initial and continued education courses. Thanks to the deployment of IPv6 on IMT networks, from the practical classes labs up to student dorm networks, our students use the new protocol on a daily basis.

"TODAY, FAR TOO FEW UNIVERSITIES [...] OFFER INSTRUCTION TAILORED TO THE NEW PROTOCOL."

Drawing on this experience, and working in cooperation with Association G6 (Association for the promotion and development of IPv6) and the Université de La Réunion, in 2015 IMT launched the first MOOC (massive open online course) over IPv6 on the France Université Numérique network. After three sessions, the "Objectif IPv6" MOOC had more than 15,000 registered students, and delivered around 1,000 statements of participation. A success that confirms the interest that exists in a quality training course on IPv6. It is therefore important that network and Internet teaching and training courses, from the technician to the engineer level, evolve to include the theoretical and practical aspects of the IPv6 protocol, and that professors not teach it like a technology of the future, but as the current network standard.



© Fotolia/SUTTIPONG

3. THE ECOSYSTEM GALVANISED AROUND AN IP♥6 WORKSHOP

As part of the process of creating forums for dialogue to be able to bring the community together, Arcep, in partnership with Internet Society France (ISOC), decided to host a workshop devoted to sharing individual experiences and best practices that would be useful to the transition to IPv6.

This will be part of the ISOC Internet Governance Forum (IGF), structured around a main event and several satellite workshops (RGPD, Cyber-security, IPv6, etc.)[51]. The "IP♥6", workshop, which will be held on Wednesday, 10 October at Arcep's offices, will result in the creation of working groups of the various stakeholders (ISPs, web hosting companies, training organisations, government organisations, etc.) which will discuss concrete topics related to the transition from IPv4 to IPv6, and particularly:

- teaching IPv6: how to ensure that majority of the courses and exercises done by students concern IPv6 and not IPv4? How to distribute useful information to network engineers and technicians so that they can train themselves in IPv6?;
- the State must lead by example: what are the main hurdles hampering the deployment of IPv6 in federal e-government services? How to overcome them?
- phasing out IPv4: how to provide players with the clarity they need on the end of IPv4? What solution can be used to encourage those lagging behind to step up their transition to IPv6 as quickly as possible?

Registrations for the workshop are open on the ISOC's website[52]. Arcep heartily encourages all of the ecosystem's stakeholders to take part, regardless of where they are at in their transition to IPv6. Participants that so desire can take part of this widely covered event to announce any progress, past or future, they have made in their switchover to IPv6.

[51] The main IGF event will be taking place on 5 July 2018, from 9 am to 8 pm, at the Université Paris Descartes. Register at https://www.isoc.fr.
[52] https://www.weezevent.com/ateliers-de-l-avenir-numerique-internet-6

PART 2

ENSURING INTERNET OPENNESS

In addition to the raw performance of Internet accesses and the quality of connectivity, Arcep is the guarantor of equal and non-discriminatory treatment of all traffic.
To ensure that the principle of an open Internet is upheld all down the line, Arcep also examines the practices of other essential technical intermediaries.

4. Guaranteeing network neutrality

ARCEP'S PRESCRIPTION

Preventive actions have paid off. Follow the recommendations carefully to avoid a drop in blood pressure

1. NET NEUTRALITY AROUND THE WORLD

1.1. The United States revives the net neutrality debate

On 14 December 2017, US telecoms regulator, the Federal Communications Commission (FCC), adopted a text called *"Restoring internet freedom"*[53], proposed by its chairman, Ajit Pai.

The text seeks to fully review the *Open Internet Order*[54] of 2015:

- it re-qualifies Internet access services, which will no longer be protected under Title II (common carrier regulation), and once again become merely information services, which are far less regulated;
- the three main messages in the 2015 Order – prohibiting blocking, throttling and paid prioritisation – have been abandoned;
- the only obligation the FCC has kept, albeit relaxed, is to inform consumers on traffic management practices.

As a result, the FCC has reverted to having the Federal Trade Commission (FTC) enforce consumer protection and competition regulations, which are necessarily ex-post, contrary to what the FCC could have done.

This means that ISPs in the US are free to employ discriminating traffic management practices, and to design plans that treat or bill particular kinds of content differently, the sole condition being that they list these practices in their sales contracts. The arguments that the FCC Chairman has used to justify his actions are, paradoxically, rather similar to the ones employed by net neutrality's proponents:

- going back to a very relaxed regulatory framework which, according to him, has enabled the Internet to develop as it has;
- giving emphasis to permissionless innovation, but this time more for ISPs than CAPs.

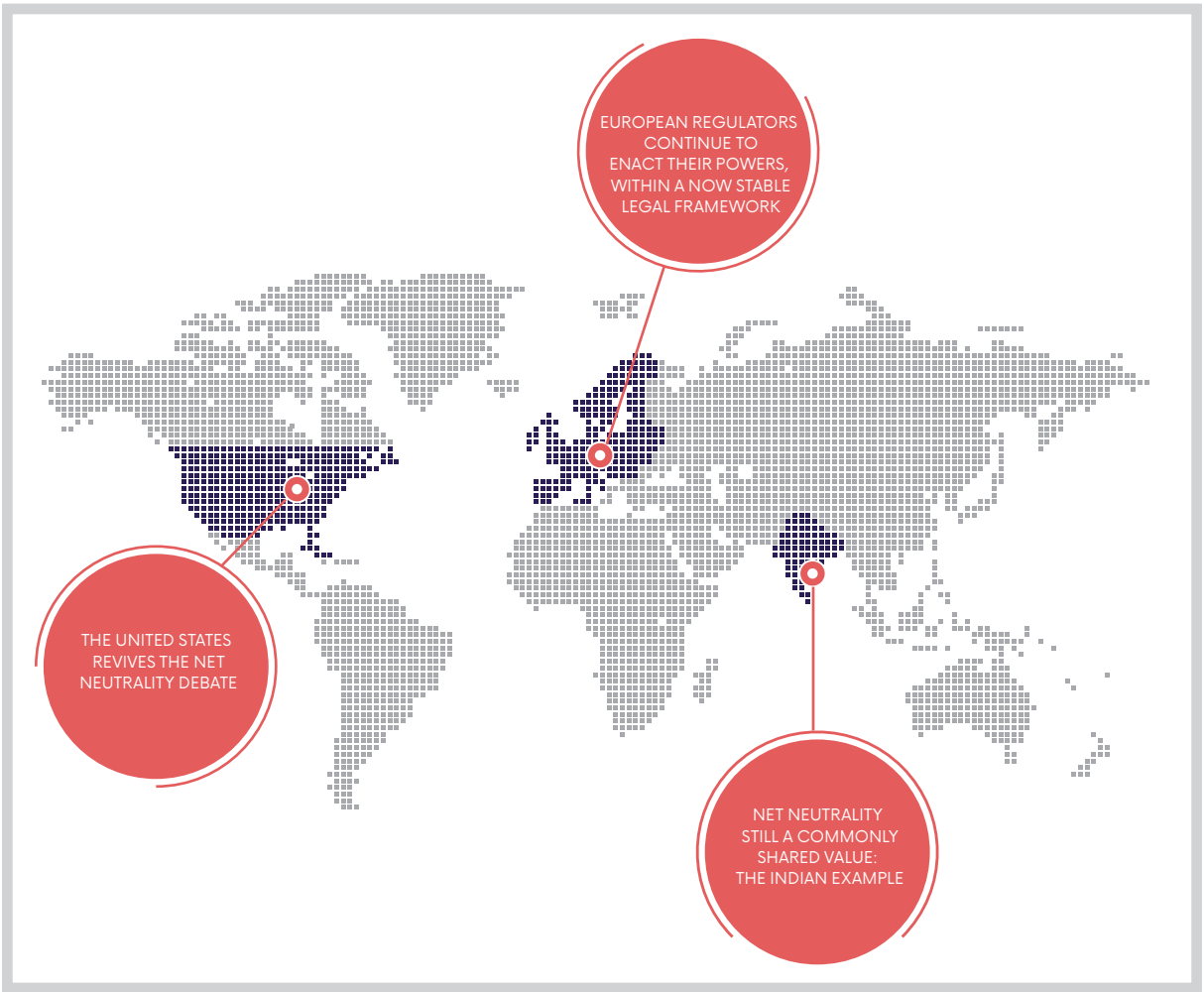
[53] https://www.fcc.gov/restoring-internet-freedom
[54] https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf

This radical change in regulation was hailed by certain ISPs in the US which echoed the FCC Chair's claim that it would help revive investment in the networks. But in the court of public opinion, there has been far more hostile opposition.

The opponents of the new FCC text have launched a number of initiatives:

- twenty two states have filed a federal suit against the FCC, as have some NGO (Public Knowledge and Open Technology Institute);
- as American law prevents the states from intervening directly on this issue that has been pre-empted by the FCC, the governor of Montana reinstated net neutrality in a roundabout way by incorporating it into the clauses of government tender contracts. Several other states and local authorities have followed suit;
- Washington State reinstated net neutrality provisions directly, and so contravening the FCC's pre-emption and thereby exposing itself to possible legal consequences. Oregon followed suit one month later;
- House Democrats have launched legal initiatives to restore net neutrality. Their success will depend on how much support they can garner from the Republican majority (close to 150 European MPs signed a petition calling for their support);
- some Republican representatives also wanted to introduce a bill to protect net neutrality, although it would be less strict that the former Open Internet Order (an approach that has the support of certain telcos, such as AT&T, which are weary of the constant back and forth on the matter).

This combination of challenges helps illustrate public interest in upholding net neutrality, and makes it difficult to predict what the American framework will look like in the medium term.



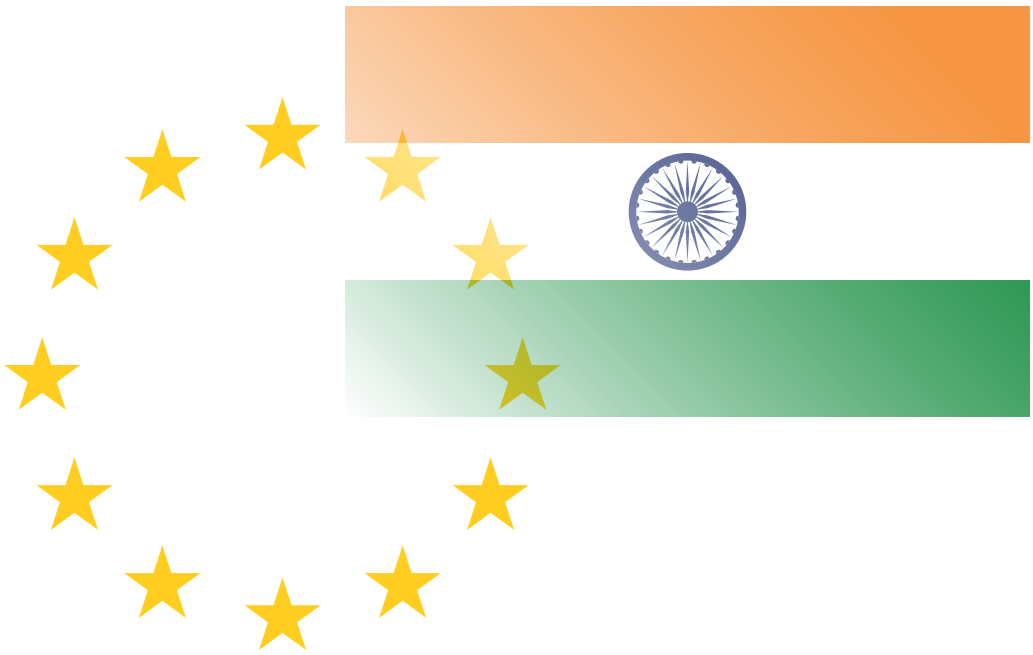
1.2. Net neutrality still a commonly shared value: the Indian example

In other parts of the world, efforts to protect net neutrality continue to make strides – a prime example being India, the world's largest democracy. On 28 November 2017, the Telecom Regulatory Authority of India (TRAI) adopted a series recommendations[55] designed to strengthen net neutrality.

The terms it chose are very close to the European Regulation of 2015, guaranteeing an open Internet in terms of both traffic management and specialised services. The TRAI establishes the principle of treating all traffic equally, while keeping the possibility of employing reasonable traffic management measures (which must be transparent, proportionate and non-discriminatory), as well as strictly supervised exceptional traffic management measures (corresponding to legal obligations or security imperatives). All of these elements are found in the European framework. And, like in Europe, the ability to provide specialised services is contingent on an objective technical need and the guarantee that it will not impede Internet access.

This new framework comes on top of the Decision of February 2016 prohibiting the application of any form of price differentiation in Internet access products (and so prohibiting zero rating), and thereby ensuring a very high level of protection for net neutrality in India.

India has thus become one of Europe's prime partners in the effort to further the principle of Internet openness around the globe. Cooperation with India has led to concrete actions such as the draft of a Memorandum of Understanding detailing the prospect of BEREC and TRAI working together on the issues of net neutrality and OTT[56]. This document is due to be signed at the second annual BEREC plenary meeting, in June 2018.



[55] https://www.trai.gov.in/sites/default/files/Recommendations_NN_2017_11_28.pdf
[56] See lexicon.

A PLEA FOR INDIAN-EUROPEAN COOPERATION ON NET NEUTRALITY

Amba UTTARA KAK,
Technology Policy Fellow, **MOZILLA**

The European example was a source of inspiration to the Indian regulator, and a support to various stakeholders that advocated for strong rules during the public consultation process. The greatest testament to this are the final provisions recommended by TRAI, which closely resemble those in the European Open Internet Regulation. For example, the important definitions of both "Internet access service" and "specialised services" are almost identical in the two texts. India and Europe now also have a similar legal standard for which traffic management practices may be considered reasonable – both require transparency and proportionality.

Given this common ground in their regulations, there is scope for European regulators and TRAI to cooperate on enforcement. Commercial practices like zero rating are relatively easy to monitor, but detecting technical practices like throttling and prioritisation continues to be a challenge. No regulator has found the definitive solution to detection, nor a fool-proof methodology for establishing violations. BEREC has taken the lead on developing and implementing net neutrality measurement tools, and the announcement of the tender has put the wheels in motion. It is hoped that the tools developed in this process will be based on open standards, so that regulators in India and elsewhere can benefit.

Beyond technical tools, transparency, and effective complaints procedures are paramount to faith in the regulatory process. BEREC sets a high standard with its meticulous review of national regulators' implementation of the Open Internet Regulation. User complaints are also a critical part of effective enforcement. ARCEP's convenient online complaints portal is another useful model for India to borrow from as TRAI looks to develop its own complaints mechanism.

Where India and Europe do diverge is their position on differential pricing practices. TRAI opted for a ban, rather than a case-by-case review, believing that the social costs on innovation would be difficult to quantify, and would not be captured in an ex post assessment. The BEREC has, for its part, put in place detailed guidelines for how to evaluate such practices and published a review of enforcement actions to date. This transparency is welcome, and essential to ensure that the flexibility in the Regulation is not misused. There may be value for both the Europe and India in monitoring the impact of these regulatory decisions in different jurisdictions.

As the Mozilla Manifesto notes, the Internet is a global public resource that must remain open and accessible. Creating common principles is critical to preserving its role as an engine of innovation. The hope is that India and Europe continue to cooperate on putting these principles into practice. Eventually, a coordinated response to net neutrality enforcement would give these regions a competitive edge in the digital economy.

"A COORDINATED RESPONSE TO NET-NEUTRALITY ENFORCEMENT WOULD GIVE THESE REGIONS A COMPETITIVE EDGE IN THE DIGITAL ECONOMY"


EVERYTHING YOU NEED TO KNOW ABOUT NET NEUTRALITY DEBATES
While the European Union enshrined net neutrality as a lasting tenet in its legal framework in 2015, the United States revised their position on the matter in late 2017, and so revived ongoing debates between the pros and cons of net neutrality. Arcep, which is responsible for enforcing the European Regulation, and therefore protecting net neutrality, has mapped out current debates.
Debates that can be distilled into five core issues.
Five arguments being made by both sides.
ANTI NN
PRO NN

1 THE WEB'S CORE VALUES

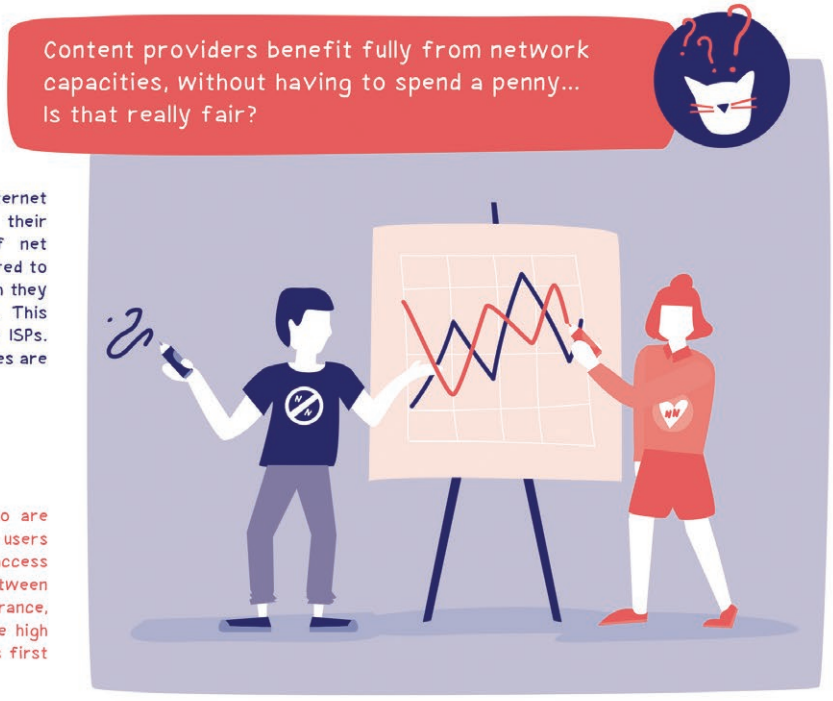
ANTI NN

The Internet developed on its own, without there ever being a need to give neutrality special protection. Net neutrality is a recent invention born of utilitarianism, created by those who want to do away with paying Internet access providers in exchange for using their networks.

PRO NN

Neutrality is entrenched in the web's founding premise: guarantee that all Internet traffic is treated and carried equally, regardless of its origin or destination. Popularised by Tim Wu in 2003, this concept reflects the values of openness that led to the internet's emergence and success. Today, protecting net neutrality has a democratic purpose: the internet has become an "essential infrastructure" in exercising freedoms, a public resource that States must regulate for the benefit of every user.

2 NETWORK INVESTMENTS



ANTI NN

YouTube and Netflix videos are forcing Internet service providers (ISPs) to increase their network's capacity. However, because of net neutrality, YouTube and Netflix are not required to contribute to these investments, even though they reap a sizeable portion of the benefits. This situation is no longer financially tenable for ISPs. Hence, when net neutrality protection measures are in place, investments decrease.

PRO NN

It is end-users, through their behaviour, who are driving the increase in traffic. And it is these users who pay ISPs through their internet access subscriptions. It is hard to find a causal link between net neutrality and decreased investments: in France, spending on networks has been at an all time high since 2015, when net neutrality regulation was first adopted.

3 INNOVATION, 5G AND THE INTERNET OF THINGS

ANTI NN

Net neutrality prohibits traffic streams from being prioritised, and so impedes innovations that should be able to benefit from this special treatment, such as autonomous cars, remote surgery, etc. If Europe lags behind the United States and China in developing 5G and the applications it enables, it is because of the European Open Internet Regulation.

PRO NN

The current regulatory framework enables quality differentiation to optimise certain services when deemed necessary. Only, the practice is regulated: players with the same needs must be treated equally, without discrimination. I.e. the same stable framework for everyone!

4 FREEDOM OF ENTERPRISE

ANTI NN

Net neutrality is tantamount to the regulator micro-managing ISPs. It is yet another regulation that prevents them from managing their networks as they see fit, to be entrepreneurs and offer users innovative products.

PRO NN

On the contrary, net neutrality means giving everyone the right to entrepreneurship, without having to ask ISPs' permission to innovate. It means preventing the ISPs' from becoming the gate-keepers of innovation. It is up to users to chose the services of tomorrow, and not to access providers who are likely to nip innovations in the bud, especially those competing with their own services (let us recall that Skype was forbidden by certain operators in its early days).

5

USERS' FREEDOM OF CHOICE AND FREEDOM OF EXPRESSION

Why would offering users access to content for free not necessarily be a good thing?

ANTI NN

If a plan offers subscribers the ability to use Spotify and not have that traffic deducted from their data allowance (a practice referred to as zero-rating), it is a very good thing, especially for users on a tight budget. Consumers also have the choice of whether or not to subscribe to plans that limit access to certain content. In a nutshell, as long as ISPs' behaviour is transparent, consumer choice is enough to steer the market. Hence, no need to impose net neutrality.

PRO NN

But there would need to be enough ISPs competing with one another, which is not always the case (in the United States, for instance). Even then, it is a deceptive generosity that creates a pretext for not increasing the data allowance attached to a plan, and which locks the users into the choices that their ISP made on her behalf. So they will eventually be deprived of access to any of Spotify's potential competitors that will have disappeared or been unable to emerge. Spotify is music, but imagine if the content being zero-rated was a single newspaper's website... then it becomes a question of freedom of expression and of information.

The paradox of net neutrality is that it is a framework, but a framework that unlocks and liberates: it regulates the way that ISPs design their products, to prevent incumbent players from foreclosing the market, and opens the way for innovation to thrive.

Net neutrality contributes to this newfound goal of making the internet a common good.

arcep

2. EUROPEAN REGULATORS CONTINUE TO ENACT THEIR POWERS, WITHIN A NOW STABLE LEGAL FRAMEWORK

In Europe, as the legal framework that guarantees net neutrality is now stable and well understood by all, regulators are fully committed to enforcing the Open Internet Regulation. The centrepiece of BEREC's actions has been sharing best practices on a very wide variety of matters, as 2017 was the first full year of enforcing the Open Internet rules that came into effect in 2016. Developing supervisory tools, a homogenous interpretation of the Regulation and its guidelines with respect to concrete practices from the sector and their tremendous diversity: it has been especially useful to pool experiences over understanding this new framework.

Arcep was especially involved in this work throughout 2017, notably because Arcep's Chairman, Sébastien Soriano, was also the Chair of BEREC that year. A sign of the ongoing commitment to his work, the Chairman of Arcep is now the Vice-chair of BEREC for 2018, with special responsibility for net neutrality issues[57].

Throughout its term of office, Arcep lobbied for the principle of increased cooperation between National Regulatory Authorities (NRA) to analyse and handle cases of application of the Regulation, so that their decisions be based on the most homogenous reasoning possible. On the impetus of the French NRA, a rigorous and systematic process for sharing case studies was developed in late 2017. It contributed to achieving the high standard of dialogue within the working group devoted to net neutrality.

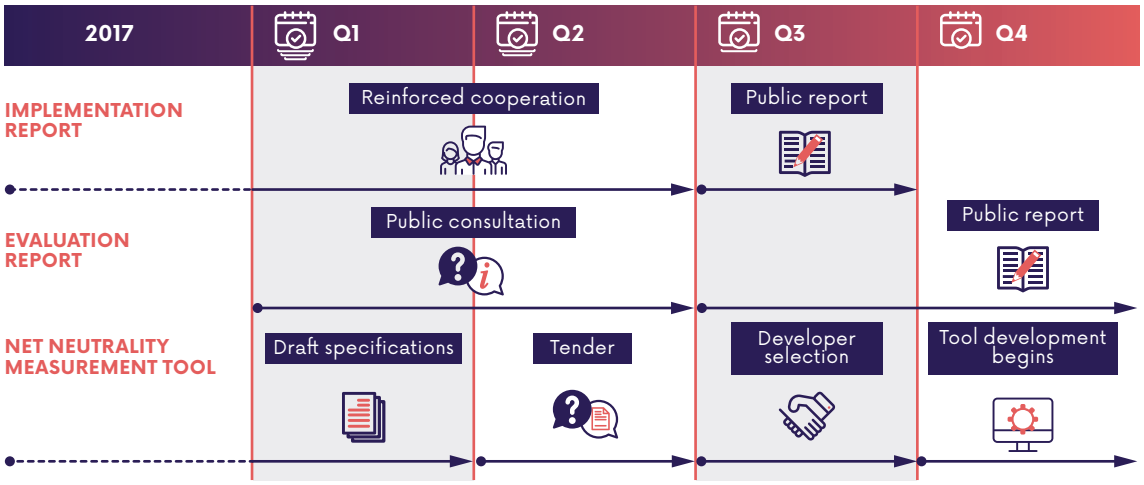
In addition to the ongoing sharing of experience, the working group drafted two reports that were published in late 2017. The first provides a consolidated account of the actions that European NRAs have taken on net neutrality. Because this "implementation" report is to be an annual publication, a similar one will be delivered in late 2018. The second report provides an overview of the tools and processes that can be used to monitor behaviour in the marketplace, and ensure the Regulation is applied as well as possible[58]. It draws not only on experiences in Europe, but also on a benchmark of actions taken by other regulators around the globe. It puts particular emphasis on the value-added of having a multiplicity of sources of diagnosis, for instance turning to crowdsourcing to develop tools either in-house or through partnerships, which thus largely validates Arcep's approach.

In 2018, in addition to producing the implementation report, BEREC has the task of publishing an opinion report as part of the European Commission's future assessment of the Open Internet Regulation. Combining all the NRAs' experiences in enforcing the Regulation should enable the Commission to determine whether the current framework has achieved its objectives, or whether some provisions need to be more finely tuned. Because this is such an important issue, a public consultation was held from mid-March to mid-April 2018 to gather feedback from the sector's stakeholders, who were asked to share their experience in enforcing net neutrality. Processing these responses will provide BEREC with a detailed analysis of the effects that the legal framework has had on the economy, and allow it to better contribute to this very important milestone for the future of net neutrality in Europe.

Following through on the work done last year, the development of a common tool for measuring quality of service will get properly off the ground with the selection of a developer to design the tool, in mid-2018 (cf. chapter one). This tool, which NRAs will adopt on a voluntary basis, could eventually become an important element in Arcep's diagnostic capabilities.

[57] Sébastien Soriano is also in charge of mobile and international relations issues.
[58] http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/7530-berec-report-on-tools-and-methods-used-to-identify-commercial-and-technical-practices-for-the-implementation-of-article-3-of-regulation-20152120.

BEREC NET NEUTRALITY WORK PROGRAMME



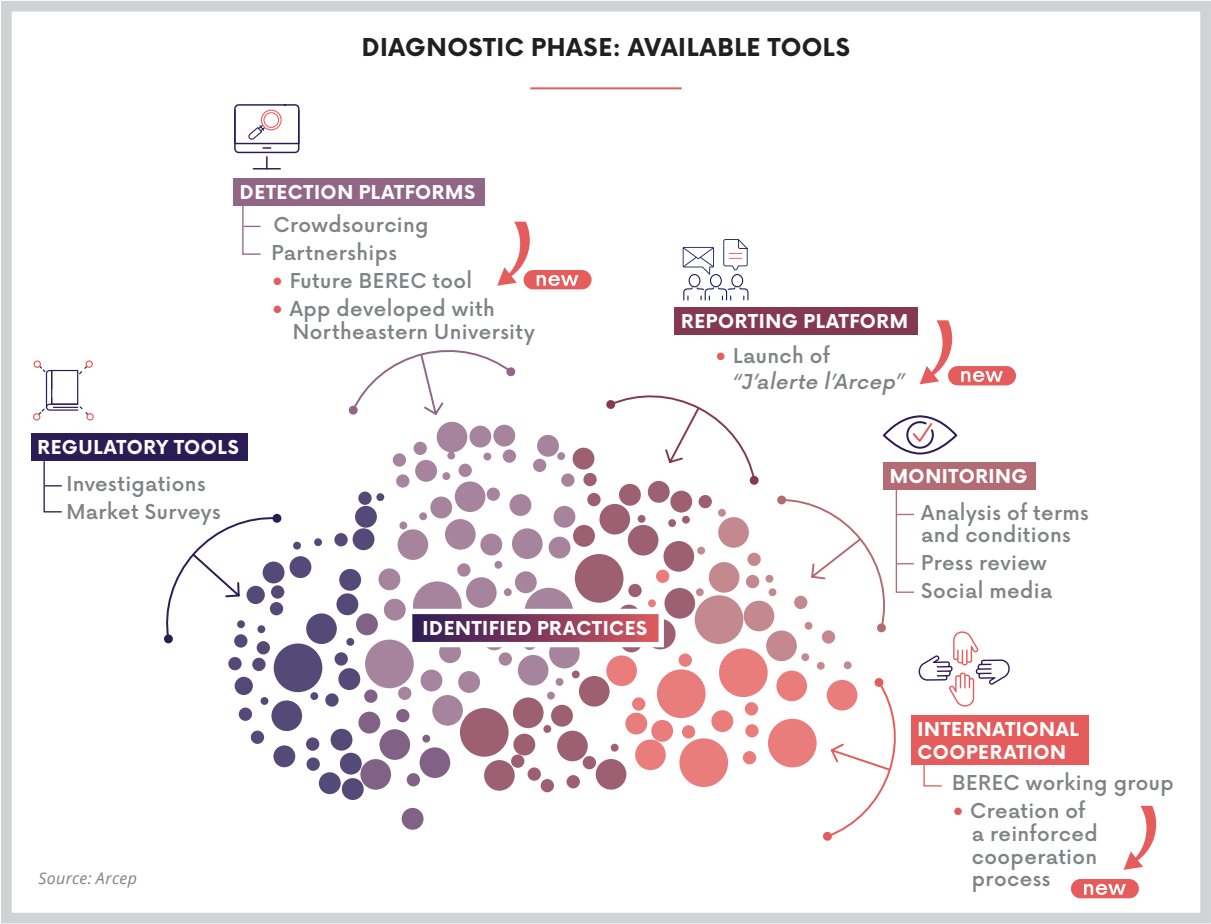
Source: Arcep

© Kaspars Ilips Dobrovolskis

3. IN FRANCE, ARCEP IS FULLY COMMITTED TO ITS THREE-STAGE ACTION PLAN

3.1. Arcep's diagnostic capabilities expanding

Arcep's diagnostic process in detail



When releasing its first report on the state of the Internet in France last year, Arcep unveiled its net neutrality action plan to the public. This process includes an initial diagnostic stage based on several sources of information. Arcep will be fleshing them out in an ongoing fashion, to obtain the most detailed picture possible of marketplace practices with respect to the four cornerstones of the Open Internet Regulation: business practices, traffic management, specialised services and transparency obligations.

Once again this year, Arcep has implemented a number of tools that had already been employed, such as information gathering campaigns and careful monitoring of the French market. The competent Arcep body drew in particular on the general questionnaire on all of operators' practices that fall under the purview of the European Regulation and, since late 2017, on more specific questionnaires that enable the Authority to deepen its understanding of certain practices in particular.

In addition, new mechanisms have been introduced to complete Arcep's diagnostic capabilities.

The *"J'alerte l'Arcep"* user reporting site, which has a section devoted to net neutrality questions, was launched in October 2017. By April 2018, 367 reports had been logged in this section. If these reports are valuable to the extent that they allow Arcep to be informed of certain problematic situations, and to understand the concrete impact they are having on users' daily lives, they do not necessarily constitute net neutrality "infractions". Most of the reports filed in that section of the site concern quality of service issues on specific applications, which

may have several causes. These reports therefore need to be examined by an expert, to understand the ins and outs of the situation they describe, and to take the appropriate action if necessary. To give an example: the following section summarises the analysis performed by the competent Arcep body regarding the diminished quality of certain services of Free's network.

In addition, Arcep wanted to support the development of a traffic management detection app designed by Northeastern University. Once complete, it should enable any users wanting to test their line to detect certain traffic management practices that could "violate" Open Internet rules. The section below explains how it works. As mentioned in this section, a tool designed to detect other possible types of infraction is also being developed, through BEREC.

Lastly, and as stated earlier, Arcep recommended increased cooperation within BEREC, which came into effect in the second half of 2017. This ongoing dialogue, as much over the introduction of tools as technical-legal analysis of concrete behaviour, has enabled NRAs to project themselves into a wide variety of scenarios, beyond just their own national situation, and gain greater insight into the full scope of the Regulation and its impact on ISPs, CAPs and citizens.

Diagnosis and crowdsourcing: examples of co-development

In its 2017 report, Arcep presented a tool to emerge from university research that makes it possible to detect traffic management practices. Challenging to implement from a technical standpoint, this feature is absent from currently available tools, and from the first version of BEREC's common tools – which should be able to detect certain forms of blocking and interference, but not throttling. It therefore seemed worthwhile to Arcep that this academic project – which complements other projects as well – be able to continue its development. This is why Arcep has been supporting its completion, working in tandem with Northeastern University, since early 2018.

This is a crowdsourced tool, and available to all consumers. Data generated by the tests conducted by users will be transmitted to Arcep, which will then have a general overview of any irregularities that arise. Should repeated and corroborated irregularities occur that would appear to indicate that they are not temporar[59] but rather structural, the regulator could, if necessary, decide to pursue its investigation through existing regulatory tools, such as investigative powers and the power to impose penalties. This new distributed tool will thus empower consumers, and make each one an integral part of the regulatory process, and able to strengthen the body of evidence that triggers Arcep's actions.

Several projects are currently underway, as part of the collaboration between Arcep and Northeastern University: increasing the tool's reliability by reducing the number of false positives, developing new features such as identifying the use of DPI , translating the tool and hosting it in France, as well as more forward-looking features.

From a technical standpoint, the tool has evolved slightly from the mechanism presented last year: removal of the VPN that created a number of not useful complexities, replaced by a stream encryption system that reverses the bit order, which does the same thing more simply. Also worth noting is that the first version of the tool specifically targeted traffic identification by DPI[60], and so traffic management techniques that would be based on that traffic identification process.

By lending its support, Arcep hopes to help create a richer, more reliable tool than the already innovative and promising one that exists, and so take a first step towards making powerful detection tools available to end users and regulators.

[59] I.e. linked to the network's status at a given moment in time.
[60] Deep Packet Inspection.

BETWEEN ACADEMIC RESEARCH AND PRACTICE: PUTTING APP DEVELOPMENT TO THE TEST

Dave CHOFFNES, **NORTHEASTERN UNIVERSITY**

Northeastern University

What kind of net neutrality violations can be detected with your tool?

Wehe detects when a network provider gives different performance to an application's traffic based solely on the contents of that traffic. We can detect behaviours such as throttling (i.e., limiting the bandwidth available to) video traffic or increasing delay to VoIP calls. We cannot detect net neutrality violations such as paid peering or unfair congestion management schemes, which do not depend on the content of network traffic.

Has your tool already made it possible to highlight such practices?

Yes, Wehe has found net neutrality violations in 22 ISPs worldwide. We typically see that video is throttled, reducing the maximum video quality that a subscriber can receive. We have also seen Wehe used for detecting censorship, for example in the United Arab Emirates where Skype is blocked.

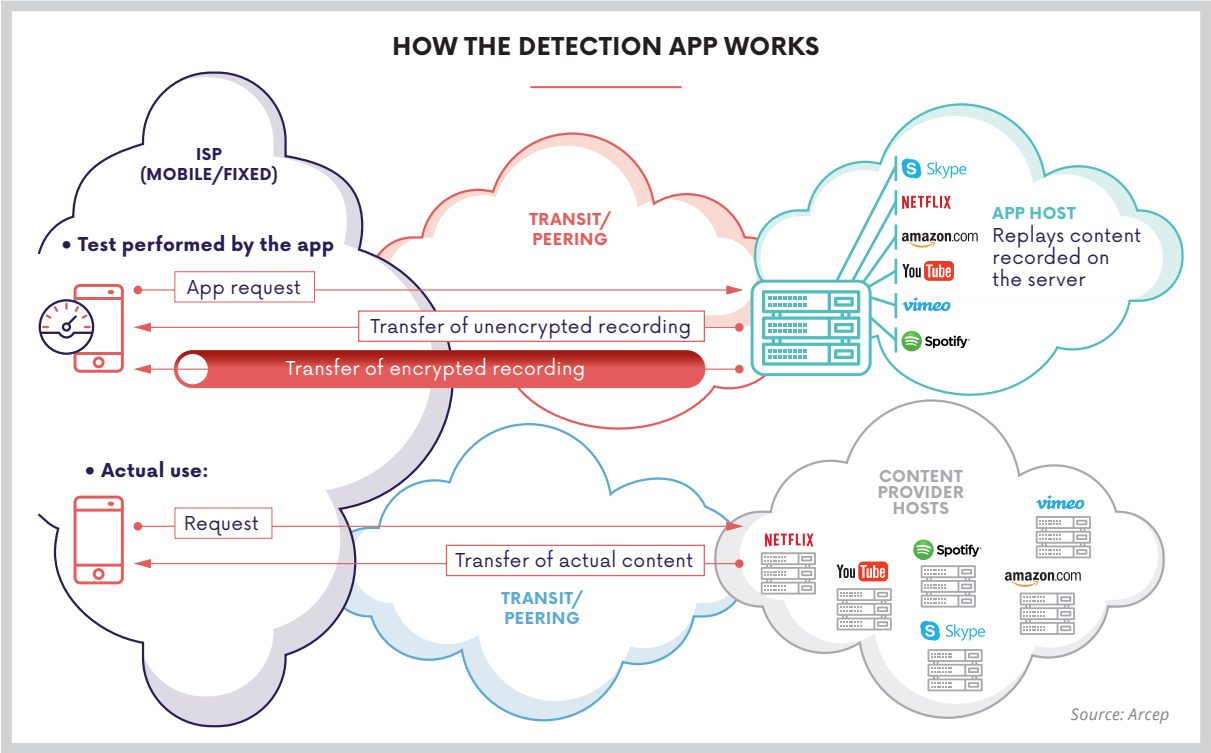
"OUR APPLICATION HAS FOUND NET NEUTRALITY VIOLATIONS IN 22 ISPs WORLDWIDE."

Can you come back to the difficulties you encountered when launching the iOS version of your application?

After several weeks of review and responses, Apple insisted that our app did not work as claimed (they thought it was a simple speed test) and thus it was rejected with no reasonable explanation. We were stunned by this lack of transparency, so we contacted Arcep for help and posted our story on Twitter. Fortunately, within a day Arcep scheduled a meeting with Apple representatives and a news story on the topic rose to the top of Reddit. With mounting pressure, Apple revisited their decision and approved the app.

We are grateful to have partners like Arcep and broad support from the public to help raise the profile of our app rejection. However, we are also keenly aware that a large number of other apps get rejected without anyone noticing. While we understand that Apple must carefully evaluate apps to ensure they are not misleading or fraudulent, there is a clear need for more transparency and productive dialogue in the app review process.

© Fotolia/Gorodenkoff



3.2. Arcep making strides in its analysis and enforcing compliance on identified practices

Arcep continues its work on several practices at the national level...

2017 was devoted largely to identifying the sector's traffic routing practices on networks, and the first general questionnaires circulated by the competent Arcep body brought in a wealth of information. It was able to analyse this material and to set it against the principles of the Regulation. After this, it seemed like an opportune time to look closely at the use of certain practices which have been the subject of dedicated questionnaires in late 2017, that sought to deepen existing information on the matter. Following through on what had been announced in last year's report on the state of the Internet in France, the competent Arcep body set out to examine the issue of freedom of choice and use of terminal equipment in ISPs' plans, and especially whether certain limitation clauses in users' contracts were compatible with the provisions contained in Article 3.1 of the Open Internet Regulation. These restrictions apply in particular to the use of tethering (completely forbidden or subject to data caps), and the inability to use Internet access services with certain types of devices (tablets, 4G cards, connected objects, 4G boxes, etc.). Arcep has noted that clauses limiting the use of tethering and prohibiting the use of SIM cards in any device will be removed from the concerned ISPs' contracts by autumn 2018. On the matter of fixed 4G products, Arcep notes that it is still a nascent market, and it will keep a close watch over how these products develop, and the resulting issues for consumers.

By the beginning of 2018, in the wake of numerous public requests and a groundswell of input on the *"J'alerte l'Arcep"* platform, the Authority wanted to obtain additional information on the reasons for the poor quality of certain particular online services on the network of the ISP Free. These recurring speed and accessibility problems appeared to affect several popular online services, starting with Netflix, and account for a sizeable percentage of the user reports posted in the net neutrality section of the *"J'alerte l'Arcep"* portal. In light of the elements obtained by the competent Arcep body, interconnection of Free's network with the rest of the Internet may be one of the causes. Contrary to other large ISPs, Free's access to the bulk of global traffic relied heavily on a single transit provider, and some of that provider's links are overloaded on a very regular basis. As a result, without there necessarily being any traffic management issues in play, the most bandwidth-sensitive services such as video streaming can experience quality issues when the lines are saturated, regardless of the end customer's theoretical access speed. Moreover, the actual quality of

service the consumer experiences depends on all of the players (ISPs, transit providers, content providers, etc.) along the technical chain, between the end-users and the content they consume. The competent Arcep body wants to expand its requests for information to other players along this chain. Furthermore, as stated in Chapter 2, interconnection methods vary (transit as well as direct relationships such as free and paid peering) and make it possible to satisfy different needs. Recently, the press revealed ongoing negotiations between Free and Netflix and the establishment of a direct interconnection, which could lead to an improvement of quality for end-users. Arcep will be monitoring the situation's evolution in the coming months.

Arcep was also solicited by the firm Inmarsat to discuss their current in-flight Wi-Fi products and their potential development. This discussion provided Arcep with an opportunity to issue a reminder – as it had done last year regarding national railway company SNCF's Internet access offers – that the Regulation applies not only to the products sold by traditional ISPs, but also this type of access offering that Arcep considers as being a publicly available service. Because in-flight Wi-Fi is by its very nature a transnational issue, on Arcep's initiative the topic was also raised in the BEREC expert working group, which tends to view this type of offer as being a publicly available service, and thus subject to the provisions of Europe's Open Internet rules. Based on the elements that have been brought to Arcep's attention, the products that Inmarsat has currently deployed on European airlines comply, *a priori*, with net neutrality Regulation.

… and is deeply involved in the work being done at the European level

Arcep welcomes the overall strong degree of cooperation within BEREC on implementing the EU's net neutrality Regulation. For more information on the first year of implementation, readers can refer to the report that BEREC published in late 2017[61], which provides a complete account of the work performed at the European level.

2017 was especially marked by the spread of zero-rating offers that allow subscribers to use one or more particular online services without the traffic being counted against their allowance. The European Regulation does not prohibit zero-rating per se, but recommends to analyse it on a case-by-case basis. NRAs must therefore assess how each of these offers affects the content market and consumers' rights. They also need to ensure that zero-rating does not go hand in hand with discriminatory treatment of the targeted content, i.e. given priority over other applications or, on the contrary, throttling quality to prevent it from eating up too much bandwidth.

Lastly, NRAs also work to ensure that these offers are available under the same terms and conditions in every country covered by the principle of roam-like-at-home, contained in EU Regulation 2015/2120[62].

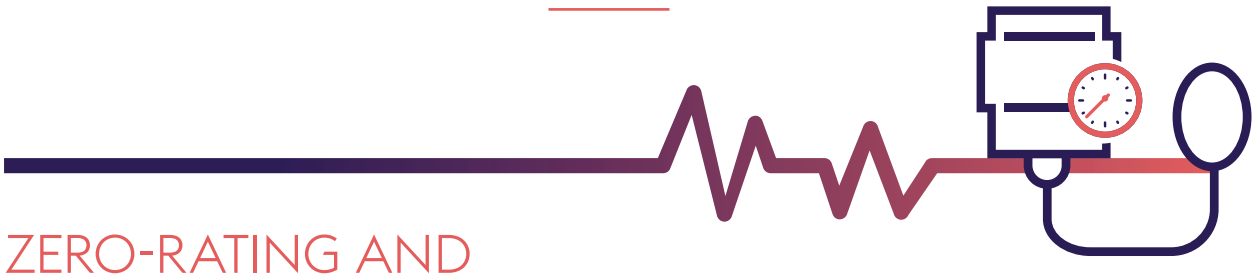
Among the many zero-rating offers to emerge, several have attracted the attention of regulators :

- Deutsche Telekom, with its *Stream On* plan (in the Netherlands, then Germany and perhaps soon in Austria and Hungary), which was the first to attract media attention in Europe, and stands out for also having been talked about on the other side of the Atlantic;
- Vodafone, with its *Vodafone Pass* service, which has been introduced by several of its European subsidiaries;
- Meo, in Portugal, and its "packaged" data pricing which is relatively close to zero-rating. It was cited by a Member of the House in the US, which earned it some media coverage.

With all of these products, an entire category of application (video streaming, audio streaming, social media, etc.) enjoys zero-rating. It is, however, difficult to assess whether they are open to any CAP: it is virtually impossible for small content and application providers to be aware of all the zero-rating plans available in Europe – and potentially around the globe – in which they may be included, nor to have the means to query every ISP involved. It is therefore possible that this type of plan, even the ones that are theoretically open to all, will eventually be more beneficial to the biggest CAPs, at the expense of smaller newcomers. Most of the regulators that have begun to tackle this issue have said that they are keeping a close eye on the market's development.

Given how challenging this exercise is, especially with respect to the impact of zero-rating on the upper end of the content market, there is an especially acute need for the value-added of increased cooperation within BEREC to obtain detailed analyses of these products.

[61] http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/7529-berec-report-on-the-implementation-of-regulation-eu-20152120-and-berec-net-neutrality-guidelines
[62] https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32015R2120&from=FR



ZERO-RATING AND THE "MINITELISATION" OF THE INTERNET

Luca BELLI, Senior Researcher,
FONDATION GETULIO VARGAS, CENTER FOR TECHNOLOGY & SOCIETY

The emergence of Zero Rating (ZR) offerings in numerous countries has triggered a new breed of Net Neutrality debates, focusing on the impact of price discrimination [63]. ZR models are mainly implemented on mobile networks and are based on subsidising a limited set of applications, whose data consumption is not counted against the users' data allowance. To understand the raise of ZR, four factors must be considered.

First, the Internet is increasingly accessed *via* mobile and wireless devices that, by 2020, will generate two-thirds of total IP traffic [64]. Second, service differentiation is becoming a key strategic objective for many operators that are vertically integrating with content and application providers. Third, personal data are the "world's most valuable resource" [65] and, in order to collect them application providers, notably the wealthiest, are becoming ready to sponsor users' access to their applications. ZR models emerge in the context of a "Scramble for Data," [66] where market players struggle to capture users' attention and, consequently, their personal data. Lastly, application providers increasingly aim at "hooking" [67] individuals into their services, through addictive [68] application configurations. Thus, the sponsorship of application increasingly aims at creating user-dependency on such application.

In this context, the purpose of ZR offerings may be to steer users' Internet experience towards the mere use of sponsored services. Particularly, when subsidised access to a few applications is combined with the imposition of limited data caps, Internet users – especially the less wealthy – may have a strong incentive to access only sponsored applications.

By sponsoring a limited selection of applications while foreseeing a payment for open Internet access, there is a tangible risk of "Minitelisation" [69] of the Internet. This phenomenon would consists in the Internet's evolution from a general-purpose network into a predefined-purpose network, where Internet users become passive customers of preselected services, rather than being "prosumers", i.e. individuals free to produce, besides consuming, innovative services and content.

Regulators should scrutinise ZR practices to guarantee they do not reduce Internet openness, competition, innovation and users' rights, which are the fundamental goals of Net Neutrality.

To have a better understanding of the different ZR offerings and of the regulatory and market contexts where they are available, the Dynamic Coalition on Network Neutrality [70] of the UN Internet Governance Forum (IGF) [71] has launched a crowdsourced Zero Rating Map [72], presented at the IGF 2017 [73]. The Map is a living tool that can be updated by any interested individual and has already allowed collecting information on ZR in 90 countries, including what applications are zero-rated and whether Net Neutrality is regulated in countries where ZR plans are available. The Map allows identifying some interesting elements.

The most zero rated applications are part of the Facebook family with Facebook being the most zero rated application. This is mainly due to Facebook's Free Basic programme and Internet.org initiative that sponsor access to a varying set of applications – amongst which the only constant is Facebook – in many developing countries.

The majority of countries where ZR offerings are available do not have Net Neutrality regulation while some operators combine vertically integrated applications and limited data caps in their ZR plans, even when Net Neutrality regulation is in place.

Given the impact that ZR practices may have, regulators should remain vigilant, refining and expanding the criteria [74] and tools necessary to monitor these practices. The social, political and economic relevance of an open Internet ecosystem is too high to allow its transformation into a collection of Minitels.

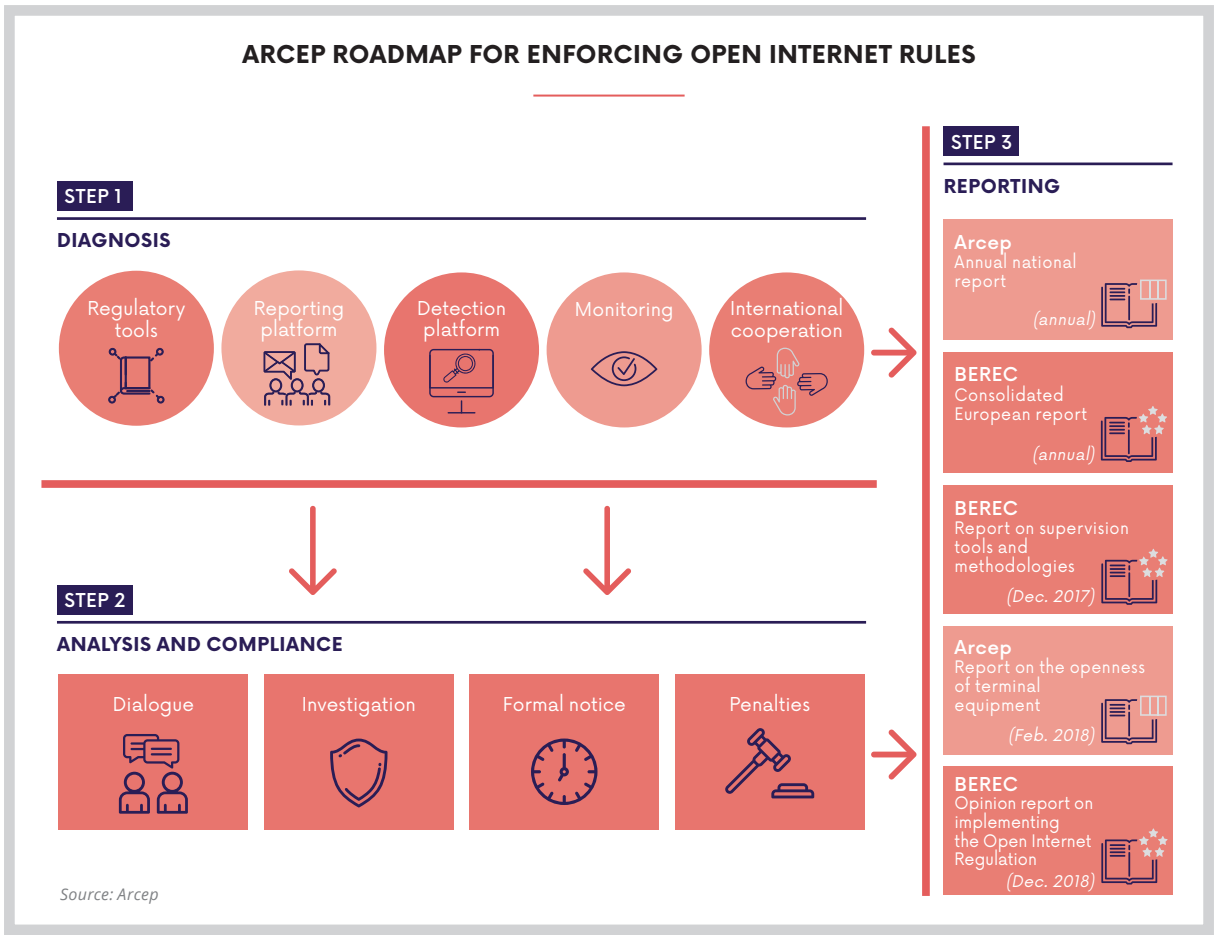
[63] Luca Belli (Ed). (2016). Net neutrality reloaded: zero rating, specialised service, ad blocking and traffic management. Annual Report of the UN IGF Dynamic Coalition on Net Neutrality.
[64] Cisco (2016) Cisco Visual Networking Index: Forecast and Methodology, 2015–2020.
[65] The Economist (6 May 2017). The world's most valuable resource is no longer oil, but data.
[66] Luca Belli (15 December 2017). The scramble for data and the need for network self-determination. openDemocracy.
[67] Nir Eyal (2014). Hooked: How to Build Habit-Forming Products.
[68] Tristan Harris (18 May 2016). How Technology is Hijacking Your Mind—from a Magician and Google Design Ethicist.
[69] Luca Belli (2017). Net neutrality, zero rating and the Minitelisation of the internet. Journal of Cyber Policy. Vol. 2. N°1.
[70] http://www.networkneutrality.info/
[71] http://intgovforum.org/
[72] www.zerorating.info
[73] http://sched.co/CTsC
[74] BEREC (2016). BEREC Guidelines on the implementation by national regulators of European net neutrality rules. BoR(16)127. Pp 12-13.

3.3. The reporting phase: a demand for transparency towards the regulator and an opportunity to establish a doctrine

As explained in the report on the state of the Internet in France in 2017, the third stage of Arcep's actions is the reporting phase. This reporting takes place at the national level, through this report, then at the European level, with the consolidated report by European NRAs (implementation report referred to above). These reports are a way of providing lawmakers and the public with an account of how the Open Internet Regulation is being implemented. The first European report on the matter, published in December 2017[75], describes the many actions that Europe's NRAs are taking, and how they are working to achieve a consistent enforcement of the legal framework across the EU.

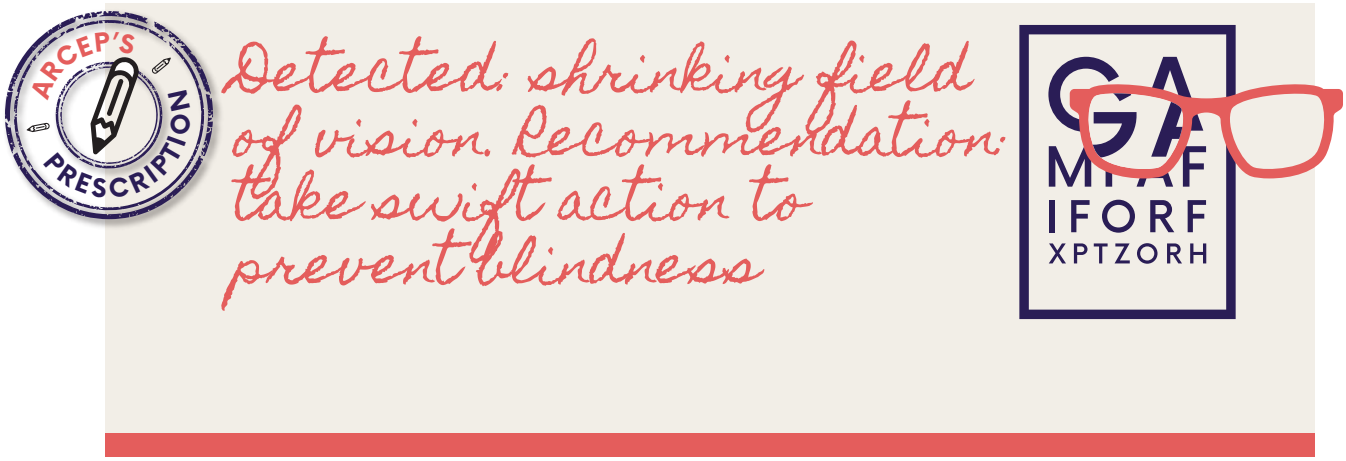
Furthermore, NRAs' combined experience on the net neutrality issue provided fodder for the more in-depth reports on certain topics that were relevant to the open Internet issue: e.g. the report on the supervision tools and methodologies published in December 2017 and the opinion report on the evaluation of the open Internet Regulation, mentioned above.

Finally, Arcep has begun ad-hoc work at the national level on matters concerning Internet openness. Arcep thus explored the issue of applying the open Internet principle to the different links in the Web's chain of technical intermediaries, and particularly to devices. This work resulted in the publication of a dedicated report in February 2018 whose conclusions are summarised in the next section.



[75] http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/7529-berec-report-on-the-implementation-of-regulation-eu-20152120-and-berec-net-neutrality-guidelines

5. Fostering the openness of terminal equipment

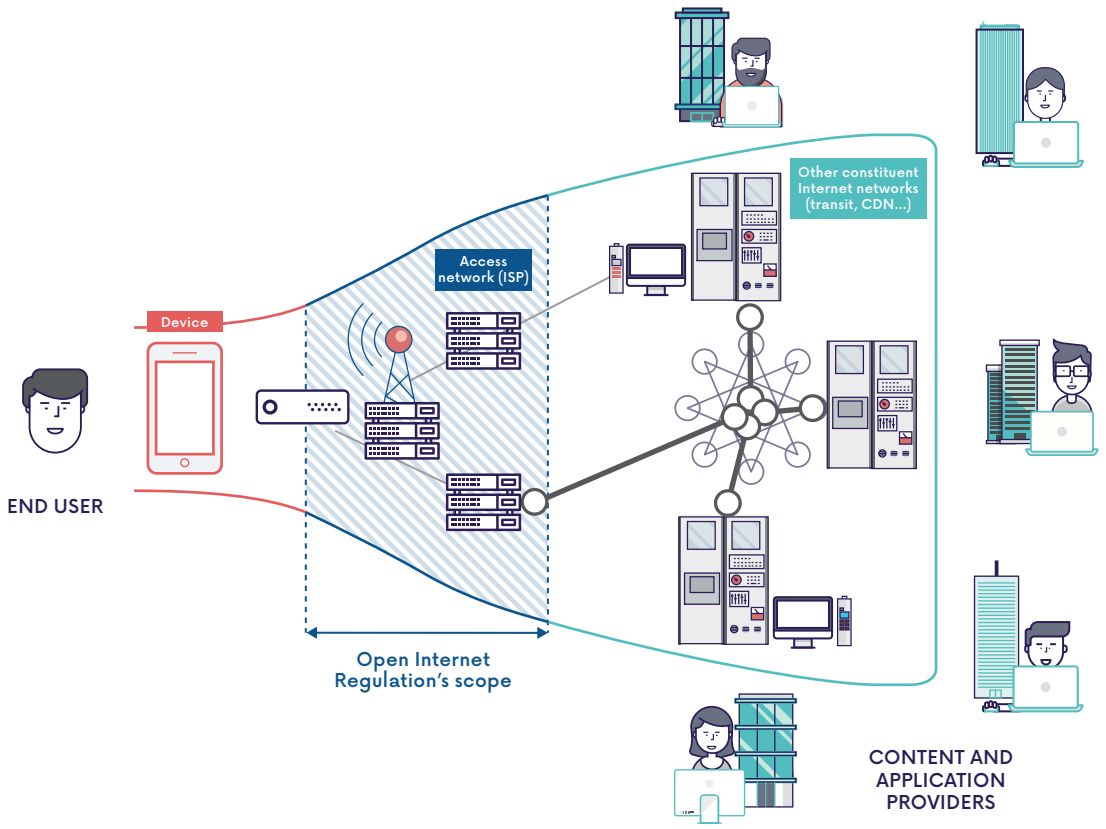


Although it introduces the umbrella principle of an open Internet, the European Regulation essentially contains measures that focus on the neutrality of ISPs' networks. But the ability to access the Internet and provide content relies on a much larger chain, in which other stakeholders also play an important role. Such is the case with terminal equipment that can limit end users' ability to access or provide certain services or content online.

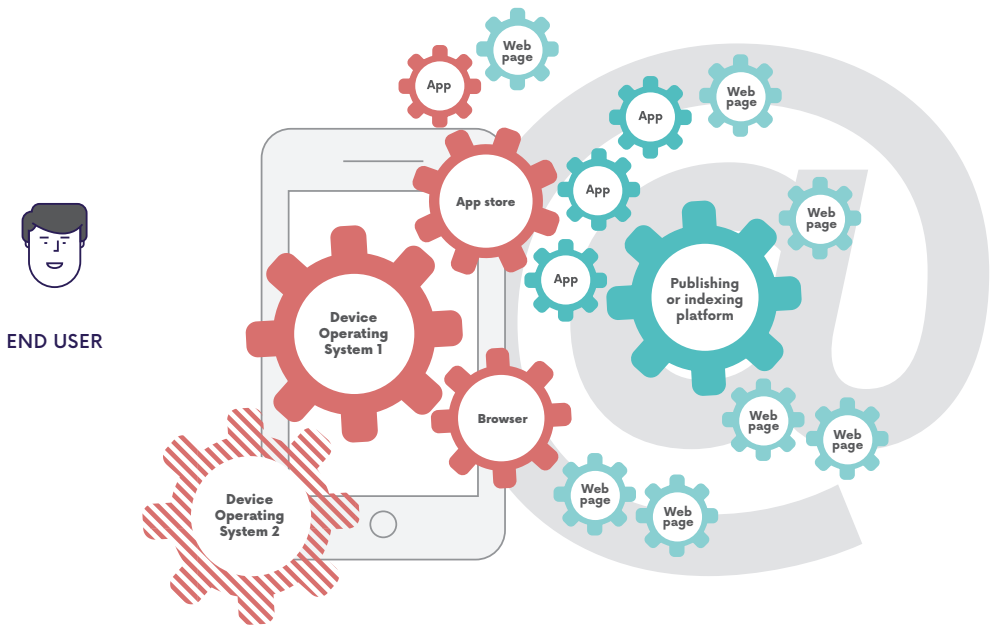
1. ARCEP SCRUTINISES TERMINAL EQUIPMENT, PRESENT AND FUTURE

Devices are located at the networks' extremity. Essential hardware and software links in the technical Internet access chain, devices, and especially their operating systems (OS), browsers and app stores, could undermine the Internet's openness.

HARDWARE LINKS BETWEEN END USER AND INTERNET



SOFTWARE LINKS BETWEEN END USER AND CONTENT



The rapid dissemination of new smart devices only increases this risk. After smartphones and tablets, voice assistants, for instance, are starting to attract users wanting to connect to the Internet. For now, smartphones are still the most popular device, being used by 48% of Internet users in France in 2017 to connect to the web, ahead of computers and owned by 73% of people in France, compared to 17% in 2011.

This is why Arcep wanted to expand its investigation into protecting Internet openness – of which it is the guarantor – to include terminal equipment, with particular emphasis on smartphones. This was the purpose of the examination of how devices affect Internet openness that it launched in 2017, following its strategic review.

The goal for Arcep is, first, to develop a common understanding of the issue by identifying and analysing any possible limitations to Internet openness that may be caused by devices and, second, to propose solutions that public authorities could bring to safeguard the principle of an open Internet. Devices were considered in their entirety, in other words both their hardware and software layers.

© IStock/PeopleImages

2. SUCCESSFUL MOBILISATION OF DIGITAL PLAYERS

To carry out this project, Arcep initiated a series of direct interactions with stakeholders – i.e. content providers, device manufacturers, OS developers, operators, consumer representatives – as well as players with a more overarching view of things: federal government representatives, consultants, lawyers and academics.

These interactions took on several forms. First, Arcep held two rounds of hearings in 2017 to allow each of the players to present their views on the matter.

Next, on three occasions, Arcep gathered different players around the table for more in-depth discussions on targeted topics:

- the workshop on 9 October 2017 Arcep brought together around a dozen content providers to think about the "ideal" way to make apps available, as much in terms of providing access to content as ensuring content providers' economic viability;
- the workshop on 13 November 2017 gave equipment suppliers and operating system developers the opportunity to deliver their diagnosis of the past, and engage in a forward-looking exercise on Internet access interfaces;
- the workshop on 24 November 2017, attended by consumer associations, was devoted to the challenge of data and content portability for users when switching devices, and especially when changing operating system.

Lastly, in late 2017 Arcep launched a public consultation for gathering stakeholders' feedback and to test out a set of initial proposals.

This multifarious dialogue led to the publication of a document on 15 February 2018[76], whose key findings were shared with the sector during an event at the Pan Piper[77], punctuated by debates with stakeholders.

[76] https://www.arcep.fr/uploads/tx_gspublication/rapport-terminaux-fev2018.pdf
[77] https://video.arcep.fr/fr/afterwork-devices-2018

STAKEHOLDERS AUDITIONED BY ARCEP SINCE 2017 FOR THE WORKSTREAM ON DEVICE OPENNESS

3. COURSES OF ACTION TO ENSURE AN OPEN INTERNET AND USERS' FREEDOM OF CHOICE

The process of drafting this report, and in particular the many interactions with stakeholders, enabled Arcep to map out a relatively large number of impediments to open Internet access that stem from devices. If some of these limitations can be justified by design, security or innovation reasons, others impede access to the Internet and its richness while offering nothing in exchange.

Having thus ascertained that the Internet's openness can be challenged by devices manufacturers and OS providers, Arcep set out a series of proposals in its report to guarantee an open Internet. The twelve courses of action are built around five main avenues:

1. clarify the scope of the open Internet by enshrining the principle of users' freedom to choose their content and applications, regardless of the device.
2. employ data-driven regulation and provide users, both consumers and businesses, with information that is both transparent and comparable;
3. safeguard market liquidity, by allowing users to move easily from one environment to another, and remain vigilant about anti-competitive behaviour;
4. lift certain restrictions that key device market players today are imposing on users and on content and service developers;
5. take swift action, thanks to an agile procedure for supporting businesses, and particularly SMEs and start-ups, when they encounter questionable practices.

Arcep recommends immediately implementing pragmatic and quick impact courses of action at the national level, with the goal of stimulating actions at the European level. It is participating as well in the work being done by BEREC, which also explored this issue in its report on the impact that content and devices have on the functioning of the telecoms market[78].

Arcep's investigation into devices did not end with the publication of this report. Stakeholders are encouraged to maintain their dialogue with the Authority, to share their experiences and their viewpoints, that to share how they see this issue evolving over time. New events dedicated to furthering this dialogue are expected to be held over the course of the year.

[78] BEREC report on the impact of premium content on ECS markets and effect of devices on the Openness of the Internet use.

MIXED VIEWPOINTS

Elisabeth BARGES,
Head of public policy, **GOOGLE**

In 2006, the idea of putting a computer in everyone's pocket still seemed like science fiction. Only 1% of the population had a mobile phone back then. At the time, the licensing fees and development costs of a proprietary system were high for manufacturers. Not everyone could afford the Internet. Faced with a fragmented market that was struggling to take off, Google and the mobile industry began investing together in 2008 to develop a unified operating system: Android.

Android is a free operating system that is available to device manufacturers under an open source license. They are free to download and use the Android source code as is, to modify it or even to use it to create a competing OS, as Amazon has done for its tablets. By reducing operating system costs, Android has helped democratise access to mobile phones, which can now be bought for less than 100 euros.
The Android model is built on a triple choice. First, manufacturers' ability to alter the operating system to create unique user experience. Second, manufacturers' and telcos' ability to choose the applications they want to offer users, as soon as they take their new mobile phone out of the box. Each is free to choose the applications or software suites they will install on a smartphone. They could pre-install (without exclusivity) Google's G Suite, or not. On average, close to 50 applications will be pre-installed, including several browsers and search engines, messaging apps, social media apps, etc. Third, Android offers users a choice. It is designed so that any pre-installed app can be deactivated, deleted from the home screen and replaced by another app. If it is installed, a user can thus replace Google Search with another search engine in less than 12 seconds. They can download any app from any source, from one of the hundreds of app libraries available on Android, or the developer's website. In 2017, more than 8 billion apps were downloaded every month from Google Play and over 50 billion from other sources.

Now, in 2018, the issues that existed when Android was first created still remain. Ensuring compatibility between devices to eliminate barriers to entry and strengthen data security are still top priorities for the ecosystem's players. The work that Arcep is doing thus provides a touchstone for finding future-proof solutions to these issues.

Paul KOCIALKOWSKI,
Head of Public Affairs for the Replicant project, **REPLICANT**

Arcep has been working on the issue of devices and how they impact Internet openness since 2017. European Regulation 2015/2120 stipulates that end users, "shall have the right to access and distribute information and content, use and provide applications and services, and use terminal equipment of their choice". As Arcep points out in its report, in practice this right is confined by the rules imposed by the makers of the devices that enable Internet access, be it restrictions created by the unique app stores for each platform (and restrictions on using alternative sources) or apps that are intrinsically linked to the system.

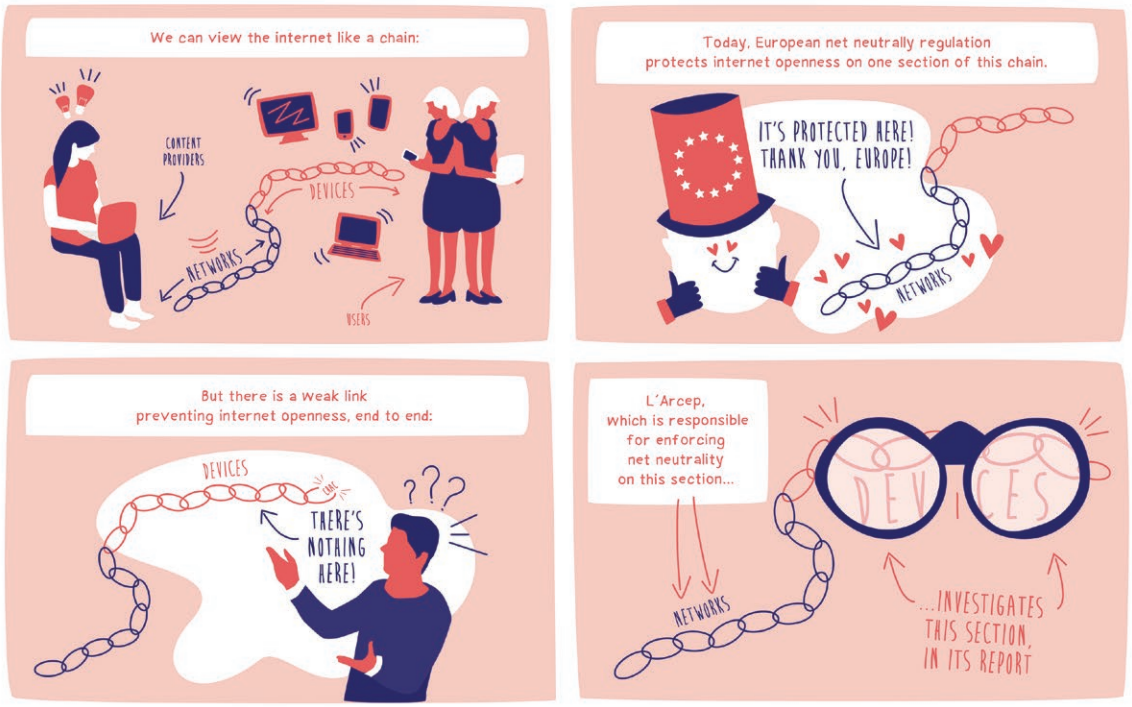
In addition to the rules established by the operating system that the manufacturer has pre-installed, is the issue of users' limited ability to install alternative systems. These systems provide different interfaces and software adapted to a variety of applications that the manufacturer may not necessarily have planned for, and that enable the emergence of new businesses and resulting services. They may also give users' increased control over the technology, through open source software. The diversification of these systems must nevertheless go hand in hand with standardisation of the interfaces, both on the service (making room for alternative software) and systems (enabling more generic applications) side, to reduce costs.

Replicant is an example of an alternative system, compatible with Android apps and composed entirely of open source software. Other systems, such as GNU/Linux distributions, make it possible to cover certain use cases such as providing services online, taking advantage of the network's ongoing deployment and devices' connectivity capabilities. The goal is to enable both entities and individuals to gain control over network transmission through their everyday devices.

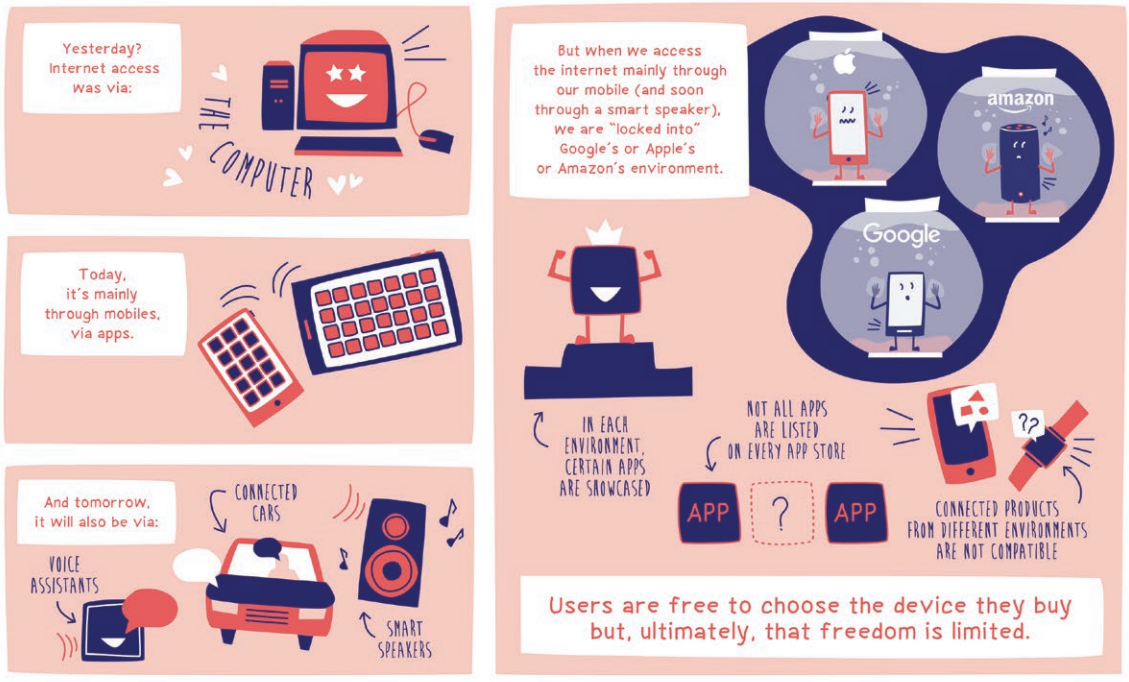
SMARTPHONES, TABLETS, VOICE ASSISTANTS...
Devices: weak link in open internet access

What if the internet you access depended on your brand of phone? Is your app store transparent? Is your voice assistant compatible with your music? In 2016, Arcep kicked off a series of meetings and workshops with stakeholders: equipment suppliers, developers, content providers... On 15 February 2018, Arcep is publishing its report and calling everyone's attention to the influence that terminal equipment has on internet openness, and to what actions might be taken.

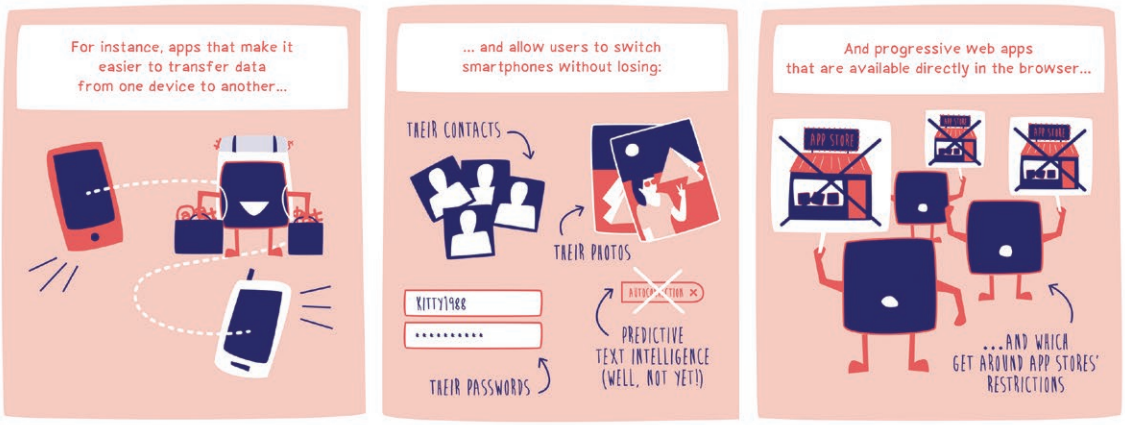
WHY IS ARCEP PUBLISHING A REPORT ON THIS TOPIC?



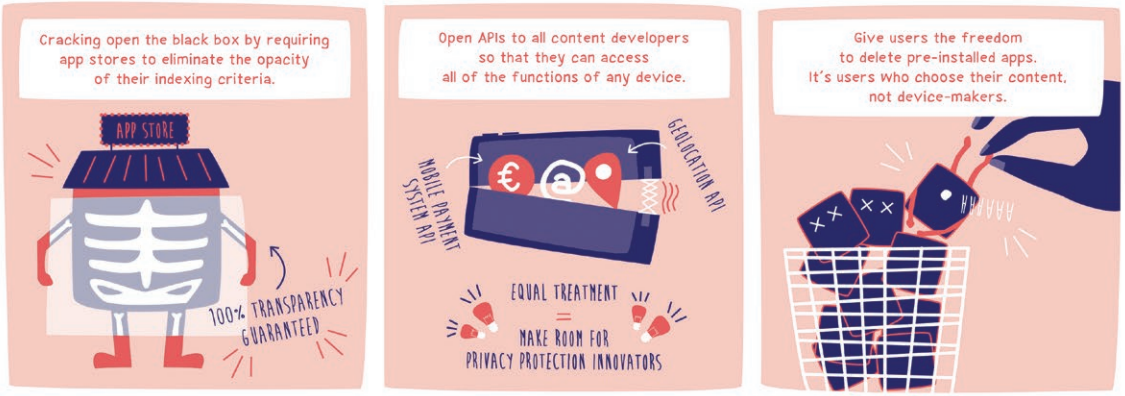
DEVICES ARE A WEAK LINK BECAUSE THEY OFFER ONLY LIMITED INTERNET ACCESS



SEVERAL INITIATIVES EXIST TO ADDRESS THESE LIMITATIONS, AND TO GIVE USERS BACK THE POWER OF CHOICE



IN ITS REPORT, ARCEP IS DOING ITS PART BY OFFERING CONCRETE COURSES OF ACTION, SUCH AS



FIND THE COMPLETE REPORT ON THE ARCEP WEBSITE

« Devices: weak link in open internet access » :

- A THOROUGH AND OPEN APPROACH
- IMPACT ON APP DEVELOPERS
- INTERNATIONAL PERSPECTIVE
- DETAILED COURSES OF ACTION

arcep

Lexicon

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

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

802.11ac: wireless transmission standard from the Wi-Fi family, standardised by the Institute of Electrical and Electronics Engineers (IEEE) in 2014. The most powerful standardised version of Wi-Fi in 2018 is 802.11ac.

Agent loaded on 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.

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.

Bitrate: quantity of digital data transmitted within a set period of time. Bitrates, or connection speeds, 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.

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: online 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: in Chapter 1, cross-traffic refers to 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: in Chapter 1, crowdsourcing tools refer to those instruments that centralise QoS and/or QoE tools performed by actual users.

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.

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

FCC (Federal Communications Commission): independent government agency in the US responsible for regulating electronic communications and radio and television content.

FTC (Federal Trade Commission): independent government agency in the United States, responsible for enforcing consumer law and supervising antitrust business practices.

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

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.

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.

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.

Multithread speed test: Internet speed test performed on several TCP connections at once.

NAS (Network Attached Storage): standalone file server, connected to a network whose main function is data storage.

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

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.

Peering policy: typically public reference document that contains operators' interconnection strategies.

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.

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.

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).

QUIC (Quick UDP Internet Connection): QUIC is an experimental protocol for transporting data on the UDP (User Datagram Protocol), developed and used by Google to reduce web page load times.

RDPI: Arcep body responsible for settling disputes, legal proceedings and investigations. It is composed of four members of the Arcep Executive Board, including the Chair, and rules on investigative decisions made in accordance with Articles L. 5-9 and L. 32-4 of the French Postal and Electronic Communications Code (CPCE), on dispute settlement decisions and decisions regarding potential penalty procedures (opening, formal notice, notification of grievances or dismissal, provisional measures).

Single thread speed test: Internet speed test performed on a single TCP connection.

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

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.

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.

TRAI: Telecom Regulatory Authority of India

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.

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.

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

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

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

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.

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.

Annexes

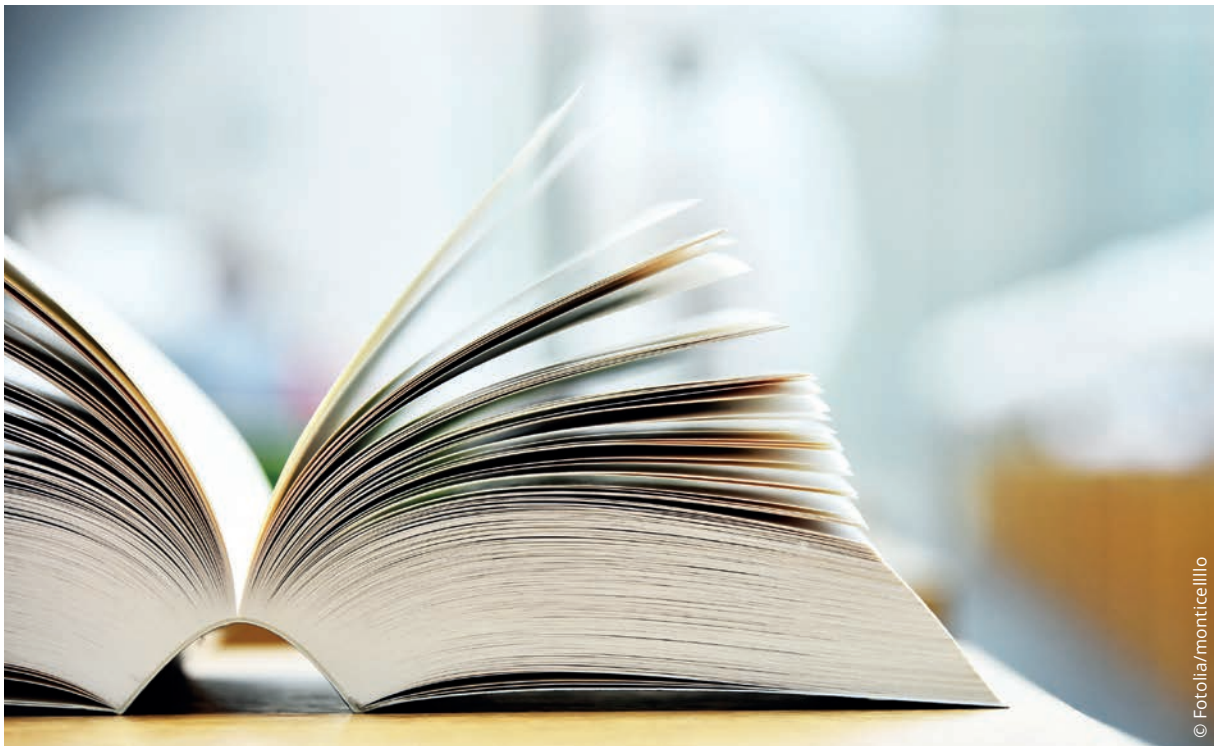
1. CODE OF CONDUCT – BETA VERSION

Arcep believes it is crucial that crowdsourcing tools' future publications be accompanied by transparent information on the choices they have made, so that any third party is able to explain the results obtained and any potential disparities between different publications. Although most of the choices that have been made have merit, some practices do seem more questionable, and warrant being modified.

Arcep would thus like to establish a "code of conduct" for players involved in measuring quality of service and of experience on the Internet, which would have two parts:

- a list of "transparency criteria" that are vital to understanding the published results of an Internet quality of service measurement, and which should accompany all published findings;
- a list of best practices that Arcep would like to see associated with certain criteria in particular.

Arcep intends for this code of conduct to evolve over time, in other words incorporate versions of new transparency criteria and newly identified best practices. This beta version of the code of conduct contains the transparency criteria and best practices that come as the direct result of the progress made on projects B and C. The ongoing work done on these projects, along with the other projects that are currently being put into place but equally vital (statistical representativeness, combatting fraud, etc.) will come to enrich future versions of this code.



1.1. Methodology for measuring technical indicators (speed, latency)

	TRANSPARENCY CRITERIA	EXAMPLES	ASSOCIATED BEST PRACTICES
BITRATE	Measurement protocols	TCP, UDP	-
	Ports used	80, 443, 8080, 8443	-
	Number of threads used (possible number of threads)	Single thread or multithread (accuracy on the number of threads)	-
	Test length or volume of data downloaded	Stops once one of the two thresholds has been reached: 10 seconds or 500 Mb	Test length > 7 seconds
	Stream encryption	Unencrypted, sslv3, tls1.2	-
	Slow start taken into account	Yes, no	-
	Internet protocol used during the test	IPv4 only, IPv6 on request, IPv6 systematically if available end-to-end	-
	Explanation of displayed indicators	Capacity, CBR, average, 90th percentile on transfer, median bitrate	-
LATENCY	Measurement protocols	TCP, UDP, ICMP	-
	Ports used	80, 443, 8080, 8443	-
	Number of samples	1, 2, 5, 10, 30 tests	Number of samples, at least equal to 10
	Time out	1 second	-
	Stream encryption	Unencrypted, sslv3, tls1.2	-
	Internet protocol used during the test	IPv4 only, IPv6 on request, IPv6 systematically if available end-to-end	-
	Explanation of displayed indicators	Minimum, average, 10th percentile	-

A speed test that is too short could affect its representativeness as it would only measuring bitrates as the connection is gathering speed when using TCP (slow start protocol).

As to measuring latency, a minimum number of samples is crucial to guarantee more reliable measurement of this indicator that varies a great deal depending on the network's status at any given time.

1.2. Methodology for measuring usage indicators (web browsing, video streaming)

	TRANSPARENCY CRITERIA	EXAMPLES	ASSOCIATED BEST PRACTICES
WEB BROWSING	Selection and number of sites tested	5 sites chosen at random from amongst 100; 10 popular sites	-
	Time out	5, 10, 15 seconds, no time out	Time out in less than 20 seconds
	Cache status	Cache empty or as is	-
	Explanation of displayed indicators	Complete page load, only the elements in the domain name, exclusion of advertisements	-
VIDEO STREAMING	Selection of videos tested	The most popular video in the country, with a resolution of at least 720p	-
	Number of threads used	1, 2	-
	Video testing protocol	http, https, QUIC	-
	Stream encryption	Unencrypted, sslv3, tls1.2	Same encryption as the one used by default on the platform being tested
	Video test length	30-second test, twice 10 seconds	-
	Video resolution	360p for the first video, 1080p for the second	-
	Explanation of displayed indicators	Number of playback halts, buffer fill	-

A too lengthy time out could artificially increase average web page load times when the service is not responding. Finally, it seems advisable that the video streaming indictor correspond to actual use of the application, by employing the same encryption as the one that the streaming platform being tested uses by default.

1.3. Test targets characteristics

	TRANSPARENCY CRITERIA	EXAMPLES	ASSOCIATED BEST PRACTICES
TEST TARGETS	Server location	(TBD)	-
	Use of anycast to identify the nearest server	Yes, no, other	-
	Test target capacity in Mbit/s or Gbit/s	1 Gbit	Exclude tests whose targets create a restriction (the server should have a capacity that is at least double that of the line being tested)
	Ability to conduct IPv6 tests with the target	Yes, no	-
	Port(s) used by the target	80, 443, 8080, 8443	-
	Dedicated TCP/IP stack tuning	Yes, no	-

For tests carried out simultaneously on the same target, or during superfast connection tests, it is possible that the test target's capacity will be a factor that limits the calculated bitrate. If this is the case, it seems advisable not to take these tests into account. Arcep is aware that it is not always easy to obtain information on server's capacity directly, but believes it is nevertheless important to be capable of identifying these tests afterwards, to exclude them from any publications.

2. DETAILS OF THE SOLUTION DESCRIBED IN PROJECT A: "CHARACTERISING THE USER ENVIRONMENT"

2.1. Implementing an API that enables the box to provide information to measurement tools

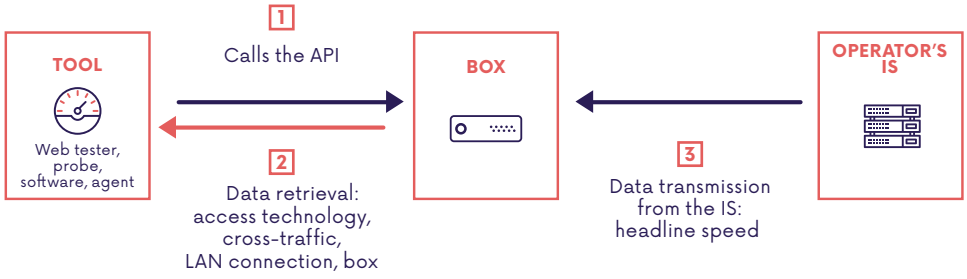
In this first part of the solution, the tool sends an HTTP GET request to the box, to which the box responds with information [the box provides the information that it has at that moment to the tool], in a yet to be defined format. For most operators at this stage, that includes:

- the technology (Re-ADSL2, ADSL2+, VDSL2, cable, FTTH, wireless 4G, satellite);
- sync speed (for xDSL);
- the box's WAN port speed/bitrate (for FTTH lines with an external ONT);
- WAN port traffic counter: the tool will call this function to verify whether the WAN counter increment corresponds to the volume of data being used by the test or, on the contrary, whether there is cross-traffic;
- the type of connection (Ethernet, Wi-Fi and PLC if the box is able to detect them);
- for a Wi-Fi LAN connection, information on the Wi-Fi signal (frequency band, 802.11 protocol, channel width);
- for an Ethernet connection, speed of the LAN port being used;
- for a PLC connection, negotiated bitrate, if the box is able to provide this information;
- information on the box's properties (brand, model, hardware version, software version).

2.2. Implementation of an API that enables ISPs' information system to transfer the missing information to the box

If the box receiving the request does not have the information listed above locally, the operator's IS will send it the information on the access plan (only for cable, FttH and satellite), at the very least the headline speed, using an API.
This solution makes it possible both to allow ISPs to choose the best way to transfer this information to the box, and to provide tools wanting to characterise their test with a single interface. Provisioning would need to take place often enough to ensure that the information being sent back is as up-to-date as possible.

AN "ACCES ID CARD" API FOR CHARACTERISING THE USER ENVIRONMENT



Source : Arcep

This document was drafted by Arcep

DIRECTORATE FOR INTERNET AND USERS
Zacharia ALAHYANE, director

"Open Internet" unit
Laura LÉTOURNEAU, head of unit
Pierre DUBREUIL, Boris GARTNER, Vivien GUEANT and **Samih SOUISSI,** advisors

DIRECTORATE FOR ECONOMY, MARKETS AND DIGITAL AFFAIRS
Stéphane LHERMITTE, director

"Economic analysis and digital intelligence" unit
Jennifer SIROTEAU, head of unit
Hélène BOUT and **Vincent TOUBIANA,** advisors

DIRECTORATE FOR MOBILE AND INNOVATION
Rémi STEFANINI and **Anne LAURENT,** directors

"Mobile coverage and investments" unit
François PHILIPPONNEAU, head of unit
Arnaud COMERZAN, advisor

DIRECTORATE FOR COMMUNICATIONS AND PARTNERSHIPS
Clémentine BEAUMONT, director
Jean-François HERNANDEZ, deputy
Anne-Lise LUCAS, advisor

DIRECTORATE FOR LEGAL AFFAIRS
Élisabeth SUEL, director

"Infrastructure and open networks" unit
Agate ROSSETTI, head of unit
Annabel GANDAR and **Rémy MAECKER,** advisors

Thank you...

Our gratitude goes to all auditioned stakeholders, for their dynamism and valuable inputs.

Afnic
Stéphane BORTZMEYER

ASSIA
Djamel BOUSABER
John CIOFFI

Bouygues Telecom
Laurent BONNET
Stéphane DE BOYSSON
Éric GILBERT

Case on IT
Agustin BATIZ
François MENDIBURU
Luis MOLINA

Cedexis
Arnaud BECART
Manuel CRACIUN

CNES
Arnaud DERALECOURT
Patrick GELARD
Sandrine LAFONT

Direction centrale de la police judiciaire
Adeline CHAMPAGNAT

Directique
Olivier BRUNOT

Europol
Gregory MOUNIER

FirstHeberg
Jérémy MARTIN

Fondation Getulio Vargas
Luca BELLI

Free
François de NANTEUIL
Marie LAMOUREUX

FRnOG
Philippe BOURCIER

Gemalto
Céline FRICHE

INC
Thierry MARTIN

Inria
Renata TEIXEIRA
Isabelle CHRISMENT

Institut Mines-Télécom
Bruno STEVANT

ip-label
Benoit BOIREAU
Laurent GOU
Alain PETIT
Éric VARSZEGI

KRY
Jonathan ARDOUIN

Google
Élisabeth BARGES
Benoît TABAKA

M-lab
Collin ANDERSON

Mozilla
Amba UTTARA KAK

Northeastern University
David CHOFFNES

nPerf
Renaud KERADEC
Anthony SAFFROY

Ookla
Adam ALEXANDER
Marc VON HOLZEN

Orange
Joseph PELAT
Régis COUTIER
Laurence PAUMARD
Anne-Jeanne SCHOTT

QoSi
Hazar AOUAD
Julie MONCORGER
Thierry MONCORGER
Fabien RENAUDINEAU

Replicant
Paul KOCIALKOWSKI

SamKnows
Sam CRAWFORD
Lucy DAVIES

SFR
Gabriel AUBERT
Frédéric DEJONCKHEERE
David GAVARRET
Antoine LEGAY
Guillaume RICHARD

UFC-Que Choisir
Antoine AUTIER

V3D
Philippe VIAL-GRELIER

Publication
Arcep
7, square Max Hymans – 75730 Paris Cedex 15
01 40 47 70 00 – www.arcep.fr

Creation and production:
www.kazoar.fr

Translation:
Gail Armstrong

June 2018

MANIFESTO
ARCEP, NETWORKS AS COMMON GOODS

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 impede users' (consumers, businesses, associations, etc.) ability to communicate.

France's 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 communications 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 safeguards against possible net neutrality violations.

From a more general perspective, Arcep fights against any type of silo 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.