2020

TOME 3

2020 REPORT

The state of the Internet in France

arcep

French Republic - June 2020

2020 REPORT

The state of the Internet in France

arcep

TABLE OF CONTENTS

EDITORIAL

A bountiful internet can also be a green internet

The public health crisis and resulting lockdown in France provided us with a stark reminder of how vital networks are to the life of the country. This unprecedented crisis also confirmed the extent to which networks are and must remain a "common good". It is more crucial than ever before to guarantee accessibility, and a smooth-running and open Internet.

By
Sébastien Soriano,
President of Arcep

The exemplary mobilisation of operators' teams and all of their subcontractors ensured the networks' ongoing operations and maintenance in the field. I would like to take this opportunity to salute them all, once again, for their dedication. Beyond that, infrastructures also demonstrated their resilience and enabled operators to cope with potential congestion risks. This is the fruit of an infrastructure deployment model that has stood the test of solidity. And regulation that promotes investment in infrastructure – which totalled €10.4 billion last year alone – has stood the test of relevance, for both fibre and 4G.

Market players' and users' shared responsibility is intrinsically bound to the very idea of a common good. This is what has ensured that the vast majority continue to have access to high-quality networks. From the very start of the Covid-19 crisis, every stakeholder was quick to rally to prevent a possible network overload. The Government and Arcep established a dialogue with operators to anticipate the potential risks ahead. The leading content and service providers decreased their footprint on the network, either on their on initiative or as the result of a dialogue with public authorities. Users too heard the call from Arcep, the Government and operators to do their part in helping balance out traffic loads on the networks.

Even though we do not really know whether this is all behind us, the unprecedented upheaval caused by this pandemic has already offered up several lessons, aside from the obvious and absolute need for connectivity.

First, Europe's net neutrality regulation has once again proven its relevance and its capacity to adapt. More importantly, it is showing the way forward. When it comes to governing common assets, the "law of the crowd" will always win out over "law of the strongest". European Union regulators who are members of BEREC* and the European Commission all reiterated these principles throughout the crisis. Arcep worked to ensure that these principles continued to be fully enforced despite the very singular circumstances, and will continue to be net neutrality's watchdog.

This period and the many events that punctuated it also fuelled awareness of the need for a clearer framework in this area. In addition to the non-discrimination obligation imposed on operators, major

content and service providers' tremendous impact on the networks warrants attention. The dialogue between these players and operators over improving network management has sometimes seemed like one of variable geometry, for instance when rolling out new services, introducing certain options or posting updates to certain especially popular games online. It would be wise to establish a dialogue mechanism that would enable operators to anticipate and plan for these events. It would also be worth assessing how efficient online service providers' optimisation measures (downgraded video format) were in reducing their bandwidth consumption. But, let us be clear, permissionless innovation needs to remain the rule for one and all, even if the handful of heavyweight OTT* companies whose traffic shapes how networks are provisioned should proactively commit to a systematic dialogue.

Although far from the subjects that fall under Arcep's purview, the development of contact tracing solutions to help fight the spread of the epidemic, thanks to the use of digital technology, also confirmed how important it is that everyone work to ensure an open Internet, beyond just telecom operators. As to the decisive role played by the two main mobile operating system (OS*) providers, it seems increasingly vital to be able to challenge these players on their technological choices, and the fetters they place on app developers. Is it really acceptable that private sector players' technical decisions can influence the choices made by democratic governments such as ours, on matters of public health? This is the question that the current public health crisis is forcing us to ask, separate from any underlying debates about the tool itself. Extending the principle of an open Internet to include operating systems, which Arcep has been proposing to public policymakers since 2018, seems more pressing than ever before.

Finally, the period of lockdown that we experienced confirmed how urgent it is to make environmental issues the centrepiece of our actions. Arcep is firmly committed to this path, with the launch of a collaboration platform devoted to "Achieving digital sustainability", building on the momentum begun last year with the "Future networks" cycle of inquiry.

This year, for the first time, Arcep's report on the state of the Internet in France devotes an entire chapter to environmental issues. This includes a reminder of the first available quantified findings on digital technology's carbon footprint, and an exposé on the preliminary actions that Arcep has taken to measure the environmental impact of a sector that today represents around 3% of the globe's greenhouse gas emissions.

But let there be no misunderstanding. The necessary digital sobriety must not be seen as synonymous with placing limits on online exchanges. The crisis revealed how crucial these interactions are to the life of the Nation, and no authority in a democracy could or should stand as arbiter of good or bad uses. The Internet's profusion must remain an inexhaustible source of vitality, expression and innovation. The challenge that awaits us is far more meticulous: it is by breaking down the different uses' technical chains that we can make every link along those chains accountable, maintaining an overall cap on digital technology's environmental footprint, and remaining deeply committed to eco-friendly design.

This report on the state of the Internet in France is Volume 3 of Arcep's annual report: it provides the keys to understanding what keeps the Internet running smoothly, before and during the coronavirus crisis, by detailing how the Internet's main components evolved over the course of 2019: quality of service, data interconnection, the transition to IPv6, net neutrality, device openness and the role played by platforms.

In addition to these issues, the latest developments surrounding telecoms networks raise a number of societal questions: sovereignty, digital inclusion, privacy, etc. These issues do not fall directly under Arcep's purview, and so are not examined in detail in this report. Arcep's work on accessibility and coverage is presented in Volumes 1 and 2 of its Annual Report.

And, finally, let us remember that Arcep would be nothing without every stakeholders' full and earnest engagement, which is why we were eager to give them an opportunity to express themselves in this report. We hereby thank them most sincerely.

* See lexicon.

Networks during the Covid-19 crisis

This report on the state of the Internet looks at Arcep's activities and the events that occurred in 2019. But the public health crisis and subsequent lockdown in spring 2020 had a tremendous impact on network use, so Arcep decided to devote a chapter to summarising its observations to date, and the first lessons learned from this period.

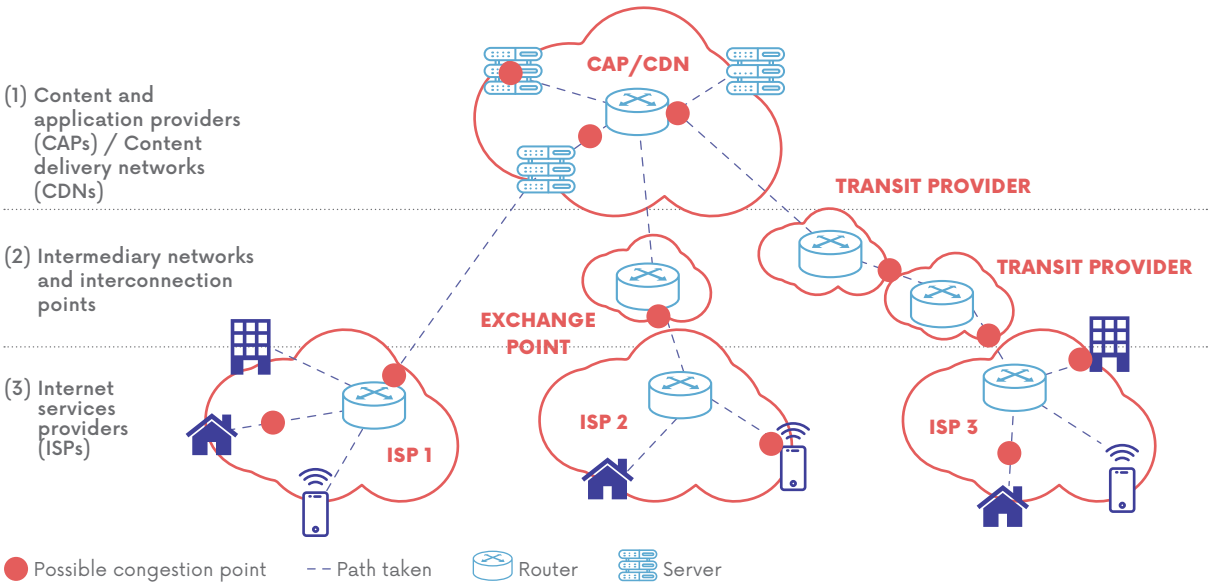
Arcep will confine itself here to the topics addressed in this report and, despite their significance, will not address the issues surrounding digital inclusion that arose during this crisis.

The volume of traffic flowing over the Internet typically varies substantially throughout the day, and depending on the day of the week. Under normal circumstances, Internet traffic spikes in the evening and at weekends, due to a surge in the use of bandwidth-hungry (notably video) applications. It is these spikes in use that determine how the networks are scaled. The Covid-19 crisis illustrated the degree to which people in France want and need to stay connected to their working, personal and cultural environments when at home. The fact of switching a number of uses to inside people's homes resulted in a tremendous increase in Internet traffic during the lockdown – as much as 30% according to initial estimates[1] – but also to a significant change in the traffic profile, with the usual evening spike spread out across the day.

This situation raised a number of questions about the Internet's operation that tie into the topics addressed in this report: were the networks properly scaled to handle the surge in traffic related to the crisis? What were the main sources of potential congestion? What best practices were adopted that enabled the Internet to continue to function? How to guarantee compliance with net neutrality rules during this exceptional situation?

WERE THE NETWORKS PROPERLY SCALED TO HANDLE THIS SURGE IN TRAFFIC? WHAT WERE THE MAIN SOURCES OF POTENTIAL CONGESTION?

SIMPLIFIED ILLUSTRATION OF POSSIBLE NETWORK CONGESTION POINTS



Source: Arcep

1. Netscout report based on data from French ISPs.

A user who connects to the Internet to access a given content or service (e.g. web browsing, videoconferencing, video streaming, download, etc.) may find that service or content, and possibly even several services at once, are unavailable. This can be due to the overload of a link in the network's or the information system's technical chain, which is used to relay traffic from the server that hosts the content to the user's device.

Overloads can sometimes occur at the Local Access Network (LAN) level inside users' homes, e.g. because of an over-solicited Wi-Fi connection[2]. Looking beyond these limitations that may exist at the end user level, this section focuses on the potential congestion points for the different players along the Internet chain. To put it simply, and as illustrated above, congestion issues can occur at three levels: with content and application providers (CAPs) or on content delivery networks (CDNs) (1), on intermediary networks and exchange points (2) and on Internet service providers' (ISPs) networks (3).

- Congestion can occur on CAP/CDN (1) servers when a service is more solicited than usual. This overload can be due to hardware (processor, memory, network card, etc.) or software-related (exceeding the maximum number of simultaneous users, open files, open TCP ports, etc.) limitations. There are a number of other possible points of congestion at the CAP/CDN level: links, aggregation, backhaul, firewall[3] and routing equipment can all create bottlenecks if their (physical or assigned) capacity in bits per second or packets per second is exceeded.
- Congestion can occur on intermediate networks and interconnection points (2) links if they are not sufficiently scaled with respect to the amount of traffic being relayed. This congestion will typically manifest itself on a private peering link, a public peering link (at an IXP), between a CAP and a transit provider, between two transit providers or between a transit provider and an ISP. Depending on where the overload occurs, it can affect one or several services, or one or several players. Internet stakeholders usually overprovision and ensure redundancy for interconnections, to be able to handle exceptional situations, such as major sporting events. To a certain extent, the situation tied to the Covid-19 crisis was unprecedented, and caused an important surge in traffic on the network.
- Congestion can occur at several levels on ISPs' networks (3): at the access level, both fixed or mobile, on the ISP's transport/backhaul network or in the ISP's core network. When a customer subscribes to a fixed Internet plan, they are not allocated their plan's advertised bandwidth end to end (unless they have a special contract): at each point in the network, a greater capacity is shared between the different users, based on the presumption that not all users employ their connection at maximum speed simultaneously[4]. Here too, the network is scaled to ensure it does not get overloaded, but an unusual situation has the potential to cause congestion. In addition, on the mobile Internet, congestion can occur in a given cell, notably when several of the users connected to that cell solicit bandwidth-hungry applications (video streaming, videoconferencing, downloading, etc.).

During the lockdown, several content providers experienced overloads, which disrupted access to several services (videoconferencing, e-learning services, etc.). Occasional, highly localised access issues were also observed on the mobile Internet.

In addition to the Internet network, congestion can also occur on voice calling networks. This happened during the first days of the lockdown: sharp increase in phone calls caused occasional and temporary overloads on voice networks. Operators' rescaling of the affected interconnections rapidly solved the problem.

Thanks, on the one hand, to telecommunication networks' capacities and performance and, on the other, to the mobilisation of the ecosystem's different players, networks in France did not experience any major congestion issues during the Covid-19 lockdown that lasted from March to May 2020. Over and above this crisis, however, the ongoing rise in usage will continue on through the long term, and require infrastructures to supply faster connections, through fibre and 5G deployments.

2. See the next section on optimising usage.
3. See lexicon.
4. The GPON standard creates the ability, for instance, to put a maximum 128 clients on a tree that supplies speeds of 2488 Mbit/s downstream and 1244 Mbit/s upstream. Several dozen GPON trees are then concentrated and often connected to the network over a 10 Gbit/s link.

WHAT BEST PRACTICES WERE ADOPTED THAT ENABLED THE INTERNET TO CONTINUE TO FUNCTION?

It was the outstanding mobilisation of all of the ecosystem's players (operators, content and application providers, end users and public institutions) that made it possible to cope with the unprecedented intensity of digital needs during the crisis.

Telecoms companies and the entire fabric of small and medium businesses, local stakeholders and associations that surround them, worked in concert to maintain the networks and ensure that they continued to run smoothly. In addition to the mobilisation of their teams in the field, operators also handed out a number of bonuses to customers: additional mobile data, free calling, free access to pay-TV channels, increased speeds for certain plans, etc.

Following a proactive dialogue initiated by the Government, or on their own initiative, content and application providers also contributed to the collective effort. "Heavy" network users, such as video streaming platforms and online gaming platforms reduced the strain their content put on the network by capping the bandwidth their services required, by downgrading the quality of their videos and by scheduling downloads and service updates during off-peak hours. The dialogue established between Disney and operators also helped anticipate the launch of Disney's new video steaming platform. Unlike other CAPs, the architecture Disney chose was not based on its own content delivery network but rather on third-party CDNs, hence the potential to overload an interconnection link shared with a CDN hosting other content, should the platform's launch cause a spike in traffic. The rescaling of certain interconnections was therefore required to prevent potential risks of network overload.

This situation testifies to the need for a proactive dialogue between operators and the main content and application providers, to enable them prepare for events that could have an impact on the networks' traffic load.

MOBILISATION OF THE ECOSYSTEM'S PLAYERS DURING THE PUBLIC HEALTH CRISIS

Source: Arcep

By the same token, end users too were able to contribute to the joint effort to relieve the networks, by adapting their usage – notably by following the recommendations that the Government and Arcep issued on best practices, for instance when teleworking,[5] as well as Arcep recommendations on how to improve a home Wi-Fi[6] connection. The end users who followed these tips thus switched from using 4G to Wi-Fi when at home, boosted their Wi-Fi connection (e.g. by using Wi-Fi repeaters), spread their digital service use out across the day, and postponed the use of any bandwidth-hungry tasks and applications to off-peak hours.

Throughout the crisis, the Government and Arcep monitored telecom networks' evolution on a daily basis. Alongside the mechanisms devoted specifically to the operational management of the crisis, operators reported to the Government and Arcep on the status of their networks – initially every day, and later less frequently. Telecoms networks' resilience is also a transnational matter, and European regulators, of which Arcep is one, worked together within BEREC to actively monitor the state of European networks. Lastly, in the very early days of the crisis, Arcep and the Government also established a dialogue with operators to ensure ongoing compliance with net neutrality rules, despite the exceptional circumstances.

HOW TO GUARANTEE COMPLIANCE WITH NET NEUTRALITY RULES DURING THIS EXCEPTIONAL SITUATION?

To meet this unprecedented and massively increased demand for connectivity, ISPs quickly hypothesised that they would need to prioritise routing on their networks for certain content that was deemed essential (notably teleworking, distance learning and telemedicine) to guarantee these services could continue to function. Sometimes held up as the solution to contain the surge in traffic streams during the crisis, it is not so simple in practice, particularly when having to distinguish between similar streams (e.g. videoconferencing and video streaming) or when services are being used for something other than their original purpose (e.g. using video game platforms for home schooling during the lockdown). If extreme circumstances require extreme measures, how do these practices hold up to the scrutiny of the Open Internet regulation?

According to Article 3 of the Open Internet regulation, ISPs are required to treat all traffic equally, and not discriminate based on the nature and origin of the data being relayed over their networks. The regulation thus strictly forbids the differentiated treatment of certain content, while nevertheless explicitly stipulating three exceptions: when there is an obligation to comply with another legal provision, an ISP's need to protect the security and integrity of its network and, lastly, an imminent risk of congestion. It was within the legal framework of this last exception that Arcep opened a proactive dialogue with operators on possible traffic management measures they might take to cope with the public health crisis.

In accordance with the Open Internet regulation, ISPs could, if necessary, take exceptional traffic management measures to reduce the impact of imminent congestion on their networks. Although they are exceptional, these measures must nevertheless also satisfy certain conditions: they must prevent the impending congestion, have as little impact as possible on network traffic, to give equal treatment to all equivalent traffic categories, and not be applied any longer than is strictly necessary. The purpose of these criteria is to enshrine non-discriminatory treatment between suppliers of similar content, including when ISPs implement exceptional measures to manage congestion.

The issue of telecommunications networks' resilience also arose at the European level. In a joint statement[7], the European Commission and BEREC reminded operators of their ability to adopt such exceptional traffic management measures when congestion was imminent. And so, despite the gravity and hardship of the public health crisis, the Open Internet regulation proved its ability to withstand any circumstances.

5. Best practices for using the Internet for telework, published by Arcep: https://www.arcep.fr/demarches-et-services/utilisateurs/teletravail-et-connexion-internet.html
6. Tips on how to improve your Wi-Fi signal: https://www.arcep.fr/demarches-et-services/utilisateurs/comment-ameliorer-la-qualite-de-son-wifi.html
7. Joint statement from the European Commission and BEREC on coping with the increased demand for network connectivity due to the Covid-19 pandemic: https://berec.europa.eu/eng/document_register/subject_matter/berec/others/9236-joint-statement-from-the-commission-and-the-body-of-european-regulators-for-electronic-communications-berec-on-coping-with-the-increased-demand-for-network-connectivity-due-to-the-covid-19-pandemic

PART 1

Ensuring the Internet functions properly

CHAPTER 1

Improving Internet quality measurement

HIGHLIGHTS

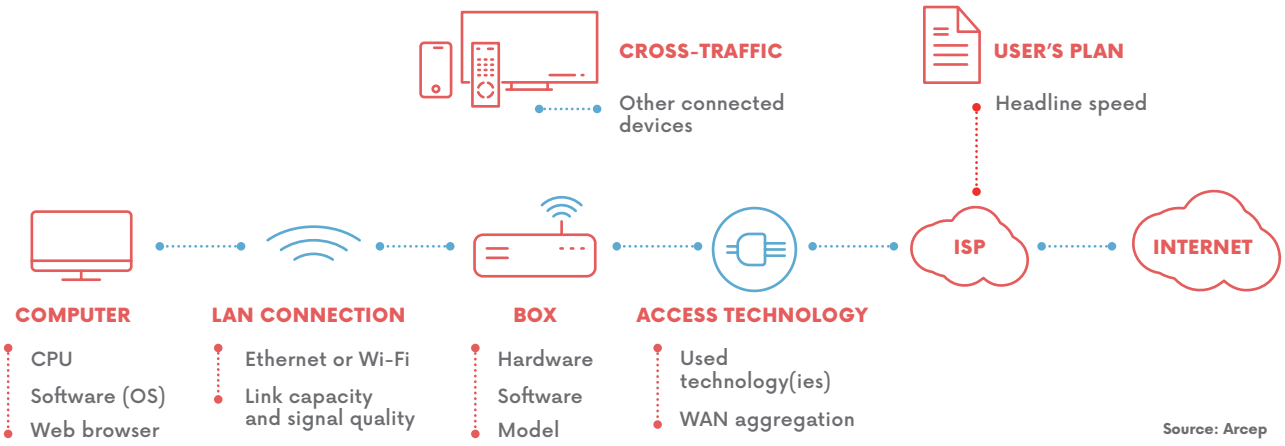
16 January 2020
marks the start of the deployment calendar for the "Access ID card" API in boxes, which will be accessible to any measurement tool that complies with Arcep's QoS Code of conduct. The goal: to improve Internet quality of service measurement.

47% of reports
received on the "J'alerte l'Arcep" platform concern a fixed or mobile service's quality and availability issues.

The quality of mobile data services has improved considerably since 2018: the average speed in Metropolitan France reached **45 Mbit/s** in 2019 (+50% in one year).

If Internet access plans, and particularly those supplied over FttH, are evolving continually to provide increasingly high speeds, Internet uses too are evolving and some applications are particularly speed-sensitive. Which is why many customers want to be able to measure the quality of their Internet service, both at home and when on the go.

CHARACTERISTICS OF THE USER ENVIRONMENT



Source: Arcep

1. POTENTIAL BIASES OF QUALITY OF SERVICE MEASUREMENT

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

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

The "user environment" is the first element that can affect test results. The diagram on the previous page summarises the main characteristics of the user environment that can influence the results.

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

2. IMPLEMENTING AN API IN CUSTOMER BOXES TO CHARACTERISE THE USER ENVIRONMENT

While speed test applications that run on mobile networks are capable of identifying the user environment (radio technology, signal strength, etc.), measuring the quality of fixed Internet services is particularly complex: it is virtually impossible today, from a technical standpoint, for an Internet speed test to determine with absolute certainty the access technology (copper, cable, fibre, etc.) being used on the tested line. This lack of user environment characterization in the testing process – which renders it impossible to isolate factors that are likely to heavily influence results – undermines the usefulness of the resulting data and, in some cases, can mislead consumers.

Which is why, in early 2018, Arcep began a wide-ranging initiative that called upon all of the market's stakeholders to help solve this challenge of accurately measuring quality of service on fixed networks. This co-construction[1] approach initiated by Arcep involves some 20 players, including crowdsourcing measurement tools, ISPs, consumer protection organisations and academia. The ecosystem reached a consensus on the implementation of an Application Programming Interface (API) that would be installed directly in operators' boxes, and could be accessed by tools that comply with the Code of conduct that Arcep published[2]. This software interface will allow to transmit the information that make up the "Access ID card".

A public consultation was held on this topic in the spring: the 17 responses that Arcep received, and published,[3] made it possible to adjust the mechanism for implementing the API, working in concert with the ecosystem's players. Arcep adopted the corresponding Decision in late October 2019[4], which the Government approved in an Order that was published in the *Journal Officiel* on 16 January 2020[5].

The purpose of the "Access ID card" API is to characterise the testing environment. It will be accessible to crowdsourcing measurement tools that users employ to test their connection speed and the quality of their Internet connection in general. Requested only when the user initiates a speed test, and remaining under their control, the API will provide the measurement tool with a set of technical indicators such as the type of box and Internet access technology being used, and the advertised upload and download speeds. The complete list of the indicators that are sent back to the tool can be found in Annex 1.

The operators and boxes concerned, the technical parameters provided, the implementation timetable, and the technical implementation specifications are all set out in the Arcep decision.

The API's operating rules take users' privacy protection concerns and demands fully into account. First, the data collected by the API are not transmitted to Arcep. The API will not transmit any information on the user's identity (user ID, name, location, etc.) to the measurement tools, thereby ensuring that users' privacy is fully protected. The API is only requested when users themselves initiate a speed test, and does not respond to requests from the Internet. When questioned about this process, France's data privacy watchdog, CNIL, was able to verify that the mechanism's design complies with data privacy requirements, while also underscoring the importance of Arcep's advisory role, notably through its "Code of conduct on Internet quality of service" for measurement tools that use the API.

The measurement results, now qualified, mark another step towards improving the accuracy of measuring quality of service on fixed network.

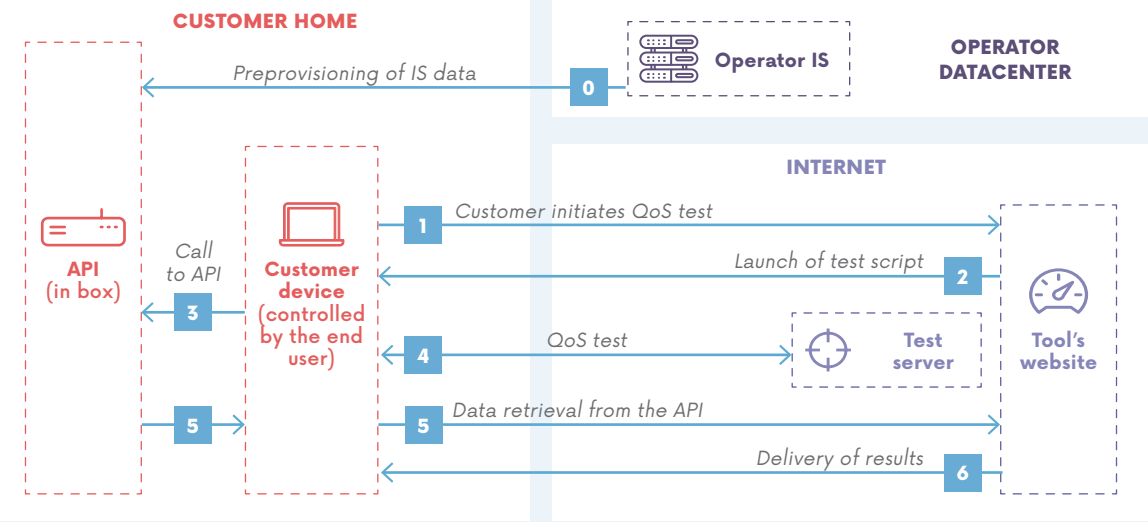
1. Description of the API co-construction process: https://www.arcep.fr/uploads/tx_gspublication/rapport-etat-internet-2018_conf050618.pdf#page=11
2. 2018 edition of the quality of service Code of conduct: https://www.arcep.fr/uploads/tx_gspublication/code-de-conduite-qs-internet-2018_FR.pdf
3. Responses received to the public consultation: https://www.arcep.fr/uploads/tx_gspublication/reponses_consultation_publique_api_box-oct2019.zip
4. Arcep Decision No. 2019-1410 of 10 October 2019: https://www.arcep.fr/uploads/tx_gsavis/19-1410.pdf
5. Order of 8 January 2020 approving Arcep Decision No. 2019-1410: https://www.arcep.fr/fileadmin/cru-1582218129/reprise/textes/arretes/2020/arr-08012020-homolog-2019-1410-api-box.pdf

MORE INFORMATION ON THE "ACCESS ID CARD" API

How does the API work?

The following diagram provides a simplified explanation of how the API works when a customer initiates a QoS test using a tool that has access to the API.

HOW THE "ACCESS ID CARD" API WORKS



This is a simplified diagram: to make it clearer, the streams to the Internet (arrows 1, 2, 4 and 6) travel through the box but are not depicted here. **Source: Arcep**

Which measurement tools have access to the API?

The API will be accessible to those measurement tools that have been declared compliant with the Code of conduct on Internet quality of service published by Arcep.

The work done on the Code of conduct is detailed in the next section.

What boxes will the API be implemented in?

Operators with more than a million customers who satisfy all of the conditions set out in the Arcep decision will be required to implement the API in most of their models of xDSL, cable, FttH and fixed 5G boxes supplied to customers starting on 17 July 2021.

Arcep also encourages to implement the API in all other box models.

Can the API be accessed from the Internet?

No, the API can only be accessed from the end user's local network, and will not respond to requests coming from the Internet. There is also an access restriction system in place so that only the authorised tools can access the API.

When will the API be available?

In July 2022, the Access Identity Card API will be implemented and activated in almost all the boxes concerned by Arcep's decision after several demonstration and implementation phases.

API DEPLOYMENT SCHEDULE

Source: Arcep

OPEN FLOOR TO ...

LAURENCE PAUMARD

*Head of fixed Internet quality of service - **Orange***

ACHIEVING FAIR, RELEVANT AND MEANINGFUL QoS PUBLICATIONS

The ability to measure Internet speeds end-to-end or browsing time, at home, depends on a complete chain: running from the more or less powerful device used by the customer to the Internet server, by way of the operator's network and the reliability of the commercial testing tool itself. The faster the connection, as with fibre, the more the customer-side link weighs in the equation, and eclipses the other performances.

This is why it is so important to characterise the user environment in end-to-end measurement: it is even the sine qua non when interpreting results!

The measurement tools that are available today do not have any information on the properties of the line being tested, or on the user's home environment: their access technology, the headline speed they chose if they have a fibre plan, whether they have chosen to perform the test using Wi-Fi or a wireline connection, whether other applications or devices are running in the home at the same time… All key elements that will lead to very different results: this measurement context, which is uncontrolled, unknown and varies from operator to operator, introduces biases in overall comparisons between operators. We therefore believe it is necessary to remove potential biases from these publications, to make them fair, relevant and meaningful.

This is why Orange is taking an active part in the Arcep's multilateral work on characterising the user environment. The chosen solution, an API that interacts with users' box, to be developed by each operator, will go a long way in enhancing end-to-end measurement with key parameters.

But we will also be very vigilant about how it is used, and this from two perspectives: controlling access to these data, to protect them and their actual use in statistics, and measurement tools' interpretations in particular. The Code of conduct must incorporate these provisos, and we are already working with Arcep to achieve this.

ADRIEN d'USSEL

*Head of network performance - **Bouygues Telecom***

QoE MUST BE AT THE HEART OF CROWDSOURCED TESTING

In the fixed network environment, measuring quality of service is a very complex issue. Too often, we confuse QoS measurements, such as speed and latency, and measuring the quality of a customer's daily experience (QoE).

The main challenge for operators is to provide every customer in every home with a better quality of experience. This naturally requires good connectivity and a stable access line, but this "technical" quality is only a fraction of what needs to be accomplished to maintain robust performance year-round. An operator's quality can therefore not be evaluated merely with a speed test since, even if it does at the very least make it possible to verify whether our actual speed aligns with our plan's headline speed, this does not necessarily reflect the actual quality of the internet services that our customers use on a daily basis. Fixed network quality derives from a combination of Wi-Fi coverage and performance, the quality of linear and catch-up TV services, the box's stability but also the availability and definition of OTT services like VOD and gaming.

The real challenge for the crowdsourcing ecosystem, then, is measuring the quality of the experience that each of us has in the evening, i.e. peak traffic time in every home, when using our favourite services. A fixed network's quality is evaluated above all in the evening, when we get home and the whole family is using the box's Wi-Fi connection. This is the moment when we need to evaluate the quality of video, internet, gaming, etc. services.

The approach being promoted by Arcep – to develop and API installed on boxes, and so be able to share technical and business data, when a crowdsourced test is performed – is thus essential. It will create the ability to obtain as clear a picture of the user environment as possible, to obtain more accurate results, and to steadily enhance the data-driven approach to regulation. It will also create the ability to correct sometimes overly hasty comparisons, and to factor in the specific features of each household, to help educate the public about performances and prevent biased results. This API is thus an important milestone in what must be followed by crowdsourcing players' transition into QoE-centric tests, to keep consumers informed about the actual daily quality of services.

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

3. TOWARDS MORE TRANSPARENT AND ROBUST MEASUREMENT METHODOLOGIES

3.1 Presentation of Arcep's 2018 Code of conduct and code-compliant tools

In addition to the characteristics of the user environment, testing methodologies also have a tremendous influence on QoS test results. In 2017, Arcep identified the need for greater transparency on measurement methodologies. In December 2018, it published a Code of conduct[6] for stakeholders involved in quality of service measurement. This Code of conduct addresses two aspects in particular: first, requesting that the tools include a clear explanation of their methodological choices when publishing their results, so that any third party can analyse them. Second, establishing best practices that are vital to obtaining reliable results. This approach creates an incentive for stakeholders to satisfy a set of minimum requirements in terms of transparency and robustness, both in their test protocols and in the delivery of their findings.

The Code of conduct is structured into two main parts:

- The first part concerns test protocols, in other words both the methodologies used to measure different indicators (speed, latency, web page load time and video streaming quality) and the test servers;
- The second part concerns aggregated publications, including a general commitment to use algorithms designed to exclude erroneous, manipulated or irrelevant results. Moreover, to guarantee statistical representativeness, tools that comply with the Code of conduct commit to publishing the number of tests performed and the factors that are likely to introduce a significant bias when analysing the compared categories.

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

The tools for measuring fixed Internet quality of service which declared themselves to be in compliance with the 2018 version of the Code of conduct on Internet quality of service are:

- nPerf, developed by nPerf;
- UFC-Que Choisir Speedtest, developed by UFC-Que Choisir;
- DébiTest 60: the connection tester from *60 Millions de consommateurs* developed by QoSi;
- 5GMark, developed by QoSi;
- IPv6-test: the IPv4 and IPv6 QoS test, developed by IPv6-test.

The tools for measuring mobile Internet quality of service which have declared themselves to be in compliance with the 2018 version of the Code of conduct on Internet quality of service are:

- nPerf, developed by nPerf;
- DébiTest 60: connection tester from *60 Millions de consommateurs*, developed by QoSi;
- 5GMark, developed by QoSi.

MEASUREMENT TOOL DEVELOPED BY BEREC (BODY OF EUROPEAN REGULATORS FOR ELECTRONIC COMMUNICATIONS)

Over the course of 2019, BEREC continued to develop then finalised its open source tool for measuring Internet quality of service. This tool includes a browser-based version, an installable version (Windows, Mac and Linux compatible) and a mobile app (Android and iOS).

In addition to measuring the usual indicators (speed, latency, etc.), this tool is able to measure certain usage indicators such as web browsing and video streaming quality, along with net neutrality-related indicators such as port blocking, proxy detection and DNS manipulation. The tool's source code has been available on Git Hub since December 2019: https://github.com/net-neutrality-tools/nntool.

The tool is currently available to national regulatory authorities (NRAs) in the different EU Member States, who can adopt it on a voluntary basis. The NRAs can then implement the tool in their country after having adapted it to local requirements (translating the user interface, installing local test servers, adding any supplementary test indicators, etc.).

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

6. 2018 edition of the quality of service Code of conduct: https://www.arcep.fr/uploads/tx_gspublication/code-de-conduite-qs-internet-2018_FR.pdf

3.2 Towards a new version of the Code of conduct

The 2018 version of the Code of conduct on Internet quality of service introduced minimum requirements in terms of transparency and robustness. As indicated when it was first published, this Code will evolve and be updated over time, not only to strengthen those criteria, but also to complete them with elements from other categories.

Following the release of this first version, Arcep continued its co-construction approach throughout 2019 to draft a new version of the Code of conduct. This meant engaging in a second round of work with players involved in measuring QoS (ISPs, measurement tools, consumer protection organisations and academia).

To keep pace with the ecosystem's gradual acquisition of skills and expertise in measuring QoS, several aspects contained in the new version of the Code of conduct will be strengthened.

First, Arcep is working with the entire ecosystem to strengthen the protocols' transparency and robustness requirements. Below are a few aspects being explored as part of the work being done to draft a revised Code of conduct:

- The relevance of displaying a median value, notably for latency. In some cases, the median could be relevant in reflecting the user experience (QoE), notably when the measured results contain extreme values which impact the representativeness of the average;
- The need to specify other factors that can affect the measurement, notably the use of Wi-Fi and its features, the model and version of the operating system and web browser, which can heavily influence QoS measurements;
- The need to introduce a minimum capacity for test servers, to prevent the test from being too constrained by these servers;
- Whether to specify the test servers' ability to perform the tests in IPv6, as the protocol used can effect speed measurement (cf. next section on test servers).

In addition, this new Code of conduct will stress a number of measurement biases that should be detailed in measurement tools' publications of aggregated findings.

This new version of the Code of conduct, which also seeks to take better account of the particular aspects of measuring Internet quality of service on mobile networks, will be published in summer 2020.

Arcep will invite all of the players involved in measuring QoS who so desire to declare themselves compliant with the 2020 Code of conduct, and will provide an account of those players who have done so.

The work being done to further improve the practices and strengthen the Code of conduct will continue with the actual implementation of the API. Factoring in the functions that this API provides for measurement tools will indeed not only help improve the reliability of QoS tests, but also of the resulting aggregated publications. Naturally, all of these changes will be made in concert with stakeholders.

BEREC'S QoS GUIDELINES*

As stipulated in Article 104 of the new European Electronic Communications Code (EECC), BEREC has just published guidelines detailing the quality of service indicators for Internet access services and interpersonal communications services available to the public.

One of the main objectives of these guidelines is to guide national regulatory authorities in choosing the QoS indicators that providers of these services must publish to ensure that end users have complete, reliable, easy to use and up-to-date information on the quality of their services.

The BEREC guidelines also address indicators that are relevant for end users with disabilities, the applicable QoS measurement methods, questions surrounding publishing the information as well as quality certification mechanisms.

In accordance with the EECC, which stipulates that over-the-top (OTT) interpersonal communications services now constitute a category of electronic communications, the BEREC guidelines include indicators for these services, among which online messaging services.

As part of process of transposing the European code, Arcep's competences are expected to be expanded to include these players in respect of the obligations that now apply to them, and Arcep's newfound responsibility to monitor them.

* BEREC QoS Guidelines – BoR (20) 53: https://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/9043-berec-guidelines-detailing-quality-of-se_0.pdf

10 GBIT/S-COMPATIBLE SPEED TESTS: A CHALLENGE FOR QoS MEASUREMENT TOOLS

The vast majority of speed tests are performed using a web browser.

However, a web browser is a complex piece of software that relies on a set of components – such as a sandbox (a computer security mechanism based on isolating software components) for instance. In theory, then, a speed test consumes far more resources in a web browser than if it runs directly on the operating system.

As Internet speeds are evolving far more quickly than the power of our computers' microprocessors, customers who now have a 10 Gbit/s connection no longer measure the speed of their Internet connection, but rather the power of their microprocessor. Indeed, only very powerful PCs can perform a speed test on a 10 Gbit/s connection using a web browser, without overload their microprocessor.

A 10 Gbit/s connection also requires a test server with a throughput to the Internet of more than 10 Gbit/s, which today is very rare.

Several solutions are emerging to tackle these new challenges, such as using a QoS measurement tool that runs directly on the operating system.

Other players are lobbying for no longer measuring connection capacity but rather quality of experience (QoE), as increasing the speed of the connections to the test servers does not necessarily make it possible to assess the quality of the user's experience. In some cases, it may even be possible to have a greater QoE on a 100 Mbit/s FttH line than on a 10 Gbit/s one. Latency, packet loss, buffer size, the ability to transport packets in order and interconnection relationships are also very important ingredients in a user's quality of experience, and do not depend on the link's capacity.

OPEN FLOOR TO ...  JEAN-FRANÇOIS GIORGI

Independent developer

NSPEED - MEASURING 10 GBIT/S CONNECTIONS

Existing internet speed tests that are available to the uninitiated in network technology are having trouble correctly measuring an internet connection with a speed of several gigabytes per second (Gbit/s):

- Using web technologies that limit performance and are incapable of obtaining information on the local usage conditions, such as the capacity of the computer's processor;
- Using a single test server. The test stresses an exact path on the internet, and not necessarily the last mile. For multi-gigabit connections, the server and/or its interconnection with the internet are often the most restrictive links.

NSpeed is a tool that was born out of this realisation, in particular following the measurement difficulties encountered by subscribers to Free's 8 Gbit/s plans. Users have no information or simple way to find out where the problem is located, if they are unable to measure the maximum speed.

The other concern is these applications' lack of transparency: none of them are open source.

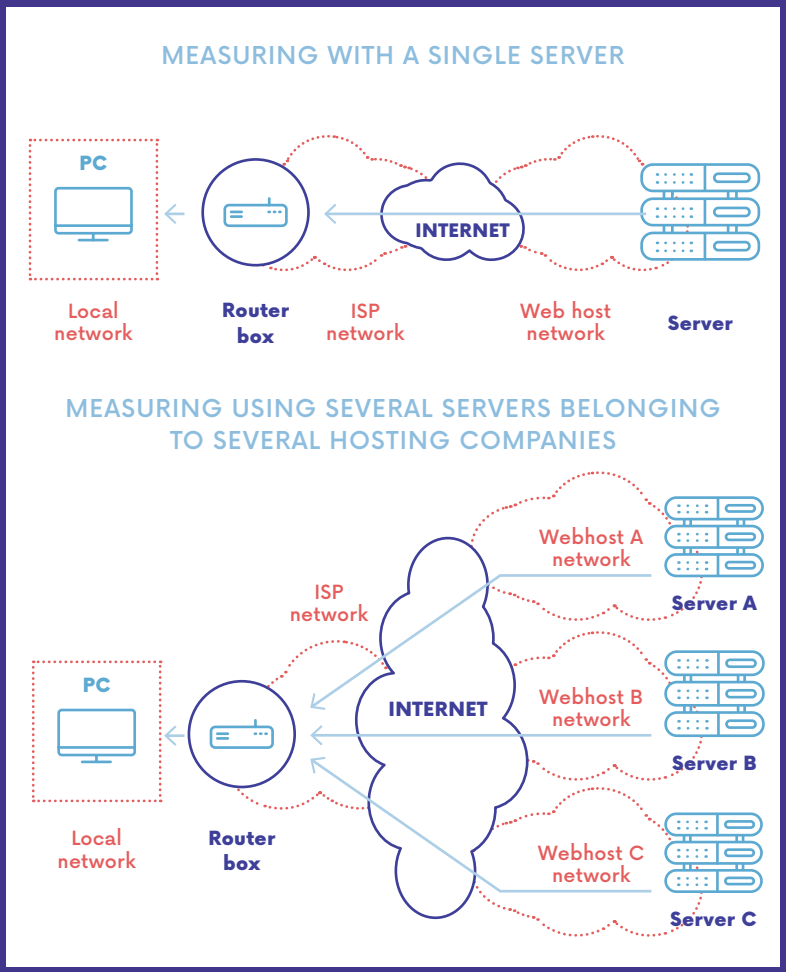
The NSpeed tool offers a different approach:

- using HTTP version 1.1, 2 and 3 with or without encryption. Versions 1.1 and 2 use TCP*, version 3 uses UDP*;
- using as many servers as we want, located all over the world;
- using dedicated NSpeed servers or any web server around the world that provides the ability to download a file and/or send one. The appeal of dedicated NSpeed servers lies in having more information on what is happening on the server end, notably the load on the network, the processor and cross-traffic.

For most operating systems, NSpeed software appears as a single executable binary file that requires no installation. It only needs to be downloaded and executed.

NSpeed software is also an NSpeed server that supplies fictitious files that can be downloaded, not only by the NSpeed software itself but by any software using HTTP. The NSpeed server also creates the ability to run peer-to-peer speed tests directly between internet users.

The NSpeed project is being developed using the Go programming language, and its open source code is available at the following URL: https://nspeed.app. We are issuing a call for contributions to all those with software development skills who are interested in helping to develop this product.



* See lexicon.

4. IMPORTANCE OF CHOOSING THE RIGHT TEST SERVERS

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

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

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

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

Arcep is therefore working with the entire ecosystem to add to the 2020 Code of conduct a set of new minimum transparency criteria for the test servers used by measurement tools, so that users can be provided with information on the bandwidth of each of the test servers in France proposed by the QoS testing tool they are using.

The 2020 Code of conduct could also recommend a minimum capacity for the test server, to reduce the number of measurements where capacity proves a limiting factor.

4.2. Impact of the test server's location

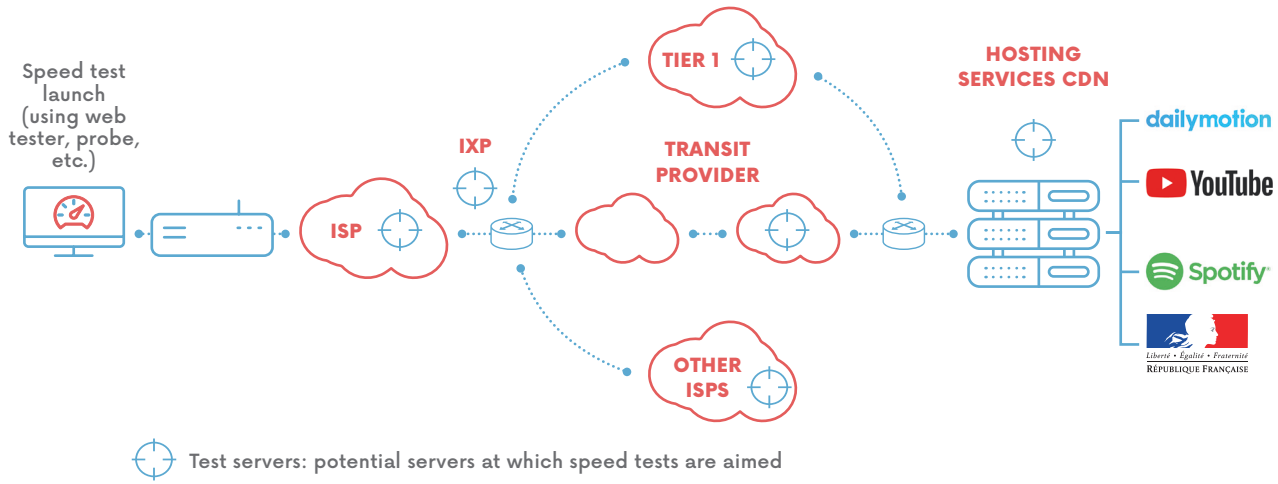
The test server's location is fundamental for calculating latency as it depends chiefly on the route the data travel between the customer and the test server[7]. The location also has an influence over the connection speed's increase and so over average speed. Location is less important for tools that display the speed in a steady state.

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

- on the user's ISP network: the results of the test depend only on the ISP but it is not terribly representative of the actual experience of using Internet services, which are often hosted outside this simple network;
- on another ISP's network directly interconnected (via peering) with the user's ISP: the test takes into account not only the user's ISP's network but also the quality of the network and interconnection with another ISP. This test is very rarely representative of the actual experience of using Internet services;
- at an Internet Exchange Point (IXP): the tested network depends almost only on the ISP and more closely matches the actual user experience, with a portion of Internet traffic transiting through the IXP;
- on the transit provider's network: the test will only be relevant if the transit provider exchanges a great deal of traffic with the user's ISP. It should be noted that the observatories produced by transit providers (e.g. the one from Akamai) only represent quality of service towards a specific point on the Internet;
- on a Tier 1[8] network: the tested network extends beyond just the ISP's network performance, and the measurements are even more representative of the actual user experience if the test targets are located at an IXP;
- close to CAPs' servers: the tested network is the one employed end-to-end up to a given web host. The tests are thus very representative of one particular type of use (the Netflix speed index, for instance, only measures the quality of the connection to its own service).

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

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



Source: Arcep

7. In addition to latency tied to the access technology, most of the path between the customer and a server is over optical fibre.
8. Tier 1 networks are the networks that are capable of interconnecting directly with any other Internet network (see lexicon).

IMPACT OF CONGESTION CONTROL ON QoS MEASUREMENT

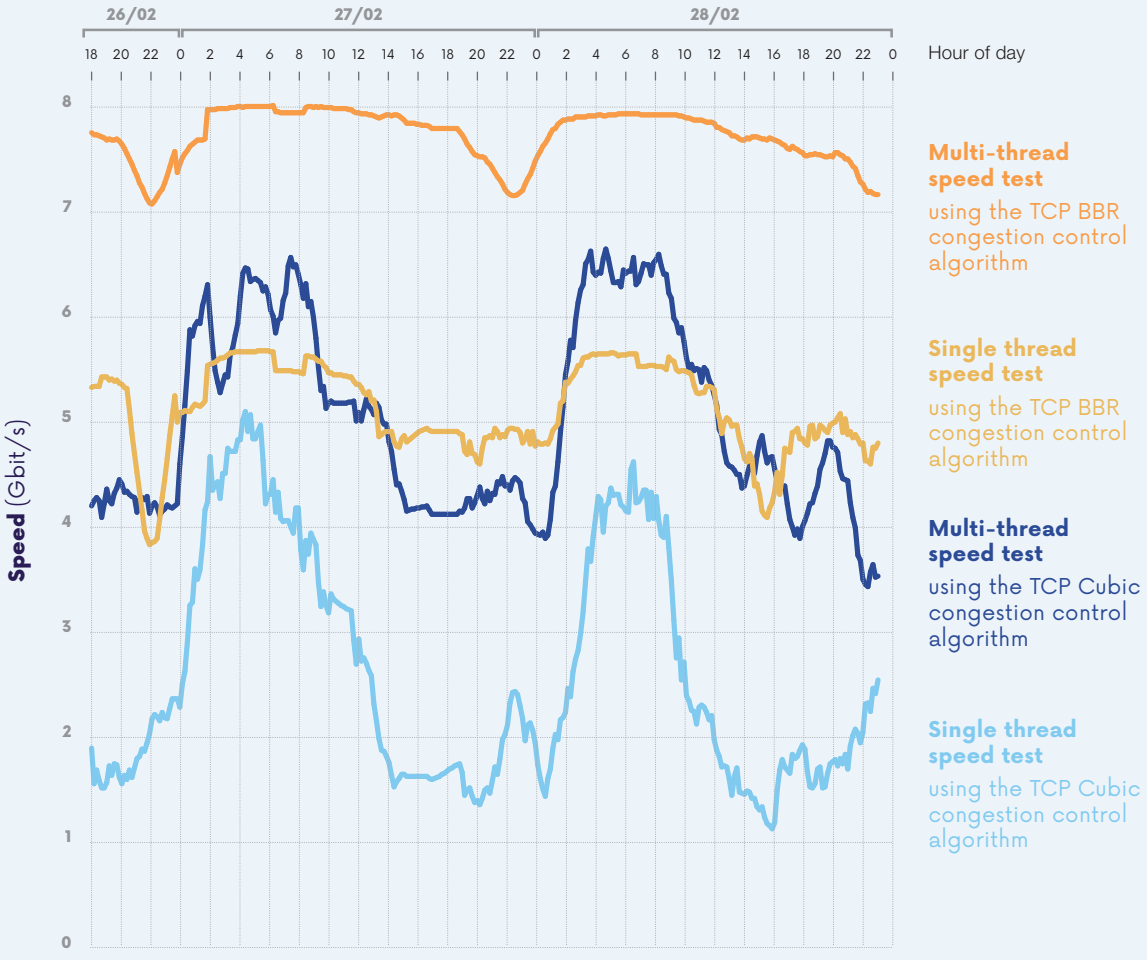
The technical choices that quality of service testing tools make can have a considerable effect on the measurement results. Some tools are only single thread, while others are multi-thread – i.e. transmit the speeds measured by adding together the speeds of multiple simultaneous connections. A third type of tool gives user the choice of running a single or multi-thread test. Multi-thread mode makes it possible to estimate a link's capacity during the test by determining its maximum throughput at that moment, using several parallel streams. Single thread mode makes it possible to provide speed results for a representative use of the Internet.

The results of QoS tests also depend on the test servers' technical properties, starting with their TCP congestion avoidance algorithm. These algorithms are used on the data transmitter side to decide packet transmission rate. Several TCP congestion avoidance algorithms exist, and all are evolving. Today, most of the Internet uses TCP Cubic, which was created in 2006 and which relies on packet loss as the signal to reduce speeds. It remains the TCP implementation by default on Linux, Android and MacOS.

In 2016 Google developed TCP BBR (Bottleneck Bandwidth and Round-trip propagation time) which uses a different model, based on maximum bandwidth and round-trip time. This approach enables TCP BBR to deliver higher speeds and lower latency than those enabled by algorithms based on packet loss, such as TCP Cubic. Some major Internet companies are starting to deploy BBR on their servers.

As illustrated below, download speed measurements will vary considerably depending on the combination of single vs. multi-thread testing and the congestion algorithm used.

DOWNLOAD SPEED ON AN 8 GBIT/S LINE, ACCORDING TO THE TYPE OF TEST PERFORMED



The lines correspond to the mobile connection average over 2 hours. Tests run by Breizh29 on a Freebox Delta with an iPerf3.7 client in Ubuntu 19.10 over IPv6, in the town of Ergué-Gabéric in the Finistère. Test server: lille.bestdebit.info hosted on the Bouygues Telecom network in Lille (Nord).

WHAT TEST SERVERS DO THE DIFFERENT QoS TESTING TOOLS USE?

For information purposes, in Annex 2 of this report, Arcep provides a list of the test servers used by the different tools. The features listed for each test server are as follows:

Sponsor: the name of the test server displayed on the QoS measuring tool. N.B. this name does not always make it possible to know which network is hosting the test server.

City/region: the test server's location.

IPv4/IPv6 protocol: some test servers are "IPv4 only" which makes it impossible to perform a test in IPv6. Tests run on IPv6-native connections and IPv4 transported on IPv6 show a slight gain in speed for IPv6 compared to IPv4. It is useful to conduct the test in IPv6 since 62 % of today's most visited web pages in France are accessible in IPv6*. Choosing an "IPv4 only" test server also enables a user to verify the quality of service they obtain in IPv4.

Connection capacity: the test server needs to have a high enough capacity to ensure that throughput is not a limiting factor in speed tests (it is often recommended to use a test server that can supply at least double one's presumed connection speed).

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

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

Host and AS (Autonomous System) name: make it possible to identify the network hosting the test server. Each AS identifies a network (at the routing level). Some companies may have several AS numbers to partition their operations, as the different autonomous systems may have different interconnection relationships.

* Source: 6lab Cisco on 28/10/2019, data on the top 730 Alexa in France.

TUTORIAL

HOW TO MAXIMISE A QoS TEST'S RELIABILITY?

On its website[1], Arcep details the minimum configuration (RAM, processor, network card, network cable, etc.) required to conduct a reliable test. This first level of methodological precautions does not, however, make it possible to circumvent any software installed on a device that may also affect connection speed. To run a QoS test that ignores the installed software, expert readers can follow the approach detailed below, which is based on creating a bootable USB drive and performing a test in Linux. A detailed tutorial is available on the Arcep website[2].

The prerequisite is to have a PC with a minimum 8 GB of RAM and a USB drive of a minimum 4 GB whose content can be erased. N.B. all of the content on the USB stick used will be lost.

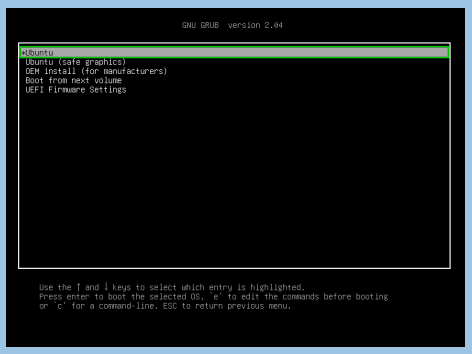
The steps are as follows:

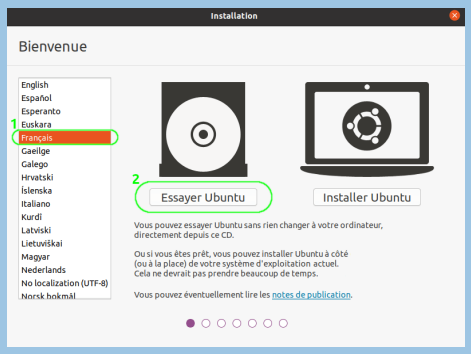
1. Create a bootable USB drive:

- Download an efficient Linux distribution such as "Ubuntu Desktop"[3];
- Download the software that will enable the creation of a USB drive, such as "Rufus"[4];
- Launch Rufus, insert the USB drive then select the ubuntu-desktop-amd64.iso file;
- Click on "Start" to launch the creation of the USB drive.

2. Restart your computer on the USB drive:

- Switch on the computer or restart it, and press the key to display the boot menu, before Windows loads. If there is a choice of two boot-up modes (either "UEFI" or "BIOS"/"legacy"), select "UEFI" mode.
- In "UEFI" mode, a screen with a black background will be displayed. Select "Ubuntu" then, on the welcome screen select "English then click on "Try Ubuntu".





3. Perform a quality of service test:

Simply launch Firefox, then your quality of service testing tool.

To monitor the CPU's usage percentage, launch the "System Monitor" application and click on the "Resources" tab. To guarantee that the quality of service test is not constrained in any way, the usage percentage in the processor's core must not exceed 70%.

1. How to design a reliable speed test?: https://www.arcep.fr/demarches-et-services/utilisateurs/comment-fiabiliser-un-test-de-debit.html (in French)
2. Tutorial for creating a bootable USB drive: https://www.arcep.fr/demarches-et-services/utilisateurs/creation-dune-clef-usb-bootable-pour-realiser-un-test-de-debit-fiable.html (in French)
3. To download "Ubuntu Desktop": https://ubuntu.com/download/desktop
4. To download "Rufus": https://rufus.ie

5. ARCEP'S MONITORING OF MOBILE INTERNET QUALITY

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

Every year since 1997, Arcep has performed a QoS audit on the mobile services provided by operators in Metropolitan France. The goal is to assess the quality of the services that mobile operators provide to users on a fully comparative basis, and thereby reflect the user experience in various situations (in cities, in rural areas, on different forms of transport, etc.) and for the most popular services (calling, texting, web browsing, video streaming, file downloads, etc.). This audit is part of Arcep's data-driven regulation strategy, and is designed to keep users informed. In 2019, more than a million measurements were taken on 2G, 3G and 4G systems in every department across the country, both indoors and outdoors, on transportation systems (TER, Transiliens, RER, metro, TGV, roadways) and in some 50 popular tourist destinations.

In 2017, Arcep launched an interactive mapping tool called monreseamobile.fr (my mobile network), which allows users to view mobile operators' coverage maps as well as all of the data collected through this QoS audit. France's overseas departments and territories have also been an integral part of monreseaumobile.fr since July 2018.

These measurements create the ability to track the progress of the quality of service available on the different networks, at a time when smartphones have become the main device used to access the Internet, and so to gauge operators' investments in their network.

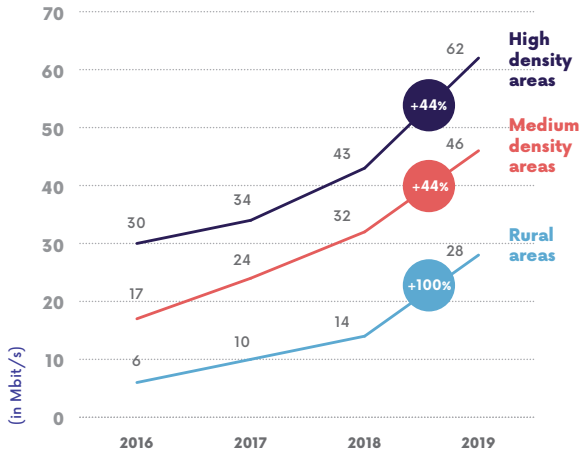
5.1. Average mobile connection speed in Metropolitan France stands at 45 Mbit/s, compared to 30 Mbits/s in 2018

The average speeds measured by Arcep continue to rise. In particular, and for the first time ever, the average download speed measured on mobile networks in Metropolitan France, all operators and all types of location (rural, medium density and high density) combined, has reached 45 Mbit/s – compared to 30 Mbit/s in 2018.

This progress is particularly striking in rural areas where speeds have doubled in a single year, reflecting operators' investment efforts including less dense areas. Performances in rural areas nevertheless still remain well below those in densely populated parts of the country.

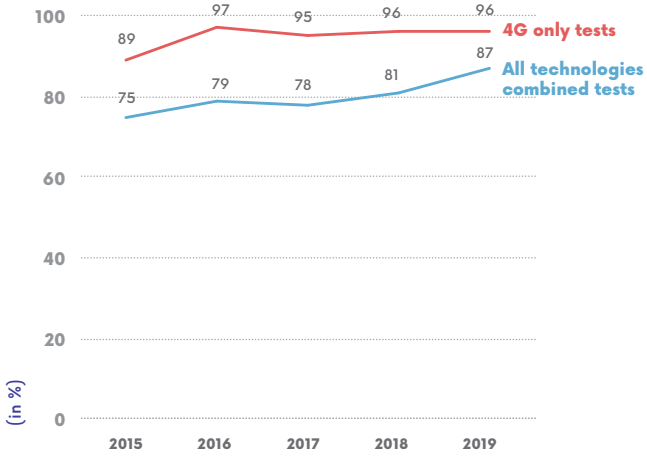
On the web browsing front, 87% of the web pages Arcep tested in 2019 – from amongst a sample of the 30 most visited websites in France – loaded in under 10 seconds. 4G has also driven considerable gains in this area, as the percentage of web pages that load in under 10 seconds over a 4G connection now stands at 96%. The ubiquity of 4G, targeted by the New Deal for Mobile, thus delivers a clear improvement in the quality of operators' data services.

AVERAGE DOWNLOAD SPEEDS (ALL OPERATORS COMBINED) IN METROPOLITAN FRANCE



Source: Arcep

WEB BROWSING (ALL OPERATORS COMBINED): PERCENTAGE OF PAGES LOADED IN UNDER 10 SECONDS IN METROPOLITAN FRANCE



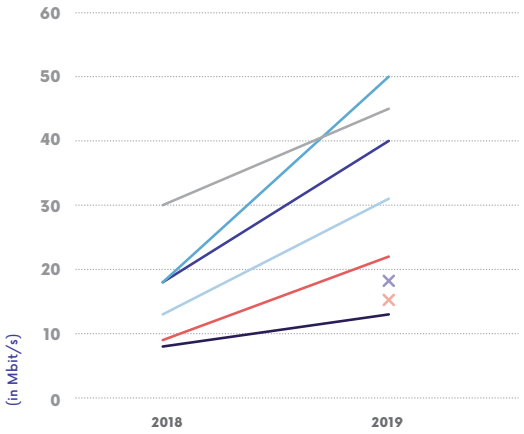
Source: Arcep

5.2. In French overseas territories too, quality of service is making a great progress

The substantial improvements in QoS achieved between 2018 and 2019 reflect the 4G rollout efforts in France's overseas departments and territories.

The quality of mobile data services has soared: average speeds have doubled in nearly every overseas territory, and web browsing quality has improved, on average, by 50%. These performances are now close to, and in some cases superior to, those found in Metropolitan France.

AVERAGE DOWNLOAD SPEEDS (ALL OPERATORS COMBINED)



Source: Arcep

WEB BROWSING (ALL OPERATORS COMBINED): PERCENTAGE OF PAGES LOADED IN UNDER 10 SECONDS

Source: Arcep

5.3. Improving *"Mon réseau mobile"*

Arcep has been working on developing its *"Mon réseau mobile"* (My mobile network) tool since late 2018.

It began by publishing a "regulator's toolkit" to address the needs of local authorities wanting to perform their own measurements, particularly to identify coverage needs under the New Deal for Mobile. The kit includes a sample set of technical specifications, that can be reused in calls to tender for selecting a service provider to carry out a field measurement campaign. A number of pioneering entities have already employed this document to conduct their own local connectivity measurements, including national railway company, SNCF, and several local authorities. Arcep has been engaged in an ongoing dialogue with these players and, since April, *"Mon réseau mobile"* has been further enhanced by the measurements obtained by different regions: Cher, Hauts-de-France, Pays-de-la-Loire and Auvergne-Rhône-Alpes. The tool will continue to become more information-rich by incorporating mobile QoS measurements that have been performed in compliance with the "regulator's toolkit".

Arcep has also published a "Code of conduct" for players who provide apps for testing the quality of users' mobile experience, such as crowdsourced app-based tests that anyone can perform on their mobile phone. The goal is to ensure a minimum set of requirements in terms of the relevance, presentation and transparency of the test results. To date, three players have declared themselves code-compliant (QoSi, nPerf and *60 Millions de consommateurs*). The solutions they provide have been adopted by several regions such as Hauts-de-France and Ille-et-Vilaine.

In more recent developments, Arcep adopted a Decision that seeks to strengthen the reliability threshold of operators' maps, from 95% to 98%. In fact, Arcep verifies the accuracy of these maps – which are produced using computer modelling – through field surveys. Up until now, Arcep have considered a map to be reliable if it had an accuracy rate equal to or above 95%. The Authority has now set that threshold at 98%. More specifically, the Decision proposes setting an "overall" reliability threshold for maps of 98%. It also stipulates local reliability thresholds: of 98% for every area of more than 1,000 square kilometres, and at 95% for all areas of more than 100 square kilometres.

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. In 2019, Arcep produced a scorecard of its pro-consumer actions and its "J'alerte L'Arcep"* reporting platform. The Authority received more than 20,000 reports in 2019. Of these, 47% concerned quality and availability issues with fixed or mobile services.

These reports provide valuable feedback for Arcep's diagnostic capabilities. They help make it possible to quantify and identify the problems that users are encountering, to then steer Arcep's actions towards the most appropriate solutions possible. For instance, to address any user experience gaps between the information that Arcep has published on its map-based tools (and on *"Mon réseau mobile"* in particular) and the reality in the field, Arcep increased the reliability threshold of its maps from 95% to 98%. User reports also help Arcep departments identify possible violations of its open Internet and net neutrality policies (cf. Chapter 4).

In 2019, Arcep also worked on improving its tool, in particular to clarify its classifications and sub-classifications. Special attention has been given to the "quality of service" classification, which represents the majority of customer complaints. It is also by increasing the number of details requested about specific cases that Arcep will be able to better examine certain topics in future. "J'alerte l'Arcep" will continue to evolve over the course of 2020, in particular to enable user reports to be sent directly from third-party tools: *Mon réseau mobile* (https://www.monreseaumobile.fr), *Ma connexion internet* (https://maconnexioninternet.arcep.fr), etc.

* 2019 scorecard of Arcep's pro-consumer actions, and of the "J'alerte L'Arcep" platform: https://en.arcep.fr/news/press-releases/p/n/data-driven-regulation-5.html

CHAPTER 2

Supervising data interconnection

HIGHLIGHTS

Inbound traffic to France's main ISPs has **increased by 29% over the last year** to reach 18.4 Tbit/s at the end of 2019.

The main ISPs' average installed interconnection capacities are **2.7 times** their inbound traffic volume.

55% of the traffic to the customers of France's main ISPs comes from four providers: Netflix, Google, Akamai and Facebook.

Interconnection[1] is the cornerstone of the Internet. It refers to the technical-economic relationship that is established between different actors to connect and exchange traffic. It guarantees a global network mesh and enables end users to communicate with one another other[2].

1. HOW THE INTERNET'S ARCHITECTURE HAS EVOLVED OVER TIME

In the beginning, the Internet was a hierarchical structure with Internet service providers (ISPs) who – to supply their customers with global connectivity – relied on transit providers to interconnect them with content and application providers (CAPs) and other ISPs. These transit providers, and especially Tier 1 providers, have thus played a central role in guaranteeing traffic routing, and Internet stakeholders have always depended on these players to ensure their traffic exchanges.

However, with the ongoing increase in Internet traffic and the need to bring content closer to end users, in particular to improve quality of service and quality of experience for end users, the Internet's architecture underwent a series of changes in a matter of years, during which several alternatives to transit emerged. These alternatives that enable ISPs and CAPs to free themselves, at least to some extent, of their reliance on transit providers come in several forms:

- The emergence and growth of content distribution networks (CDNs), which replace long-distance transport with proximity data storage on cache servers. CDN companies are thus able to circumvent the regular traffic routing value chain to some degree.
- The deployment of international networks, especially by the largest CAPs, which enable them to develop and own a long-distance transport infrastructure and improve their connectivity.
- The development of peering (other than peering between Tier 1 providers):
  - Some CAPs no longer rely on transit providers and instead connect directly to ISPs. Internet exchange points (IXPs) have facilitated the development of this type of direct interconnection;
  - More and more, ISPs are interconnecting directly with one another at the national or regional level, again in large part thanks to direct interconnection or at IXPs.

The transit market also continues to be highly competitive, with prices that vary depending on the routes, the number of competing players and the amount of data traffic being exchanged. Because they are so numerous and so heavily used, transatlantic links are among the least expensive in the world – contrary to links with Africa, for instance. Transit prices have fallen steadily over time, due to a combination of increasing traffic volume, a decrease in the unit price of network equipment, and competitive pressure. To give an example: according to market research firm, Telegeography[3], the average price of transit at the end of 2018, all routes combined, was around €0.50 per Mbit/s a month in Western Europe and in the United States, or 10 times less than in 2011, and around €2.50 per Mbit/s a month in São Paulo, Brazil (compared to €30 per Mbit/s a month at the end of 2011). These prices continue to decrease dramatically, especially in the most competitive markets.

1. Definitions of the technical terms related to interconnection that are employed here can be found in the Barometer of data interconnection in France: https://www.arcep.fr/cartes-et-donnees/nos-publications-chiffrees/linterconnexion-de-donnees/barometre-de-linterconnexion-de-donnees-en-france.html
2. N.B. this report refers only to data interconnection on the internet network, and does not address the interconnection of two operators' networks for the purposes of voice call termination.
3. https://global-Internet-map-2018.telegeography.com

As a result, even if global traffic continues to significantly increase, driving a steady rise in transit volumes, these two previous trends, i.e. strong competition and the advent of alternatives to transit, have been fuelling concerns for several years over the effects of the global transit market reaching maturity, which would result in transit providers' growth and revenue stabilisation.

Transit providers are working to adapt to the changing paradigm in two ways:

- Consolidation. This was an especially prevalent trend in the transit market during the previous decade, which saw a series of mergers and acquisitions of which the latest was Centurylink's takeover of Level 3 in 2016.
- Diversification. This mainly involves branching out into providing value-added CDN and security services, such as anti-DDoS solutions. This diversification is achieved either by developing the new business activity internally or by acquiring a company that specialises in that activity – with prime examples that include Tata Communications' takeover of Bigravity in 2011 and Centurylink's acquisition of Streamroot in 2019.

The interconnection market in France has been part of this global trend. The results obtained from the information gathering campaigns on data interconnection reveal a rise in the rate of peering compared to transit, an increase in the percentage of traffic coming from ISPs' on-net CDNs, as well as a concentration of traffic between a small number of players.

OPEN FLOOR TO ... DAVE SCHAEFFER

*By Dave Schaeffer, Founder and CEO - **Cogent Communications***

INTERNET TRANSIT DYNAMICS

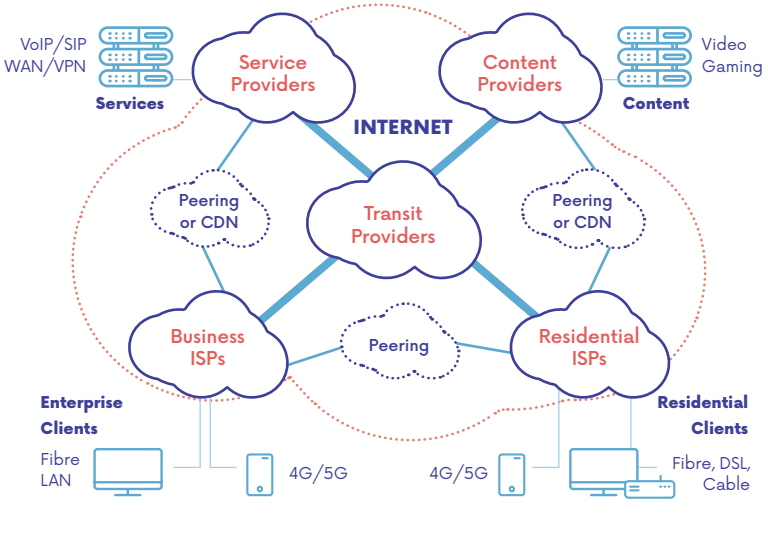
Since its inception, the Internet has developed as a network of interconnected networks: from a handful in 1996, to over 65 000 active Autonomous Systems (AS) today, all around the globe. The need for a transit layer developed very early: connecting locally to a transit provider (or a couple, for redundancy reasons), is obviously much more efficient than having to establish direct links to thousands of networks worldwide. Transit is at the core of the Internet. While peering exchanges, CDNs and other direct connect initiatives developed over the years, Internet transit has proven most efficient to cope with traffic growth, at a rate of over 45% p.a. on Cogent's network over the last 20 years, and has been consistently acting as a welcome "last resort" route when other connectivity methods failed.

As a matter of fact, CDN and other approaches to place online content and applications closer to end-users play an important part in the Internet ecosystem, however they have not become as ubiquitous as transit, because the vast amounts of capital required to establish and operate those edge nodes is not efficiently utilized. Internet transit today provides adequate connectivity, at a neutral network layer, to support all OTT applications, yet remaining independent from them. As an example, wide area networks (WAN*) for multi-site businesses tend to migrate from expensive and clumsy MPLS* VPNs* to flexible and cost-efficient SD-WAN* solutions, based on Internet access at each location: this is only possible because interconnectivity between last-mile Internet Service Providers (ISP) operates, often realized through transit networks, at equal or even higher standards than traditional private networks.

Transit has a unique place in the Internet connectivity ecosystem, and, at the same time, transit is a competitive marketplace. Technology, both transport and processing, has been consistently driving down costs of bandwidth, with no end in sight. Cogent's founding idea was that Internet bandwidth would become a commodity, such as power or water, and that, as a result, Internet carriers needed to act as utilities and produce bandwidth in large amounts, at the lowest possible unit cost. This vision has come true and Cogent, with its 150 000 km fiber network, more than 7 000 connected AS worldwide and a traffic volume of over 625 Petabytes crossing its network every day, is one of leading transit providers worldwide. The Internet is the only network that matters, and transit is the cornerstone of the Internet.

*See lexicon.

ROLE OF TRANSIT IN THE INTERNET ECOSYSTEM



OPEN FLOOR TO ...  JORG DEKKER

*Head of Internet services - **Telia Carrier***

FACING THE EVOLUTION OF INTERNET ARCHITECTURE

Leading the internet social responsibility

Telia Carrier's global Internet backbone, AS1299, accounts for nearly 60 percent of global Internet routes. Being a leader in its field entails plenty of responsibilities. For us, it implies duties for every customer, everywhere and one of these duties includes Internet routing security and stability. In the corporate world, this is called social responsibility. In our Internet ecosystem, this is called RPKI (Resource Public Key Infrastructure*) and Telia Carrier is the first Tier 1 service provider to have implemented it on a global scale, for both peers and customers, in February 2020.

RPKI is a mechanism by which IP resource owners can ensure that they provide an authoritative list of allowable upstreams to the world. This helps the BGP* announcement route validation and filtering of every provider, therefore preventing BGP hijacks (illegitimate advertisement of foreign address or AS number space, intentionally or not) and route leaks (illegitimate announcement of a route received from a peer/upstream to another one). Although not a new technology, RPKI has struggled, like IPv6, with poor uptake across resource owners and network operators. With our new global scale achievement and the unanimous acclamation received from our customers, both content providers and eyeballs, we believe many others will join us during 2020.

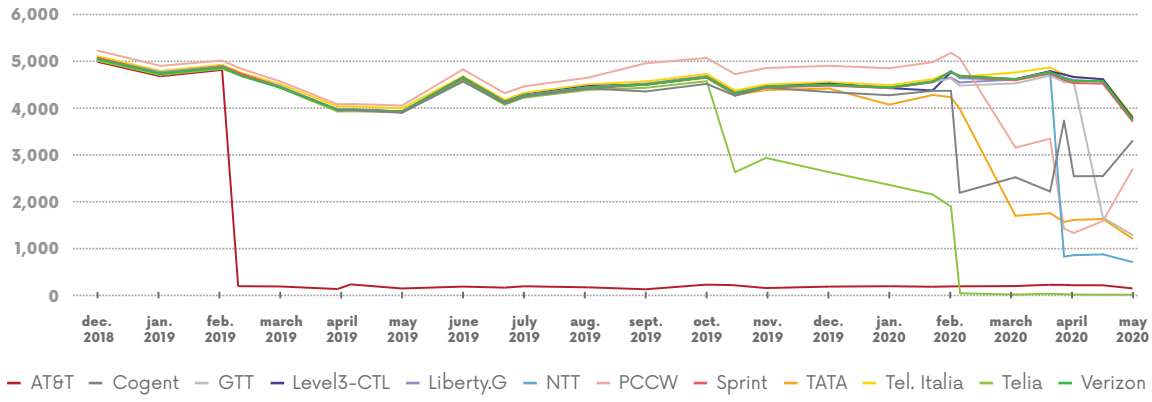
Always getting ahead of the growth curve

AS1299, represents over 2,000 direct customers, plus around 30 direct peers. The total traffic of 60 Tbit/s is spread over 150 edge devices, resulting into nearly 10,000 BGP sessions. During 2019, we deployed more than 10,000 new 100 Gbit/s ports. Increasing its agility while decreasing its costs, with the challenge of global scale, is not new for network providers. The change in today's reality is that networks need not only to plan the constant appetite for on-demand, unlimited and high-quality capacity required for 5G, streaming, gaming and always-on connections, but also to act fast and support its users in all situations.

The ongoing standardization of 400 Gbit/s coherent technologies incentivizes new, simplified and partially disaggregated IP over DWDM* architectures. Our ambition became to spearhead that wave with open optical line systems across several continents. In February 2020, we started the deployment of our new network architecture with unparallel network density, from 1 Gbit/s all the way to 400 Gbit/s, with cloud scale routing technology. More value has shifting to software, hardware cycles have become shorter and ongoing 400 Gbit/s standardization is poised to finally disrupt the optical networking market.

* See lexicon.

NUMBER OF NON-VALID IPv4 ROUTES



Source: CAIDA https://www.caida.org/publications/papers/2020/filter_not_filter/filter_not_filter.pdf

2. STATE OF INTERCONNECTION IN FRANCE

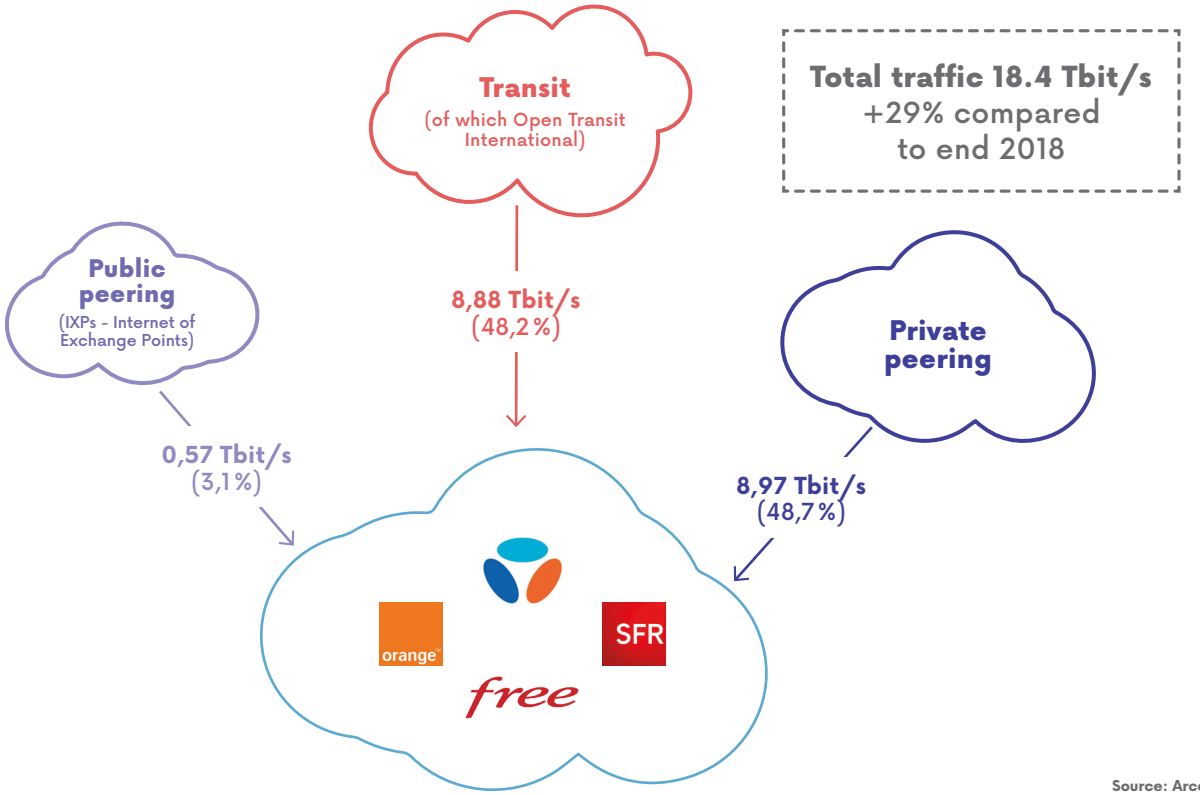
Thanks to the information gathering it does on data interconnection and routing, Arcep has technical and financial data on interconnection from the first half of 2012 to second half of 2019. For confidentiality reasons, the published findings[4] are aggregated results only.

2.1. Inbound traffic

Inbound traffic to the four main ISPs in France has increased from more than 14.3 Tbit/s at the end of 2018 to 18.4 Tbit/s at the end of 2019, which translates into a 29% increase in a single year. Half of this traffic comes from transit links. This relatively high rate of transit is due in large part to transit traffic between Open Transit International (OTI), a Tier 1 network belonging to Orange, and the Orange backbone and backhaul network (RBCI), which makes it possible to relay traffic to the ISP's end customers.

This rate is much lower for the country's other ISPs who do not operate as transit providers, and so make greater use of peering.

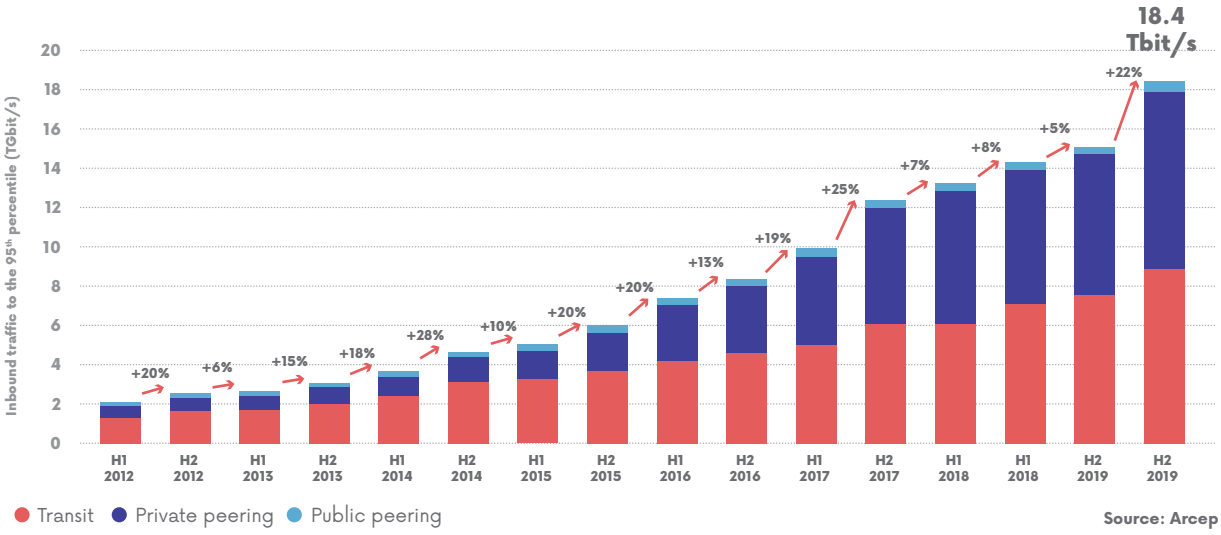
BREAKDOWN OF INBOUND TRAFFIC (95TH PERCENTILE) ON THE NETWORKS OF THE MAIN ISPs IN FRANCE (END OF 2019)



Source: Arcep

4. Results obtained from operators' responses to information gathering on the technical and financial conditions of data interconnection and routing, whose scope is detailed in Arcep Decision 2017-1492-RDPI (https://www.arcep.fr/uploads/tx_gsavis/17-1492-RDPI.pdf).

INBOUND TRAFFIC AT INTERCONNECTION LEVEL TO THE MAIN ISPs IN FRANCE, FROM H1-2012 TO H2-2019

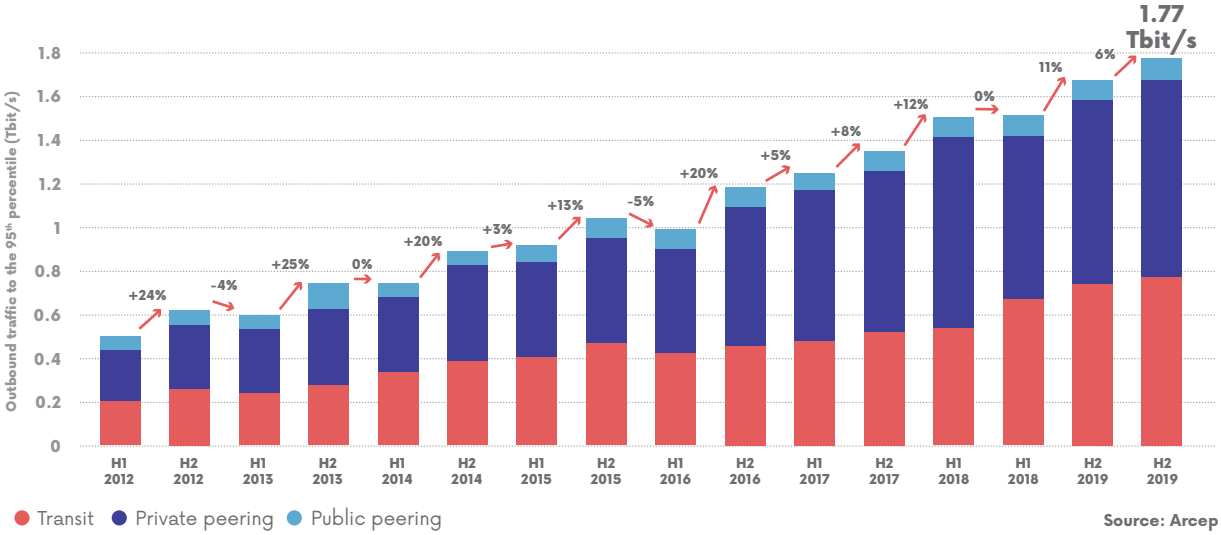


Source: Arcep

2.2. Outbound traffic

By the end of 2019, outbound traffic on the networks of France's four main ISPs stood at around 1.8 Tbit/s, or 17% more than at the end of 2018. This traffic quadrupled between 2012 and 2019.

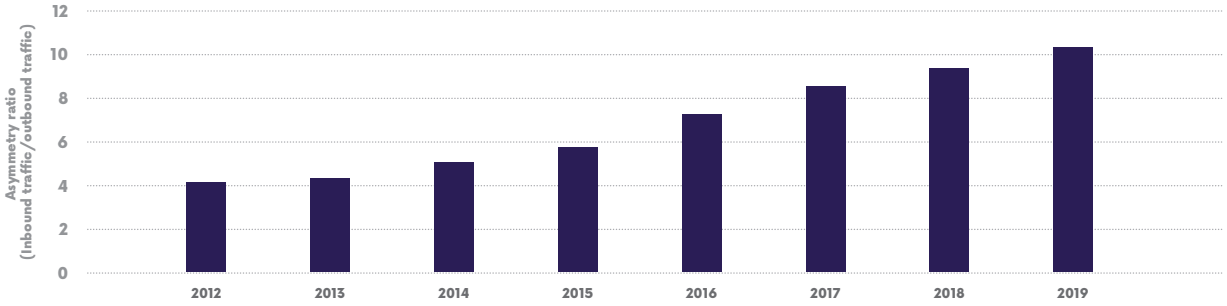
OUTBOUND TRAFFIC AT INTERCONNECTION LEVEL FROM THE MAIN ISPs IN FRANCE, FROM H1-2012 TO H2-2019



Source: Arcep

Outbound traffic is well below incoming traffic. Moreover, the asymmetry between the two has increased from a ratio of 1:4 in 2012 to one of more than 1:10 in 2019. This widening gap is due chiefly to the increase in the amount of multimedia content (audio and video streaming, downloading large media files, etc.) customers consume.

ASYMMETRY RATIO BETWEEN INBOUND AND OUTBOUND TRAFFIC AT INTERCONNECTION LEVEL FOR THE MAIN ISPs IN FRANCE BETWEEN 2012 AND 2019

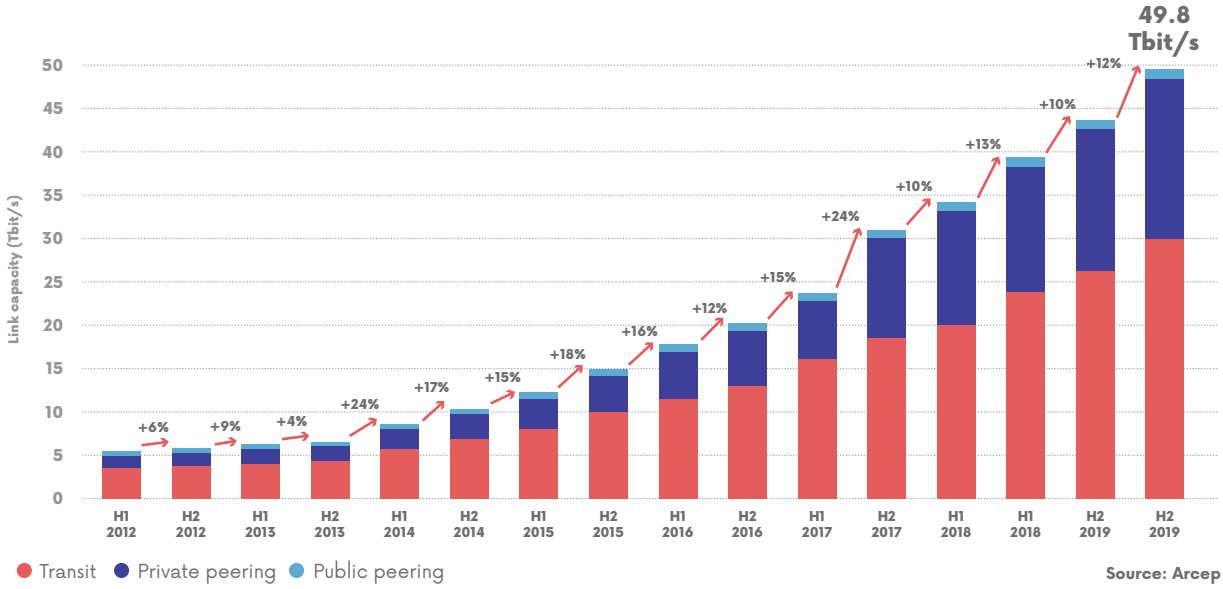


Source: Arcep

2.3. Evolution of installed capacities

Installed interconnection capacities have increased at the same pace as inbound traffic. Installed capacity at the end of 2019 is estimated at 49.8 Tbit/s, or 2.7 times the volume of inbound traffic. This ratio does not exclude occasional congestion incidents, which can occur on a particular link or links, depending on their status at a given moment in time, especially during peak traffic times.

INTERCONNECTION CAPACITIES OF THE MAIN ISPs IN FRANCE BETWEEN H1-2012 AND H2-2019



Source: Arcep

2.4. Evolution of interconnection methods

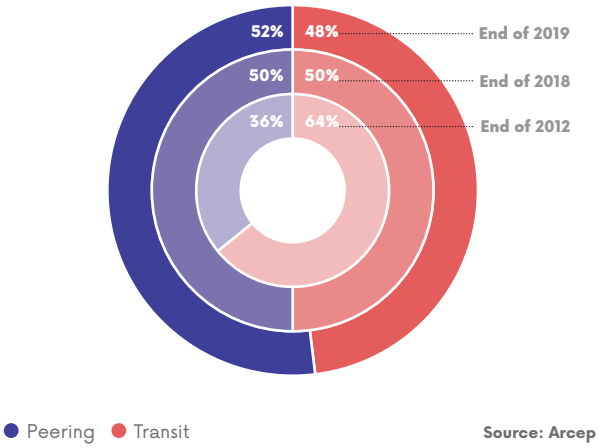
Peering vs. transit

By and large, peering's share of interconnection has been increasing steadily, due chiefly to the increase in installed private peering capacities between ISPs and the main content providers.

Peering's share increased slightly last year, going from 50% at the end of 2018 to around 52% at the end of 2019. This rise can be attributed to the increase in private peering traffic, and of public peering traffic to a lesser extent. Private peering's relative share rose from 47.5% at the end of 2018 to 48.7% at the end of 2019, while public peering's has gone from 2.5% to 3.1%.

EVOLUTION OF PEERING AND TRANSIT FOR THE MAIN ISPs IN FRANCE

(in proportion of inbound traffic volume)



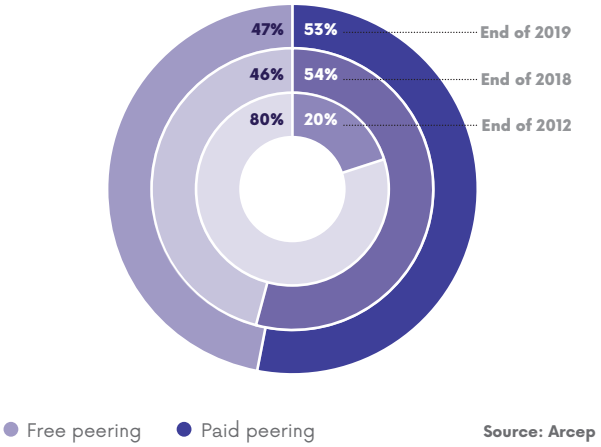
Source: Arcep

Free vs. paid peering

Paid peering's percentage of interconnection traffic has remained relatively steady (54% at the end of 2018 vs. 53% at the end of 2019). This situation can be attributed to the concomitant increase of private peering traffic – of which a substantial percentage is paid, notably when there are considerable traffic asymmetries – and of peering between companies of a comparable size, which remains free, by and large.

EVOLUTION OF PAID PEERING PARTS FOR THE MAIN ISPs IN FRANCE

(in proportion of inbound traffic volume)



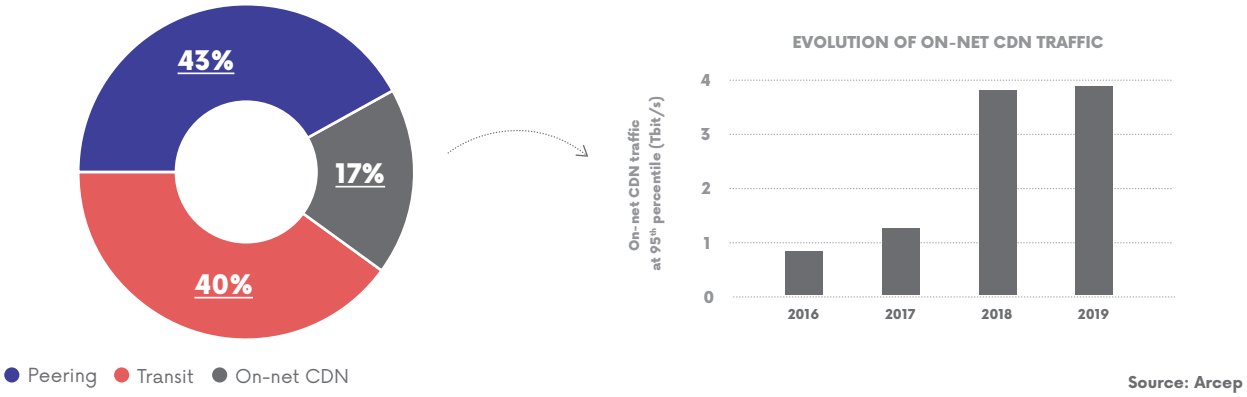
Source: Arcep

2.5. Traffic breakdown by interconnection type

Between the end of 2018 and the end of 2019, traffic coming from on-net CDNs to the top four ISPs' customers increased slightly to reach 3.9 Tbit/s. The percentage of traffic coming from on-net CDNs (17%) is down compared to last year (21%), which confirms that operators continue to make heavy use of both peering and transit. This percentage varies considerably from one ISP to the next: for some operators this traffic represents not even 1% of their traffic to final customers, while for others it accounts for more than a third of the inbound traffic being injected into their networks.

In addition, the ratio of inbound to outbound traffic ranges from 1:5 and 1:14 depending on the operator. In other words, data made available through on-net CDNs are viewed between five and fourteen times, on average.

BREAKDOWN BY INTERCONNECTION TYPE OF TRAFFIC TO CUSTOMERS OF THE MAIN ISPs IN FRANCE (END OF 2019)

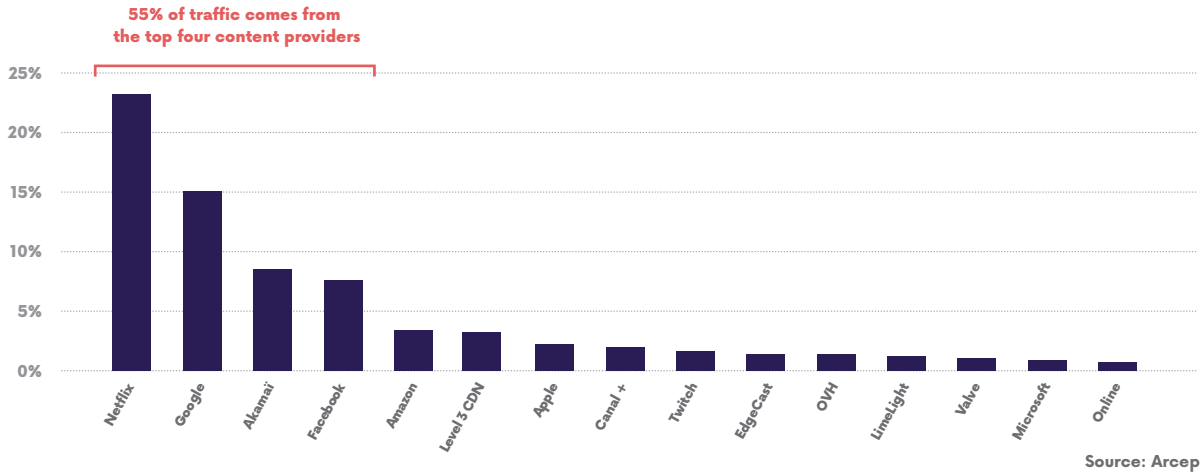


Source: Arcep

2.6. Traffic breakdown by origin

More than half (55%[5]) of all traffic to the customers of France's main ISPs comes from four providers: Netflix, Google, Akamai and Facebook. This testifies to the increasingly clear concentration of traffic around a small number of players, whose position in the content market is more and more entrenched. Added to which, the gap in the volume of traffic coming from Netflix compared to other service providers is actually widening.

BREAKDOWN BY ORIGIN OF TRAFFIC TO CUSTOMERS OF THE MAIN ISPs IN FRANCE (END OF 2019)



Source: Arcep

2.7. Evolution of costs

The range of transit and peering fees has not changed since last year. Based on collected data, the negotiated price of transit services still ranges from below €0.10 (excl. VAT) and several euros (excl. VAT) per month and per Mbit/s. For paid peering, prices range from between €0.25 (excl. VAT) and several euros (excl. VAT) per month and per Mbit/s[6].

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

5. Traffic coming from the top four content providers accounted for 53% of all Internet traffic at the end of 2018.
6. Price ranges only reflect the prices that the companies who answered the questionnaire pay for transit, peering or on-net CDN solutions.

OPEN FLOOR TO ... GINA HASPILAIRE

*Vice President - **Netflix Open Connect***

NETFLIX CONTENT DELIVERY: EFFICIENT STREAMING FROM BOXES TO BITS

ISPs and CAPs have a symbiotic relationship. ISPs create robust networks to deliver the internet to people's homes, businesses and schools. CAPs create and operate the internet-based services that make internet access valuable. In the case of Netflix, we have engineered a system which simultaneously reduces ISP's cost of operation, enables a higher-quality experience for our mutual subscribers, and minimizes the impact of streaming on the environment. We do this in three ways:

1- Netflix Open Connect: closer is better

Netflix Open Connect partners with over a thousand ISPs, including many in France, to help deliver Netflix traffic efficiently. Netflix provides its own cache servers, called Open Connect Applicances (OCAs) to ISPs free of charge and has deployed over 13,511 of these cache servers in 142 countries. ISPs install the OCAs within their local networks, allowing content to be served locally. This helps reduce an ISP's costs by minimizing the traffic flowing over transit connections, leased transport, and/or owned long-haul infrastructure. The closer the content is to those who watch it, the fewer circuits, routers, and other equipment are needed. If an ISP does not wish to take OCAs, Netflix offers to peer directly with ISPs at a mutually agreeable interconnection location. Either way, the localization of traffic substantially reduces the need for infrastructure running over long distances.

Open Connect is truly a partnership between Netflix and ISPs. We work together to deliver customised OCA deployment solutions that can localize up to 100% of an ISP's Netflix traffic. And ISPs exclusively determine the routes announced to deployed OCAs.

Further, refresh of the OCAs' content occurs off-peak when the volume of overall data traffic is at its lowest, minimizing the impact of content replenishment on traffic volumes by avoiding refreshing content during the busiest time of the day. Because networks are built and typically billed based on peak utilization rather than per byte, ISPs do not bear additional costs for using network capacity at off-peak times. This "pre-positioning" of content is unique to Netflix.

Finally, we increase efficiency by pre-loading popular content onto flash drives within the OCA so that less content is accessed from spinning drives, which require more power. Using faster media for popular content allows us to serve more traffic from a single device while using data center power as efficiently as possible.

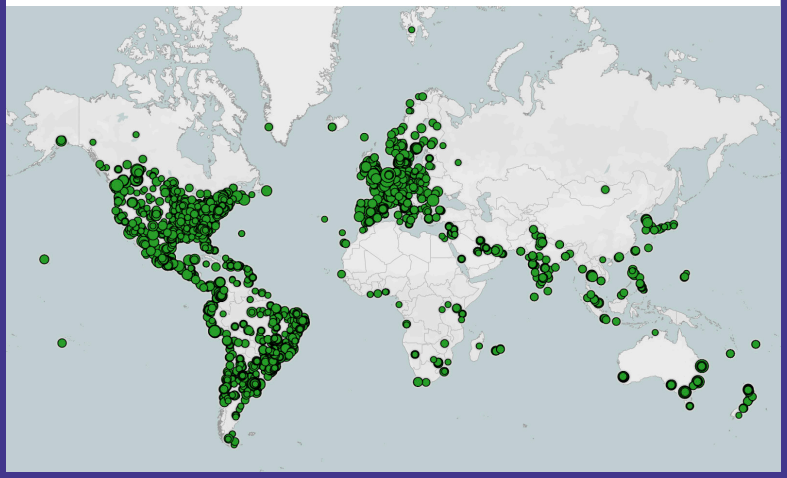
2- Open Connect Appliances: industry leading efficiency, provided free of charge

The amount of throughput per watt of power that each OCA is capable of delivering has grown over 100% while the OCA itself has become smaller. Previous models of OCAs required 4 rack units in a data center while new models deliver greater throughput with only a 2 rack chassis. This allows operators to get considerably higher throughput over time while the need for data center resources shrinks or remains flat.

3- Video Encoding: higher quality with less data

Netflix video encodes deliver high quality video with lower amounts of data. We recently announced AV1[1], a new encode that can reduce the amount of bandwidth needed for high quality video by 20% on mobile devices. We also adjust the amount of data needed for a video on a scene by scene basis so that simpler scenes require less data than complex ones. Netflix encoding reduces the amount of bits needed on a scene by scene basis so that an action scene may require a higher bitrate than a less complex scene (e.g. someone standing in front of a blank wall).

MAP OF OCA DEPLOYMENTS



1. https://netflixtechblog.com/netflix-now-streaming-av1-on-android-d5264a515202

OPEN FLOOR TO ... SAMUEL TRIOLET

*Director, Founder - **LyonIX/Rezopole***

THE TECHNICAL-ECONOMIC IMPACT OF IXP

Up until 2001, Lyon-based networks interconnected in Paris.

In addition to the technical aspects, such as poor latency, a lack of resilience and the system's *de facto* centralisation in Paris, this lack of a local exchange had, above all, an economic impact on the local IT industry, and on every economic player in general.

The outcome: we relied very little on local datacentres, local operators and local fibres. And businesses hosted their data in Paris or somewhere else abroad.

A substantial number of players, including locals, initially scoffed at the idea of creating an IXP in Lyon: " It makes no sense to set it up in Lyon, it will never work!"

Particular attention was given to the neutrality of the entity running the IXP, to foster cooperation, peering, between sometimes rival companies, which eventually resulted in the use of a consortium model.

With no initial capital, subsidies were needed and, in 2006, the Grand Lyon metropolitan area and the Rhône-Alpes region offered their support with subsidies. Which still represent 20% of the budget in 2019.

From the beginning, LyonIX enabled the different players connected to it, including large private and public sector accounts, not only to exchange IP traffic locally, but also to buy and sell a full range of telecom services through a straightforward and neutral marketplace. It was thus an IXP/NAP*.

In addition to peering and VLAN* interconnections, members could host their telecom equipment in LyonIX bays, and so further increasing the strategic nature of Lyon's IXP.

LyonIX is committed to being innovative, and in 2014 deployed an RPKI*, followed by a 100 Gbit/s VXLAN* EVPN* platform in 2018. Having been confined to the scale of a regional IXP from the start, interconnections with other IXP (8 French and 5 foreign) were encouraged, making LyonIX, the most interconnected IXP amongst its peers in Europe.

At the end of 2019, LyonIX had 100 entities connected to it, in 21 bays across seven PoP*. A team of nine employees ensures its operation 24/7 and hosts more than 20 events across the region every year. The machine network certainly requires a human network

Will the driving need for a local IXP be merely technical? Is the goal of gaining a few dozen milliseconds or enjoying free peering enough to motivate stakeholders?

There is of course a technical side, but it extends well beyond that: into economic aspects, employment, ecosystem, start-up, open-source economy and security through resiliency aspects that the IXP brings.

If entire swaths of today's IT operations are heading for a distant cloud, there is still a strong argument for local solutions. They prevent the flight of capital and the destruction of local jobs. We might also point out that a high quality telecom network is needed for accessing cloud solutions. The network cannot be relocated.

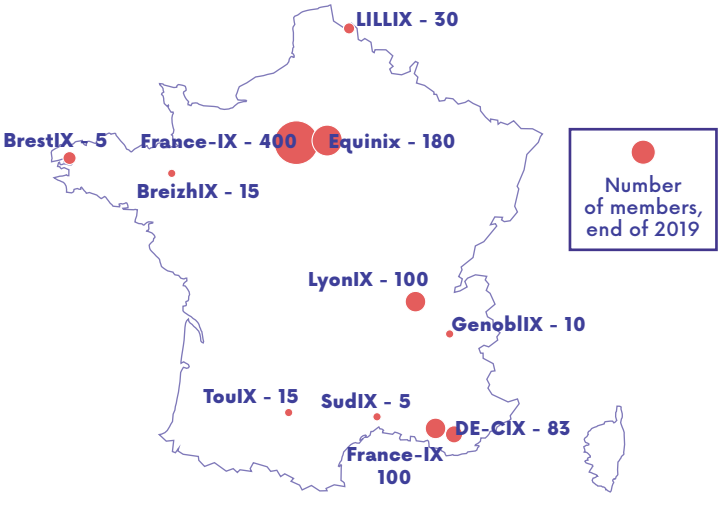
Lastly, now at the dawn of the 5G era, there is not a single digital industry player who is not aware of how vital it is to be as close as possible to human activity, as new use cases are set to explode around edge computing and artificial intelligence.

First assessement, 18 years after LyonIX was created: there are close to 15 datacentres in Lyon, more than 25 local and regional operators sell their services to businesses. And all of these players are of course connected through LyonIX.

Who says a regional IXP makes no sense?

* See lexicon.

MAP OF IXPS IN METROPOLITAN FRANCE



CHAPTER 3

Accelerating the transition to IPv6

HIGHLIGHTS

15 November 2019:
Arcep and Internet Society France launched the IPv6 task force. The goal: to encourage the entire Internet ecosystem to accelerate the transition to IPv6.

The exhaustion of IPv4 addresses was announced on **25 November 2019.**
Consequence: the Internet will continue to function, but will stop growing. The transition to IPv6 is the only future-proof solution.

Despite which only **27% of the most popular websites** in France are IPv6-enabled.

IPv4 and IPv6, which stand for Internet Protocol version 4 and version 6, are the protocols used on the Internet to identify every device or machine connected to the network (computer, phone, server, etc.). Public IP addresses are registered and routable on the Web, and are therefore unique worldwide identifiers. IPv4 and IPv6 are not compatible: a device with only IPv4 addresses cannot talk to a device with only IPv6 addresses. The transition is not performed by replacing IPv4 with IPv6, but rather by adding IPv6 on top of IPv4[1].

1. PHASING OUT IPv4: THE INDISPENSABLE TRANSITION TO IPv6

IPv4, which has been used since 1983, provides an addressing scheme of close to 4.3 billion addresses[2]. However, the Internet's success, coupled with the diversity of uses and the growing number of connected objects, has resulted in a steady decrease in the number of available IPv4 addresses, with some parts of the world being more heavily affected than others. By the end of June 2019, the top four operators in France had already allocated more than 90% of their IPv4 addresses[3].

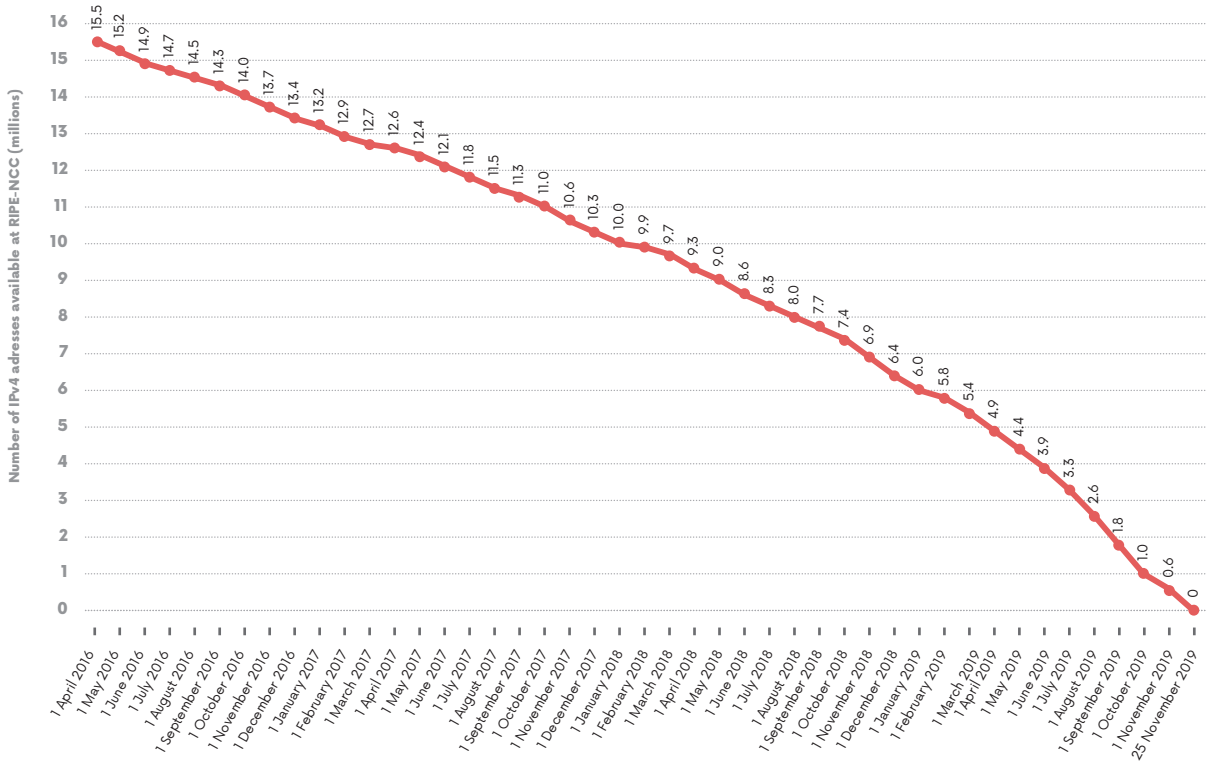
IPv6 specifications were finalised in 1998. They incorporate functions for increasing security by default and optimising routing. Above all, IPv6 delivers almost an infinite number of IP addresses: 667 million IPv6 addresses for each square millimetre of the earth's surface[4].

But the complexity of today's Internet means the transition from IPv4 to IPv6 can only be achieved gradually, starting with a period of cohabitation with IPv4. Once every player has migrated to the new protocol, IPv6 will fully replace IPv4 (switch-off phase). Even though the transition began in 2003, in 2019 the process was still only in the early part of the cohabitation stage[5].

In the 2019 edition of its report on the state of the Internet in France, Arcep estimated that the stock of IPv4 addresses would be exhausted by the end of Q2 2020, but the pace at which the last remaining blocks of IPv4 addresses were acquired accelerated, and IPv4 addresses had in fact run out by the end of 2019. On 25 November 2019, RIPE NCC (the regional Internet registry which is tasked with allocating IP addresses in Europe and the Middle East) announced that it had run out of IPv4 addresses, after having made the final /22 IPv4 allocation from the last remaining addresses in their pool.

1. In some instances, particularly on mobile networks, IPv6 is deployed instead of IPv4, in which case protocol translation mechanisms are put into place on the network (NAT64 and DNS64) and on devices (464XLAT).
2. IPv4 addresses use a 32-bit code. A maximum of 2^{32}, or 4,294,967,296 addresses can theoretically be assigned simultaneously.
3. Data collected by Arcep from ISPs, in accordance with Arcep Decision No. 2019-0287 of 12 March 2019 (https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000038383523&categorieLien=id).
4. IPv6 addresses use a 128-bit code. A maximum 2^{128} (i.e. around 3.4×10^{38}) addresses can theoretically be assigned simultaneously.
5. N.B. the observations and work mentioned in this document concern only the Internet and do not apply to the private interconnection between two actors, in particular the interconnection of the networks of two operators for the termination for voice calls in IP mode.

TIMELINE OF IPv4 ADDRESS EXHAUSTION



Source: RIPE-NCC data

There is a waiting list for IPv4 addresses that come back to the RIPE NCC, even though few of them do. RIPE NCC explains that these necessarily rare allocations will not be able to meet networks' current IPv4 address needs.

If continuing to have the Internet operate in IPv4 will not prevent it from functioning, it will prevent it from growing, because of the risks inherent in solutions that enable the Internet to continue to function in IPv4 despite the lack of addresses:

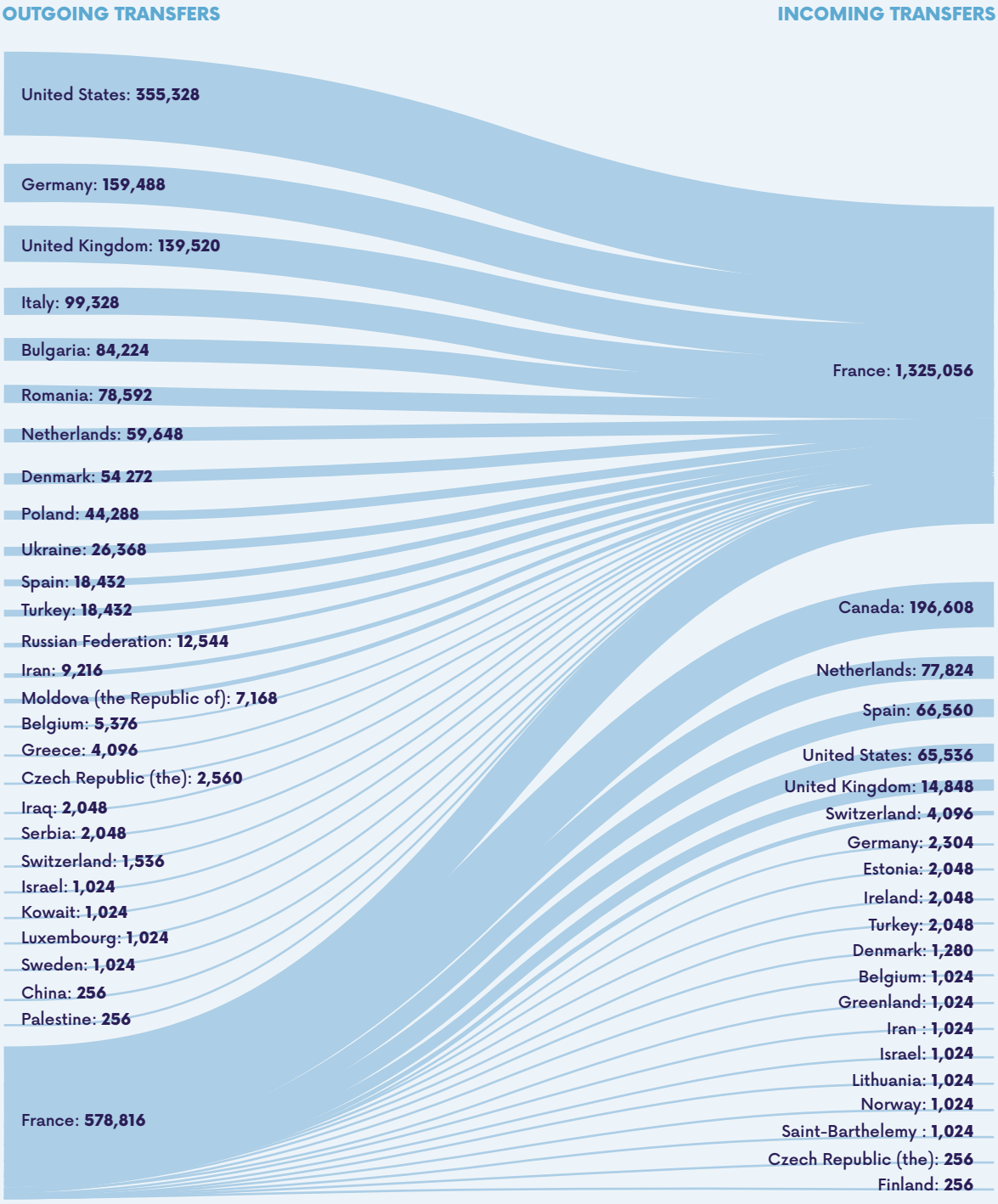
- Having several customers share IPv4 addresses could cause malfunctions on certain categories of Internet services (smart home control systems, network gaming, etc.). Added to which, these sharing mechanisms increase the risk to users of being denied access to a service, e.g. when an IP address they share has been put on a blacklist due to fraudulent behaviour by another user of that same IPv4 address. Another collateral effect of IPv4 sharing is the increased difficulty in identifying a suspect in a criminal investigation based on their IP address, in some instances requiring law enforcement agencies to investigate people whose only "crime" is sharing an IP address with the suspect.
- It is possible to buy IPv4 addresses on a secondary market, but the prices charged are likely to create a sizeable barrier to entry for newcomers to the market. Added to which, IPv4 address bought on the secondary market can block access to certain banking and video on demand services if the address's geolocation has not been updated.

These practices **increase the risk of seeing the Internet split in two, with IPv4 on one side and IPv6 on the other.** Some web hosting companies, for instance, now offer IPv6-only solutions, and the websites hosted on their servers cannot be accessed by IPv4-only operators' customers.

IPv4 ADDRESS TRANSFERS IN FRANCE

The graph illustrates the number of IPv4 addresses imported into, exported out of and transferred within France, along with the source and destination countries, up to March 2020.

NUMBER OF IPv4 ADDRESSES TRANSFERRED WITHIN, INTO AND OUT OF FRANCE



Source: RIPE NCC, March 2020

OPEN FLOOR TO ... MARCO HOGEWONING

RIPE NCC

THE IPv4 RUN-OUT

In November 2019, the RIPE NCC handed out the last of its remaining IPv4 address space. Four of the world's five Regional Internet Registries now have only token amounts or no IPv4 address space at all left to allocate to Internet service providers and other large-scale network operators. As a result, most companies look to alternatives – such as buying IPv4 addresses on the secondary market, deploying technical workarounds like Network Address Translation (NAT*), which allows multiple users to share addresses, or deploying IPv6.

The IPv4 market

The RIPE community developed a policy in 2012 to satisfy a need for RIPE NCC members to transfer unused addresses to one another. As a result, an active secondary market has developed.

With high demand and a limited supply, IPv4 space is costly, with current market prices ranging from 18-24 USD per address. In addition to the increased cost of expanding networks, an unintended consequence of IPv4 acquiring monetary value has been an increase in attempted fraud, theft and hijacking.

Technical workarounds

Technical solutions like NAT have been around for decades. Originally used in private networks, the same technology is now widely used in public networks, most notably by mobile network operators.

Although NAT has largely scaled to accommodate current demands, the equipment needed is costly, it can significantly increase latency, and it often reduces resiliency by introducing additional choke points or even single points of failure.

In addition, law enforcement agencies such as Europol have warned that large-scale NAT impacts their ability to investigate online crimes. Similarly, NAT hampers banks' fraud detection and mitigation systems. Many thousands of regular Internet users can also be affected if someone sharing their IP address is blocked from online services due to abusive behaviour.

Several governments are investigating legal options to reduce the number of users that can share a single address, or have successfully encouraged industry to reduce its use of NAT.

IPv6 adoption

Deployment rates for IPv6 are slowly but steadily increasing among Internet service and content hosting providers. IPv6 capability rates surpass the 50% mark in a few countries, while a number of the larger content providers – most notably Google, Facebook and Netflix – have already begun using IPv6 as a replacement for IPv4, not only by offering all their services on both IPv4 and IPv6, but more importantly by reducing the use of IPv4 in their internal systems to a bare minimum.

However, IPv6 rates remain low in many countries, even in those without enough IPv4 addresses to connect every citizen or household.

The situation in France

France currently has more than 83 million IPv4 addresses, with a population of just over 65 million, which puts it in a relatively favourable position compared to many other countries.

There have been 481 IPv4 blocks transferred within, into or out of France since 2012, comprising more than 14 million addresses. Some of these were the result of large acquisitions and mergers; removing those, there were about 136,000 addresses transferred within the country, 444,000 addresses imported, and 1.9 million addresses exported.

When it comes to IPv6, only 38% of French networks (Autonomous Systems) advertise IPv6 prefixes in the global routing system. Although this is above the global average (27%), it is also substantially lower than some other countries like Germany (56%)[1], suggesting that more work is needed to reach full IPv6 deployment.

Looking ahead

IPv4 run-out has real implications, and temporary measures to cope with it simply won't scale forever. Societies and economies are migrating online. There are still billions of people who require connectivity. And new and emerging technologies like the Internet of Things place ever greater demands on the Internet. The transition to IPv6 is the only long-term solution that will allow for this future growth, and for citizens, businesses and governments everywhere to benefit from the full potential of the digital transformation.

1. http://v6asns.ripe.net/v/6

* See lexicon.

This shortage of IPv4 addresses and the resulting risks make the transition to the new Internet communication protocol especially crucial to sustain competition and innovation.

In the report delivered to the Government in June 2016, which was produced in cooperation with Afnic, Arcep set out several courses of action designed to support and accelerate the transition to IPv6. Every year since then, Arcep has been publishing a barometer of the transition to IPv6, as part of its data-driven regulation approach. It has also begun a co-construction initiative with the Internet ecosystem in France, to federate the community and help speed up this transition.

THE TRANSITION TO IPv6 IS ON BEREC'S RADAR

In light of the exhaustion of IPv4 addresses and its consequences, BEREC has included the transition to IPv6 in its work programme for 2020. An internal workshop for experts from European NRAs will be held in the second half of 2020, to discuss the current status of the transition to IPv6 in Europe, to share best practices and to explore what role the regulator can play in helping to accelerate this transition.

THE "OBJECTIF IPv6" MOOC: USING EDUCATION TO HELP DRIVE THE TRANSITION TO IPv6

The "Objectif IPv6" massive open online course (MOOC) is a free training platform, operating under a Creative Commons licence, which allows anyone to acquire the basic skills and knowledge needed to implement and manage an operational IPv6 network. It was designed by teachers and researchers from Institut Mines-Télécom and from the Université de La Réunion, as well as network experts. Hosted on the Fun MOOC* platform, it had 2,000 registered students from 60 countries for its session 5, which was available from 6 June 2019 to 9 September 2019.

The aim of this course is to help participants **learn to implement IPv6 using an operational approach:**

- After a video that explains the key concepts, a **complete course** details the operational implementation process;
- Some **practical exercises** enable students to apply the IPv6 protocol in a functional virtual network on a workstation;
- More in-depth **exercises** include an examination of **case studies** encountered in the field.

The "Objectif IPv6" MOOC is open to students, professionals and non-professionals who are interested in the Internet's evolution. It provides a detailed description of the protocol and the mechanisms of computer networks. Mastery of the IPv4 protocol is no longer required. Key points will be reviewed as needed throughout the course.

This MOOC allows students taking the course to:

- Explain the different types of IPv6 address, **their notation and uses;**
- Create an IPv6 addressing plan **by taking network developments into account;**
- Implement the mechanisms required for an **operational IPv6 network;**
- Draft **an IPv6 network management plan** (fault detection, ensuring smooth operation and security);
- Explain the need for **network and service** interoperability **between IPv6 and IPv4;**
- Apply solutions **in different interoperability situations.**

The next session of the IPv6 MOOC, which will become available in autumn 2020, will include a partially updated curriculum, with new videos and new topics tailored to beginners and policy-makers, but also to IPv4 network experts wanting to learn to manage the implementation of IPv6 in their companies.

* Fun Mooc platform: https://www.fun-mooc.fr

OPEN FLOOR TO ... STÉPHANE BORTZMEYER

Afnic

THE IPv6 TRANSITION FOR DUMMIES

If you read Arcep publications, or if you have ever read an article about today's internet, you have no doubt heard of "IPv6". And you have probably read that there is a problem with the "transition to IPv6". This transition, and the snail's pace at which it is progressing, is in fact one of the internet's major failures. And one that truly warrants our attention.

All of the data circulating on the internet are broken down into small units called "packets". These packets must comply with a certain, standardised format so that any device connected to the internet can communicate with every other device. This format is called IP, which stands for Internet Protocol. The format has evolved over time, and three initial versions were tested unsuccessfully, before the fourth version, IPv4 (IP version 4) was adopted. IPv4 has one serious flaw: the space reserved for devices' IP address only allows for a maximum four billion addresses. This may sound like a lot, but that is not even equal to one address for every person on the planet. And a lot of people today have more than one device connected to the Web, and so require more than one IP address.

Awareness of this shortage of IPv4 addresses has become increasingly acute over the past several years, which has led to more or less honest workarounds, including the recent IPv4 address heist in Cape Town (and from a number of other South African players), not to mention the address theft reported to the authorities by African domain name registry, AFRINIC. As my grandmother used to say, "if there's not enough hay in the barn, the horses will fight".

The problem was identified a long time ago and, in 1995 (an eternity in internet years), version 6 of the Internet Protocol, aka IPv6, was created to solve it. Don't ask me what happened to version 5. So my personal blog has the address 204.62.14.153 in IPv4 and 2605:4500:2:245b::42 in IPv6.

It then "only" remained to move the entire internet to this new version, in the same way we moved from MS-DOS to Windows 3 then to Windows 95, then… (right up to Windows 10 today). But – and here's the rub – this transition that, according to the most optimistic predictions, was supposed to take just a few years, is still not complete. If every operating system has been compatible with IPv6 since the last century, if the main content hosts, like Google and Facebook, have had IPv6 in place for a long time, and if the many web hosting companies in France, such as OVH and Gandi, offer their customers IPv6, there is still not a complete IPv6 coverage. Some ISPs have still not made the transition to IPv6, and some websites still only have an IPv4 address.

So why the delay, after all this time? How many times since 1995 have we upgraded to a new computer, to a new smartphone, updated our web browser or our version of Android? Everyone and their dog has an opinion about this. Let us quickly dismiss the hypothesis that there is a technical issue. IPv6 is not a new protocol, just a new version of an existing protocol, and there is nothing scary about upgrading. Especially in a sector that is used to making much more disruptive changes, much more frequently. It is true that IPv6 is not compatible with IPv4, but that's often the case with upgrades: the HTTPS protocol (the secured version of the Web) isn't compatible with HTTP, despite which the transition was achieved far more quickly, in response to security issues with HTTP.

So if the hold-up is not technical, what is it? More than anything, it is a decision-making problem. For an internet company, switching one's network, servers and applications over to IPv6 is not a technical exploit, it is not very complicated to do, but the cost of doing so is also not zero. And, if each expense is assessed in terms of its eventual financial benefit, it's not hard to do the math: IPv6 benefits the collective good (as it eliminates the dearth of addresses) but there is no individual financial pay-off for players. Because the internet does not have an Overlord who could bark out the order: "Everyone switch to IPv6, and look lively!", and because everything depends on local decisions, it is extremely difficult to achieve transitions that are for the good of the whole, but not the individual.

Studying the issues surrounding the transition to IPv6 doesn't tell us anything about the technical aspect, or about computer network management. It does, however, tell us a lot about our decision-making processes. As with environmental issues, we are seeing that decisions that are made based on potential financial gains for the operator making the decision result in situations that are not good for the community as a whole.

TUTORIAL

HOW TO UNDERSTAND HOW IPv4/IPv6 STREAM DISTRIBUTION ON A SERVER?

Several tools can be used for network monitoring, but this tutorial is based on Munin for a Linux server.

Munin is an open source monitoring system, which is easy to install and integrated into virtually every Linux distribution. It is typically used to monitor several dozen servers, but can also be used in a desktop PC environment.

The Munin architecture is composed of a server process, called Munin-master, which collects information every five minutes on one or several PCs where the Munin-node is installed.

Munin-master creates the ability to generate a series of graphs that are presented through a web interface. These graphs can represent CPU usage, network memory, the motherboard or processor's temperature, etc.

Munin-node needs to be installed on every Linux station to be analysed. A number of plug-ins are available for Munin-node, including the one below for creating an IPv6 and IPv4 usage graph. The data are those culled from all of the analysed machine's network interfaces, if it has more than one.

To generate IPv6 statistics: first get the Munin IPv6 plug-in code from GitHub[1], then place it in a file named/usr/share/munin/plugins/ipv6_ and make the script executable:

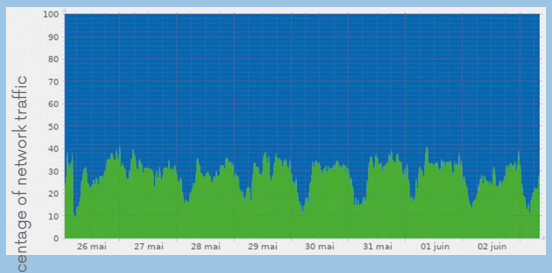
- **chmod +x/usr/share/munin/plugins/ipv6_**

Two links need to be created to activate the plugin: one for the graph expressing usage in percentages, and one for the graph expressing it in Mbit/s (or Gbit/s):

- **ln -s/usr/share/munin/plugins/ipv6_/etc/munin/plugins/ipv6_total**
- **ln -s/usr/share/munin/plugins/ipv6_/etc/munin/plugins/ipv6_percent**

Below is an example of graphs produced by this IPv6[2] plug-in:

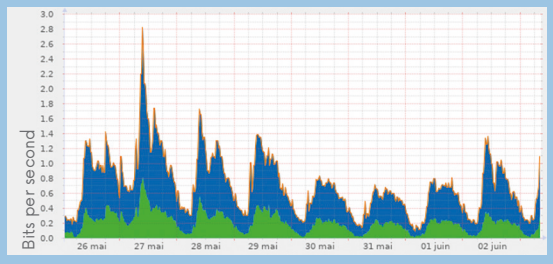
ALLOCATION OF IPv4 AND IPv6 PROTOCOLS – BY WEEK



	Current	Minimum	Average	Maximum
% IPv6	27.64	5.19	28.32	50.44
% IPv4	72.35	49.55	71.67	94.80

Last update: Wednesday June 3 2020 08:30:23

NETWORK TRAFFIC BY IP PROTOCOL – BY WEEK



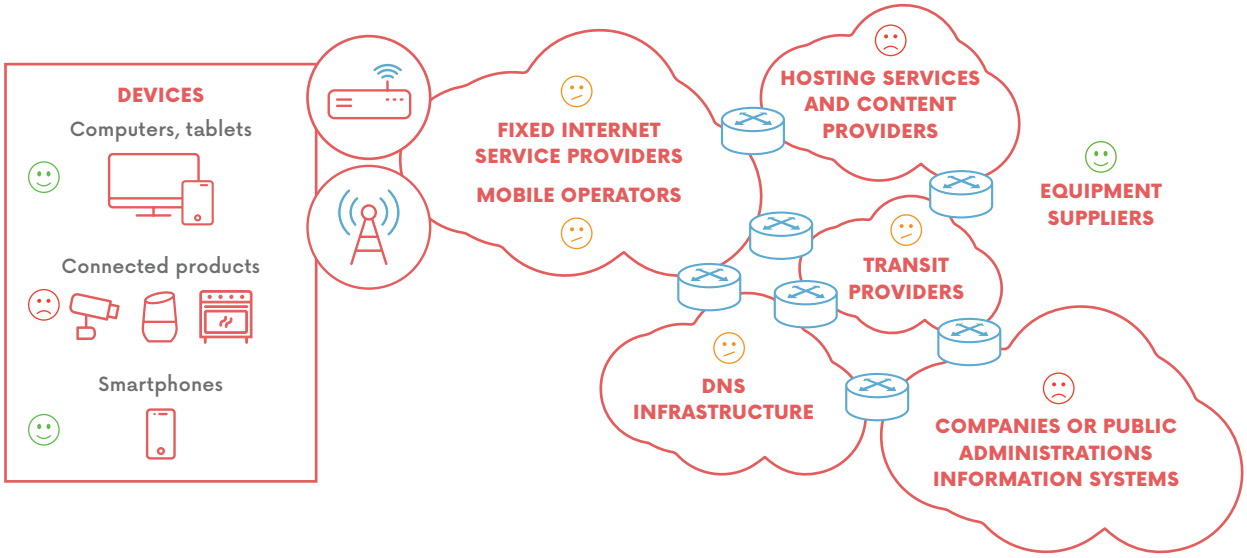
	Current	Minimum	Average	Maximum
IPv6 bps	304.15 M	8.61 M	210.29 M	864.46 M
IPv4 bps	793.40 M	58.95 M	499.13 M	2.35 G
Total bps	1.10 G	76.32 M	709.42 M	3.16 G

Last update: Wednesday June 3 2020 08:30:18

1. IPv6 plug-in for Munin: https://github.com/MorbZ/munin-ipv6/blob/master/ipv6_
2. Graphs excerpted from https://fr.archive.ubuntu.com/stats/stats_server.html

2. BAROMETER OF THE TRANSITION TO IPv6 IN FRANCE

STATUS OF THE TRANSITION TO IPv6 FOR THE DIFFERENT ECOSYSTEM ACTORS



Full or high compatibility with IPv6 — Partial compatibility with IPv6 — Little or no compatibility with IPv6

Source: Arcep

The purpose of this annual barometer is to keep users informed in an ongoing fashion. The barometer compiles data produced and provided by third parties (Cisco, Google and Afnic) and data that Arcep collects directly from the main operators in France[6]. It delivers a snapshot of the progress being made in IPv6 deployment in France, by the various stakeholders involved in the transition. Arcep published the 2019 edition of the barometer on 15 November 2019.

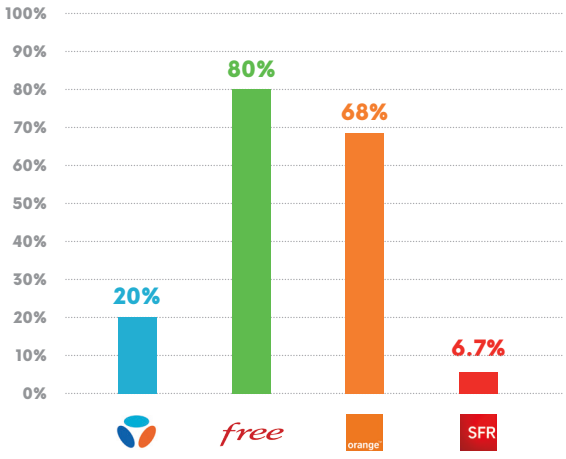
The 2019 barometer is an even richer source of information than previous editions, thanks to an expanded scope of information gathering (notably from operators with between 5,000 and 3 million active subscriptions in consumer retail markets) and the addition of exclusive data supplied by Afnic, notably on hosting services. As detailed here below, stakeholders are at different stages in the transition.

These findings confirm the progress made in the rate of IPv6 use in France, which stood at more than 38% in March 2020. After ranking below the European average last year in terms of IPv6 use[7], this year it has risen to fourth place, behind Belgium, Germany and Greece. The barometer provides a detailed look at the status of the transition for each of the ecosystem's stakeholders.

2.1. Fixed Internet service providers

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

FIXED NETWORK: PERCENTAGE OF IPv6-ENABLED CUSTOMERS



Source: data as of end of June 2019, collected by Arcep from operators

6. Arcep Decision No . 2019-0287 on implementing surveys in the electronic communications sector (https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000038383523&categorieLien=id)
7. Cisco 6lab as of 28/10/2019 (https://6lab.cisco.com/stats/index.php?option=users)

FIXED NETWORK: PERCENTAGE OF IPv6-ENABLED CUSTOMERS EVOLUTION

* **Figures subject to change**

Source: data as of end of June 2019, collected by Arcep from operators

Progress has been made on the main telecom operators' fixed networks in France, even if they do need to step up their efforts:

- At the end of June 2019, 100% of SFR customers were already IPv6-compatible on xDSL, 60% on FttH and 0% on cable. There has been notable progress on making FttH customers IPv6-ready, even if their numbers remain small (fewer than 7%, all technologies combined). Upcoming activations also remain inadequate: between 25% and 35% by mid-2020 and between 45% and 55% by mid-2022. Because the vast majority of users will not take the initiative to enable IPv6 manually, SFR is being urged to perform this configuration by default, as most other operators are doing.
- Bouygues Telecom has also made deployment efforts on its fixed networks (around 20% of customers were IPv6-ready as of mid-2019 compared to 2.5% in mid-2018) although IPv6 compatibility is still very low. Forecasts also remain far from sufficient (between 50% and 60% by mid-2022) to tackle the shortage. Bouygues Telecom is being urged to increase the number of IPv6-ready customers, and to step up deployment efforts on its fixed network.
- The percentage of Free and Orange fixed network customers who are IPv6-ready is relatively high: around 80% and 68%, respectively, at the end of June 2019, in addition to having increased. Projections for mid-2022 are encouraging (100% for Free and between 85% and 95% for Orange) but the dearth of IPv4 addresses requires an even greater acceleration in their transition.
- Free installed new firmware on the vast majority of its boxes in May 2019, and removed the ability to deactivate IPv6, which significantly increases the use of IPv6 in France.

As stated earlier, to improve the process of monitoring the transition to IPv6, Arcep has expanded data collection to include operators with between 5,000 and 3 million customers in the fixed network market. The number of operators that have begun their transition is still small, outside the welcome initiative of several operators, such as Coriolis, K-Net and OVH Telecom which continue the transition to IPv6 they started several years ago, as well as that of Orne THD which has already migrated all of its customers to the new protocol. More detailed information is available in the IPv6 barometer[8].

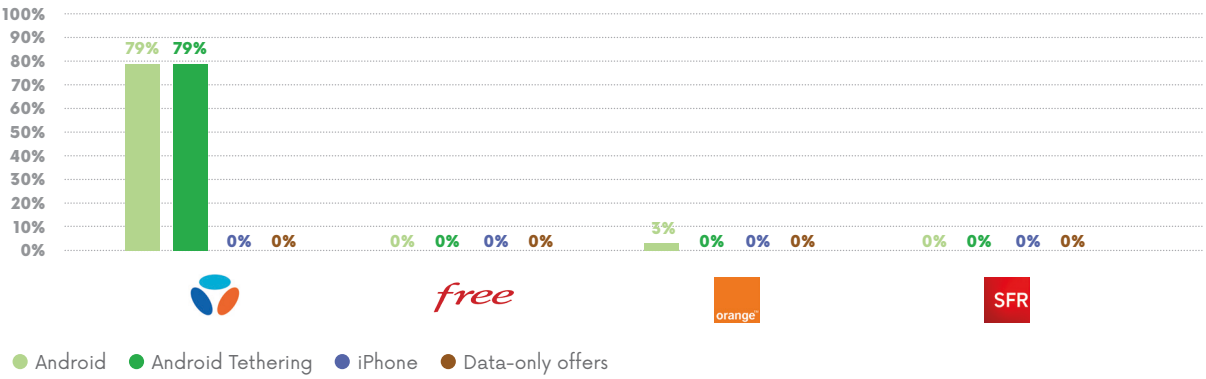
Even though Europe is currently experiencing a shortage of IPv4 addresses, some operators still have no plans to deploy IPv6 on their fixed networks which, as indicated above, would seem problematic.

8. Arcep's 2019 barometer of the transition to IPv6, "Operators with between 5,000 and 3 million fixed network customers": https://www.arcep.fr/fileadmin/cru-1574699937/reprise/observatoire/ipv6/Arcep_2019_Barometer_of_the_Transition_to_IPv6.pdf#page=9

2.2. Mobile operators

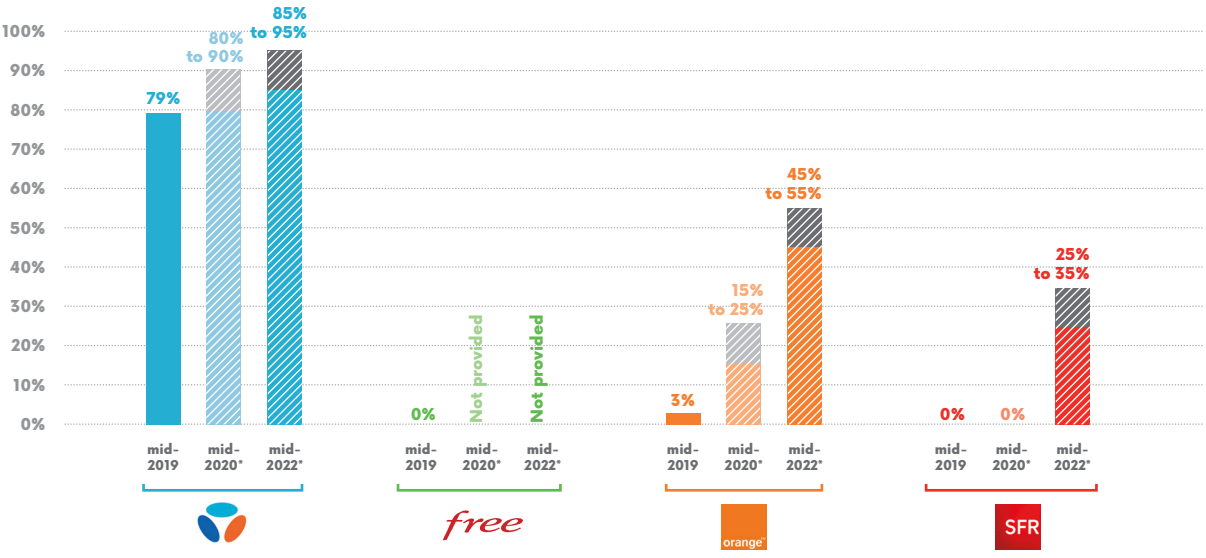
The following charts provide a snapshot of the current status of IPv6 deployment, along with forecasts for the main operators' mobile network in France.

MOBILE NETWORK: PERCENTAGE OF IPv6-ENABLED CUSTOMERS



Source: data as of end of June 2019, collected by Arcep from operators

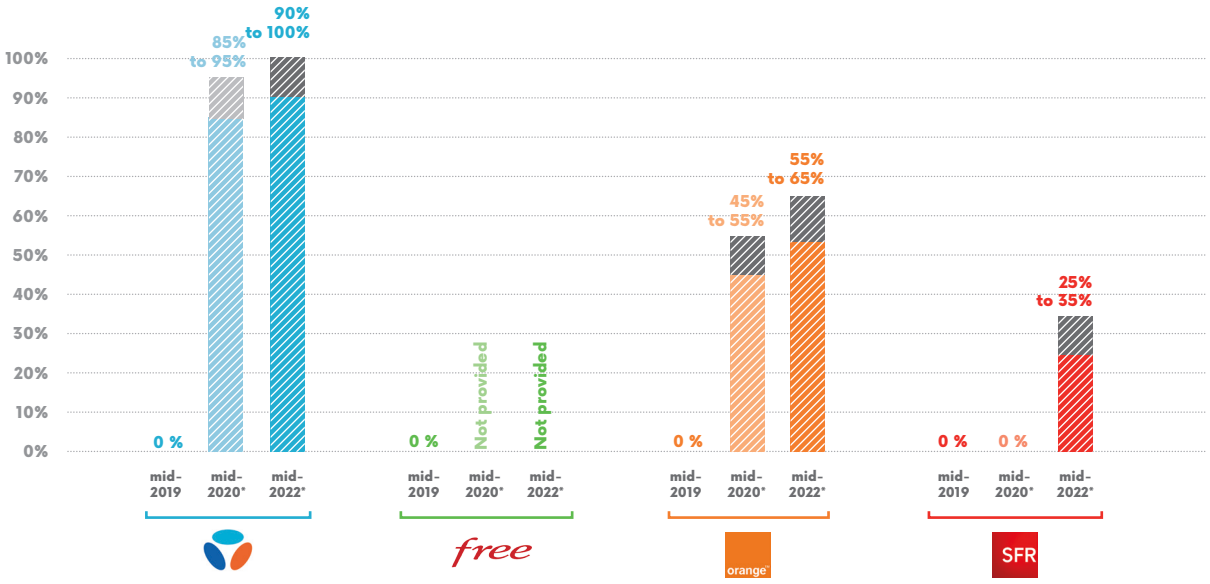
ANDROID: PERCENTAGE OF IPv6-ENABLED CUSTOMERS EVOLUTION



* Figures subject to change

Source: data as of end of June 2019, collected by Arcep from operators

iPHONE:
PERCENTAGE OF IPv6-ENABLED CUSTOMERS EVOLUTION



* **Figures subject to change**

Source: data as of end of June 2019, collected by Arcep from operators

Arcep has serious concerns about the sluggishness of IPv6 deployments on mobile networks, and is urging operators to take the necessary steps to respond to the dearth of IPv4 resources:

- Bouygues Telecom continues its mobile network deployments, with 79% of Android customers now IPv6-enabled.
- Orange forecasts for Android customers are worth noting (between 15% and 25% by mid-2020 and between 45% and 55% by mid-2022) even if the operator is being urged to increase the number of IPv6-compatible devices.
- Bouygues Telecom and Orange made a remarkable push on iPhones in September 2019: 68% and 30% IPv6-enabled, at the end of October 2019.
- Despite SFR's forecasts for 2022, Arcep believes the pace of deployment and the targets are insufficient.
- It is particularly regrettable that that Free Mobile was unable to supply its forecasts.
- Operators are being called on to begin IPv6 deployment on all of their products, notably "data only" plans and those aimed at businesses.

Zeop is the only mobile operator with between 5,000 and 3 million customers which has begun to enable IPv6 on its network[9].

Even more than on fixed networks, the pace of mobile networks' future IPv6 deployments is very likely to slow down the transition to IPv6.

2.3. Web hosting services

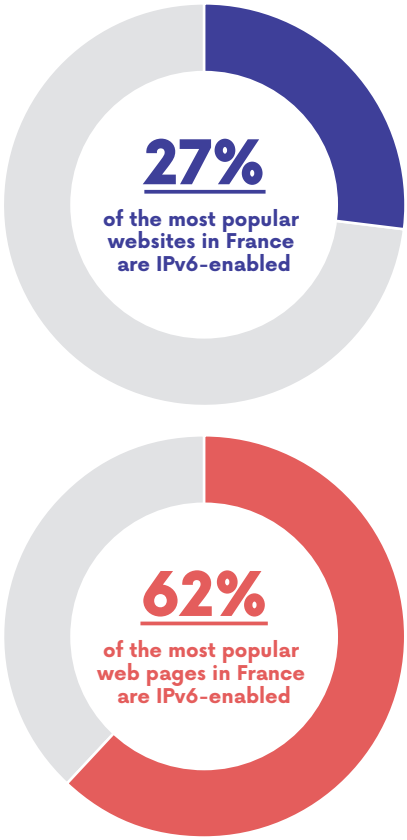
Web hosting services continue to constitute one of the main bottlenecks in the migration to IPv6: of the most popular websites in France according to Alexa rankings, only 27% are IPv6-enabled[10]. A site is considered IPv6-enabled if its domain name is mapped as being IPv6 (AAAA) in the DNS server record.

Note that the percentage of web pages that are IPv6-enabled (IPv6 content) is significantly higher than that (62%)[11]. The reason is that many of the smaller content providers operate websites (generally small number of pages viewed) that are not IPv6-compatible.

The percentage of IPv6-enabled sites falls to a mere 15.5% when looking at the 3.5 million .fr, .re .pm .yt .tf and .wf[12] websites. This figures has been rising since 2015, but the pace of this increase seems far from making it possible to achieve a complete transition to IPv6 over the next few years.

Even though several hosting services offer IPv6, the percentage of IPv6-enabled websites is very low amongst the Top 10 because it is not enabled by default. Of the Top 10 players, only 1&1 IONOS and Cloudflare are leading by example, with more than three-quarters of websites IPv6-enabled.

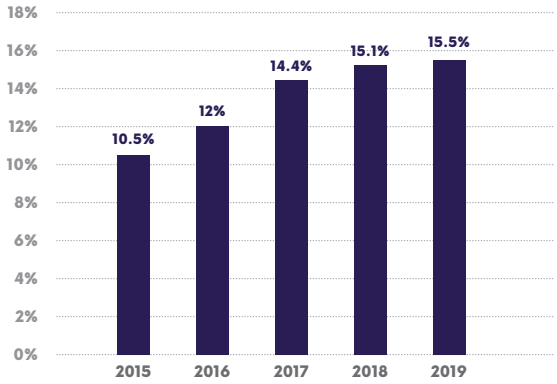
9. Arcep's barometer of the transition to IPv6 in France 2019: https://www.arcep.fr/fileadmin/cru-1574699937/reprise/observatoire/ipv6/Arcep_2019_Barometer_of_the_Transition_to_IPv6.pdf#page=13
10. Cisco 6lab as of 28/10/2019 (http://6lab.cisco.com). Data on Alexa's Top 730 sites in France www.alexa.com/topsites/countries
11. Ibid
12. Afnic data, September 2019



Source: Cisco 6lab as of 28/10/2019 (http://6lab.cisco.com)
Data on Alexa's Top 730 sites in France
www.alexa.com/topsites/countries

EVOLUTION OF THE PERCENTAGE OF IPv6-ENABLED WEBSITES

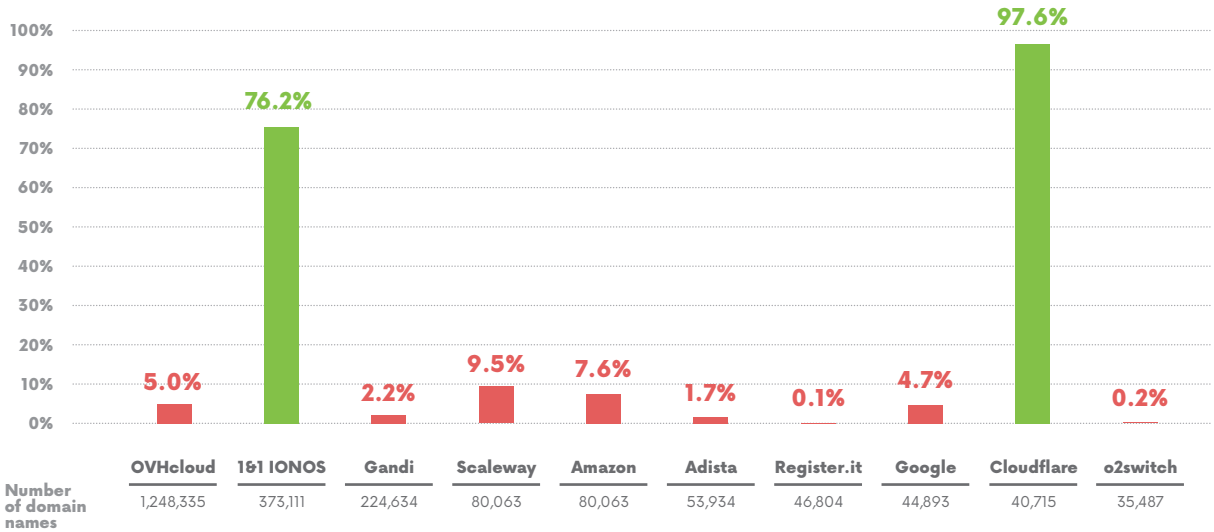
on .fr, .re, .pm, .yt, .tf ET and .wf domain names



Source: Afnic data, September 2019

PERCENTAGES OF IPv6-ENABLED WEBSITES

on .fr, .re, .pm, .yt, .tf ET and .wf domain names



	OVHcloud	1&1 IONOS	Gandi	Scaleway	Amazon	Adista	Register.it	Google	Cloudflare	o2switch
Number of domain names	1,248,335	373,111	224,634	80,063	80,063	53,934	46,804	44,893	40,715	35,487

Source: Afnic data, February 2020

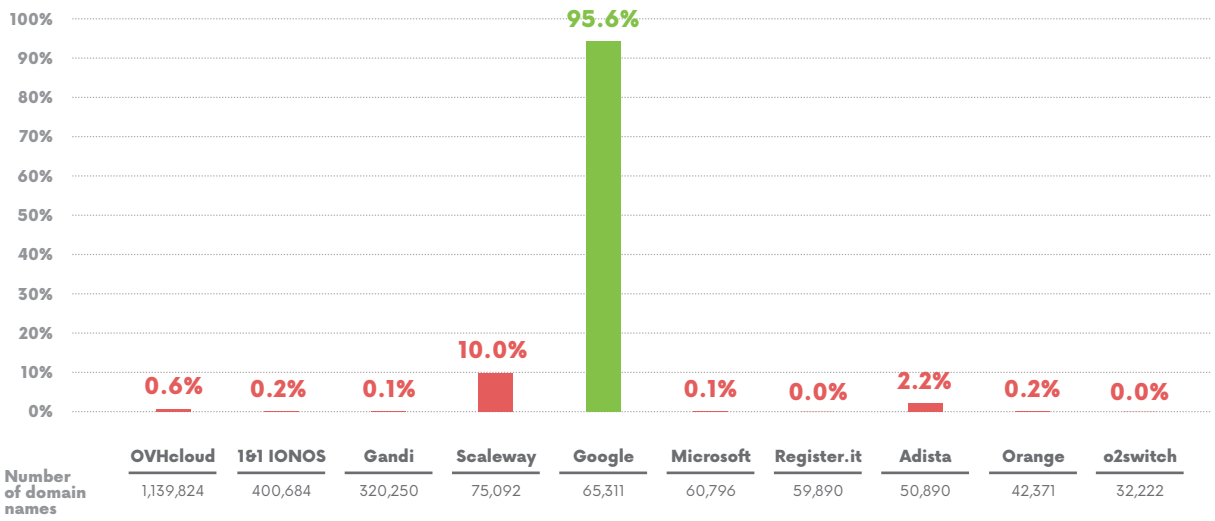
2.4. Mail hosting services

The transition of the main mail hosting services is also proving extremely slow: only 5.8% of mail servers on .fr, .re, .pm, .yt, .tf et and .wf domain names[13] are currently IPv6-enabled (compared to 5.2% at mid-2018). It should also be noted that on a number of them, there is an IPv6 redundancy level that is below the one provided for IPv4, which is likely to create resilience issues.

This lack of IPv6-readiness amongst mail hosting services is alarming, as a protracted lag on this section of the Internet value chain could force IPv4 to be kept for far longer than expected, with all the resulting costs. Only Google stands out here, with more than 95% of domain names for mail in IPv6.

PERCENTAGE OF IPv6-ENABLED MAIL HOSTING

on .fr, .re, .pm, .yt, .tf ET and .wf domain names



Source: Afnic data, February 2020

For more information on the status of IPv6 deployment, the barometer of the transition to IPv6 is available on the Arcep website[14].

To help improve the quality of the information that Arcep publishes, and to guarantee greater transparency on the transition's progress, Arcep's annual survey will incorporate several improvements:

- Streamlining the requested indicators to improve the accuracy of the published information, and better detect any possible bottlenecks;
- Replacing the questionnaire for web hosting companies with a data analysis supplied by Afnic, to have a more complete progress report on these players;
- Adding a questionnaire for the main operators serving the business market, to obtain information on the status of this market's transition.

When it comes to the transition to IPv6, it is very important that the Government lead by example to help galvanise the process. To this end, the possibility has been raised of including indicators on the transition status of the Government's different websites and online services in the next edition of the Barometer.

The next barometer will be published in the second half of 2020.

13. Afnic data, September 2019
14. https://www.arcep.fr/cartes-et-donnees/nos-publications-chiffrees/transition-ipv6/barometre-annuel-de-la-transition-vers-ipv6-en-france.html

OPEN FLOOR TO ...  JOAQUIM DOS SANTOS

*Director of Research and Development - **IKOULA***

IPv6 MICRO-SERVERS ARE NOT IPv4-COMPATIBLE

You already know that one of the resources that supports the internet's development – namely IPv4 addresses – has been exhausted. You might say: but we can still buy them, or request them from official registries, as long as you are willing to wait for some to become available... But, realistically, what can a hosting company like IKOULA do to cope with this shortage?

The world of web hosting has been dealing with this threat for several years now. We at IKOULA, for instance, already decided some years back to supply a (small) slash of IPv6 addresses (65536), to enable the transition for every dedicated server that had an automatically configured IPv4 address. There was no shortage of questions that needed answering. What addresses do we provide to our customers? How many? How to facilitate the transition in people's minds, from 127.0.0.1 to ::1? How to help understand and handle addresses such as 2a00:0c70:abba:fa00:de00:-ca00:7833:547b?

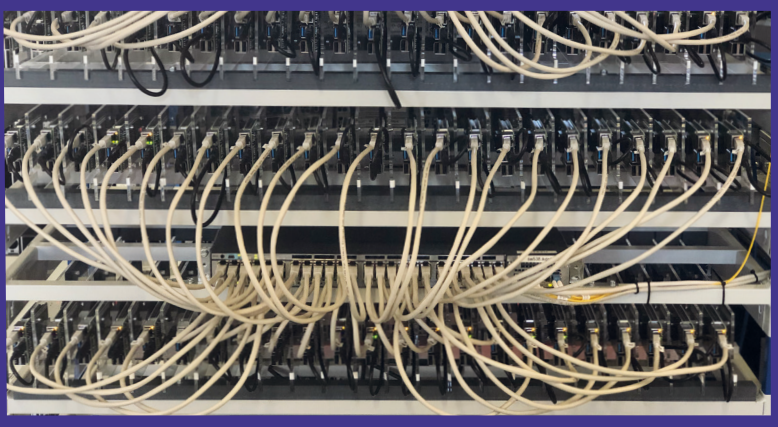
Initially, we decided to "match" the IPv6 addresses received with the configured IPv4 address. For instance, an IPv4 address such as 213.246.53.53 would be assigned 2a00:c70:1:213:246:53:53:0/112. Unfortunately, this was not as well received as we had hoped, even if it did help several customers to implement certain services, and to make the most of the famous /112. A few bugs and side-effects also appeared over time, one of the most memorable being the specific way an smtp/http parser processed the characters [and] in IPv6 addresses, which needed to be tweaked...

The RIPE announcement in April 2018 came at a time when we at IKOULA were in the process of exploring what some call micro-servers. We were looking for a way to satisfy several needs: to reduce our servers' carbon footprint and the amount of space they occupied, but also to streamline their daily operation for the technical teams and, last but far from least, to design leading edge and ultra-competitive solutions for our customers! Some of our team members, who are passionate about ARM architecture, had even begun testing out the brand new Raspberry Pi 4 and its 4 Gb of RAM. So all of the elements were in place to give birth to a full IPv6 solution, with a unique /128 address, without dual stack and which was not IPv4-compatible.

Some aspects had to be rethought, such as the holder for these Raspberry computers, but also adding HD/SSD drives to these machines (as there is not distributed storage or boot on the network), the bootstrap, and the operating system's configuration. Ultimately, very few alterations were required on the "purely" network side of things, as IKOULA had been prepared for the advent of IPv6 for a long time.

But the story doesn't end there, since an IPv6 address CANNOT connect to the entire Internet, and vice-versa! We have therefore installed a transition mechanism – NAT64 – using open source software, which creates the ability to provide full internet access to a machine that DOES NOT have an IPv4 address but only an IPv6 one (e.g. our Raspberry computers). The mechanism is composed of two elements: the NAT64 to translate the original IPv4 request to the internet using a source IPv4, and the DNS64 to answer a specially "calculated" IPv6 address for any domain WITHOUT an AAAA record (present if the domain name has an IPv6 address).

This solution was an immediate hit with our customers who, for several months now, have been able to take things further still, thanks to the added option of an IPv4 address.



ARCEP INTRODUCES AN OBLIGATION OF IPv6 COMPATIBILITY FOR FREQUENCY LICENCE-HOLDERS

Arcep introduced an obligation for operators who are awarded a licence to use 5G frequencies in the 3.4 – 3.8GHz band in Metropolitan France to be IPv6 compatible*: "The licence-holder is required to make its mobile network compatible with the IPv6 protocol as of 31 December 2020". As stipulated in its reasons, the goal is to ensure that services are interoperable and to remove obstacles to using services that are only available in IPv6, as the number of devices in use continues to soar, and because the RIPE NCC has run out of IPv4 addresses.

Arcep also proposed an IPv6-compatiblity obligation in its consultation on the award of new frequencies (700 MHz and 3.5 GHz bands) for mobile networks in Reunion and Mayotte.

* Arcep Decision on the terms and conditions for awarding licences to use frequencies in the 3.4 – 3.8 GHz band: https://www.arcep.fr/uploads/tx_gsavis/19-1386.pdf

3. CREATION OF AN IPv6 TASK FORCE GATHERING THE INTERNET ECOSYSTEM

3.1. Launch of the IPv6 task force

Arcep began implementing the first courses of action identified during the workshops devoted to the transition to IP♥6, by creating an IPv6 task force. Operated in partnership with Internet Society France, this task force is open to all of the players in the Internet ecosystem: operators, hosting companies, businesses, public sector players, etc. Its purpose is to accelerate the transition to IPv6 by enabling participants to discuss specific issues and share best practices.

The kick-off meeting held on 15 November 2019 was attended by some 50 stakeholders who took part in multilateral working groups devoted to two topics:

- The first working group focused on the **impacts of the IPv4 address shortage.** The workshops explored alternatives in the case of non-transition to IPv6, technical solutions for making the transition and issues surrounding equipment, software and applications' compatibility with IPv6. The working group was preceded by a keynote from RIPE NCC which provided a regional view of the current exhaustion of IPv4 addresses, and served to underscore how urgent it is to accelerate the transition to IPv6.
- The second working group addressed **IPv6 security issues.** Discussions tackled the topics of securing the local network, anonymisation and privacy issues as well as filtering challenges. A keynote from France's National Cybersecurity Agency, ANSSI, introduced this working group by focusing on the need to rethink security with IPv6.

3.2. The first IPv6 task force meeting findings[15]

The different workshops held as part of the inaugural meeting of the IPv6 task force helped to identify concrete proposals for actions to accelerate the transition, on two different fronts[16]:

1. Impacts of the IPv4 address run-out

Issues	Workstreams
- Need to keep IPv4 for as long as the transition to IPv6 has not been finalised on every link of the Internet's technical chain; - Problems created by alternatives to making the transition (buying or sharing IPv4 addresses); - Existence of various options for making the transition: IPv6 in an IPv4-only network, dual-stack or IPv4 in an IPv6-only network; - IPv6-compatibility issues on certain equipment, applications, software, services, etc.; - Management differences between IPv4 and IPv6, notably in the features deployed and in terms of performance; - Need to increase the Government's role in leading by example in the transition to IPv6.	- Communicate with businesses to encourage them to make the transition to IPv6; - Include IPv6 activation in calls to tender, on top of IPv6 compatibility; - Obtain testimonials from enterprises that have switched from IPv4 to IPv6 (at least in dual-stack) to estimate costs, benefits, technical conditions, etc.; - In addition to these testimonials, draft an in-house development guide for IPv6 deployment; - Identify the different categories of application, equipment and software for which malfunctions caused by Carrier Grade NAT (CGN) have been observed; - Inventory the different categories of application, equipment and software that cause IPv6 compatibility issues.

2. IPv6 security issues and challenges

Issues	Workstreams
- Existence of several IPv6 network security aspects, similar to IPv4's but IPv6 requires a security rethink; - Lack of available skilled labour and poor understanding of existing IPv6 security solutions; - Several standards and RFCs not updated, - Taking anonymisation and privacy protection issues properly into account when implementing IPv6: - Lack of knowledge of IPv6 filtering best practices.	- Inventory updated RFCs[17] and IPv6 security training resources; - Compile the RIPE's existing resources as well as Internet Society initiatives, and update them; - List the privacy issues caused by IPv6 and discuss the different countermeasures; - Issue recommendations on how IPv6 filtering must be performed.

3.3. Task force work follow-ups

The priorities of the actions to be implemented will be set in concert with all of the community of task force participants. The first workstream identified during the inaugural task force meeting is focused on encouraging businesses to make the transition to IPv6. Operating in partnership with Internet Society France, Arcep will convene the task force twice a year, to work together on deepening several of the identified courses of action.

To facilitate communication with the ecosystem, Arcep and Internet Society France are also working on creating an online platform.

People wanting to share their experience or help in the implementation of IPv6 are invited to submit the following form to Arcep, detailing their interest in joining the task force: https://www.arcep.fr/la-regulation/grands-dossiers-Internet-et-numerique/lipv6/suivi-de-la-fin-de-lipv4/appel-a-candidature-task force-ipv6-en-france.html

15. Proceedings of the first meeting of the IPv6 task force: https://en.arcep.fr/news/press-releases/p/n/transition-to-ipv6-1.html
16. This account in no way constitutes an expression of Arcep's position on the relevance, feasibility or priority ranking of the workstreams. Its sole purpose is to describe the information shared by the different IPv6 task force participants. The priorities for the actions to be taken will be set in concert with the community of stakeholders.
17. See lexicon.

OPEN FLOOR TO ...  JEAN-CHARLES BISECCO

*Network architect - **EDF***

THE TRANSITION TO IPv6 AT THE EDF GROUP

If it is very hard to imagine infinity, the opposite is equally true. And it is just as hard to imagine that the private IPv4 addressing system used by a company's internal network is finite. 18 million IP addresses, exhausted.

Many companies have had to grapple with this issue in the past, and they often chose to use public IPv4 addresses that existed on the internet, for their in-house system. A practice that today is reaching its limits, at a time when we are interconnecting with more and more cloud computing providers, going so far as announcing their actual public IP addresses on the internal network, or authorising teleworkers to join SaaS applications directly, without going back through the VPN (split tunnelling). SD-WAN* solutions also enable this type of local breakout on a campus-wide scale. Not to mention the fact that some real time streams like voice calls need to go through a minimum amount of intermediary processing before heading to the cloud.

Faced with this internal addressing issue, we chose to examine the possibility of solving it with IPv6 rather than using workarounds for overlapping IPv4 addresses – based on the fact that the protocol's implementation appeared to be mature, or close to it, for a vast number of solutions. To save time, we nevertheless ratified the in-house use of the 100.64/10 block and its 4 million IPv4 addresses.

The company's entire information system (IS) is reliant on IP, so one needs to be methodical when sequencing dual-stack implementation, and when removing IPv4 addresses from certain portions of the IS.

Our ultimate goal is to get rid of IPv4 on tertiary campus networks that are major IP consumers, and which have the advantage of operating around a relatively homogeneous desktop ecosystem, based on popular market solutions. We can therefore take advantage of a scaling-up factor.

The order of implementation consists of moving through the IS layers from the bottom up: network (backbone, campus and datacentre), then system (OS base) and, finally, applications on both the client and server side (browser, middleware, monolithic applications…).

Few environments have an ecosystem with complete operational qualification, qualification servers are often on production networks in dedicated areas, etc. So impossible to qualify if the underlying production is not ready, etcetera.

Priority for dual-stack implementation must be given to infrastructure services, consumers of bandwidth and real time traffic streams (DNS*, DHCP*, proxy, directory, messaging, telephony/collaboration, NAS*, printing, update deployment…) before tackling business applications.

It is important for deployments to be end-to-end on small-scale testing areas, to be able to gradually qualify each type of element and to capitalise, and so eventually be in a position to industrialise the deployment horizontally by expanding its scope incrementally.

The goal must not, however, be a complete transition to dual-stack, beyond the campuses and infrastructure services. Our strategy is to achieve a gradual transition to dual-stack for front-end applications. So no immediate need to migrate backends, especially as they are extremely numerous and heterogeneous.

We will be using DNS64/NAT64 translation at the datacentre entry point, enabling IPv6 clients to reach IPv4 applications. Another major prerequisite when removing IPv4 is to ensure that all users are able to make phone calls over IPv6, which means it must be deployed across entire campuses before beginning to phase out IPv4.

There is very little feedback on the transition to be had, aside from companies for whom IT is their core business, and it is extremely difficult to estimate the added cost of operating in dual-stack, on top of the many possible repercussions that cannot be identified beforehand. Relaying traffic in IPv6 is one thing, adapting the entire ecosystem upstream and downstream is quite another. Merely adapting the SIEM* that correlates the company's logs will be a challenge, and this was probably one of the easiest points to identify.

Lastly, one of the project's aims is of course to provide dual-stack public websites. Companies will need to work on migrating streams between Wi-Fi base stations and the IPv6 controller, and to provide dual-stack on their guest network to master the learning curve – and so be ready for the likely explosion in addressing needs in the coming years, driven by microservices/containers and the Internet of Things.

* See lexicon.

TUTORIAL

IPv6-ONLY ACCESS AND THE NAT64/DNS64 MECHANISM

Some operators provide their customers with Internet access using IPv6, without offering IPv4 access. This is especially true today on mobile networks, where most of the solutions providing IPv6 connectivity are IPv6-only.

How to access IPv4-only resources on the Net without IPv4?

Because a substantial portion of today's Internet remains accessible only in IPv4, the solution used for more than 99% of IPv4-only traffic is NAT64/DNS64. The DNS resolver will not return an IPv4 address for websites in IPv4, but rather a special IPv6 address: an IPv6 address that points to an NAT64 platform, placed on the operator's network. The NAT64 platform creates the ability to communicate the customer's IPv6 network stack with the IPv4 Internet. The platform will perform network address translation (NAT) in the usual way, except that the private IPv4 address is replaced by an IPv6 one. The NAT64 platform recovers the encoded destination IPv4 address in IPv6: to route the traffic over an IPv6-only connection, the NAT64 platform generates an IPv6 address that is built using the reserved 64:ff9b::/96 prefix, followed by the 32 bits of the IPv4 address.

A dedicated DNS resolver, such as DNS64, is required to be able to use the NAT64 platform. If you are unable to configure the DNS64 supplied by your operator, there are two public DNS64 services hosted in France: Cloudflare DNS[1] and Google Public DNS[2].

Below are some illustrations of a DNS64 resolver's behaviour:

Type of site	Domain name	Classic DNS resolver[3]	DNS64 resolver
Dual-stack	www.orange.fr	2a01:c9c0:a3:8::70 193.252.148.70	2a01:c9c0:a3:8::70 193.252.148.70
IPv4 only	www.sfr.fr	80.125.163.172	64:ff9b::507d:a3ac 80.125.163.172
IPv4 only	www.bouyguestelecom.fr	23.38.100.155	64:ff9b::1726:649b 23.38.100.155
Dual-stack	www.free.fr	2a01:e0c:1::1 212.27.48.10	2a01:e0c:1::1 212.27.48.10
IPv4 only	www.ovh.com	198.27.92.1	64:ff9b::c61b:5c01 198.27.92.1
IPv4 only	www.ionos.fr	217.160.86.38	64:ff9b::d9a0:5626 217.160.86.38
IPv4 only	www.gandi.net	151.101.1.103	64:ff9b::9765:167 151.101.1.103
IPv4 only	www.scaleway.com	212.47.255.70	64:ff9b::d42f:e146 212.47.255.70

How to access an IPv4 literal address which, by definition, does not use a DNS resolver ?

This is a rare instance on the Internet, but some services use IPv4 literal addresses (e.g.: http://46.227.16.8/) even though the best practice is to systematically use domain names. In these cases, the DNS64 will be of no use as no DNS resolution is performed. To prevent regressions, mechanisms such as 464XLAT (RFC 6877[4]) and/or CLAT have been incorporated into operating systems (Android since Android 4.3, iOS since iOS 12.0, Windows10 since 2017, Linux using Clatd[5]) so that applications, in appearance, have a functional IPv4 address, even though the host only has IPv6 addresses.

1. DNS64 Cloudflare DNS: 2606:4700:4700::64 and 2606:4700:4700::6400
2. DNS64 Google Public DNS: 2001:4860:4860::6464 and 2001:4860:4860::64
3. Only the first IPv4 and the first IPv6 addresses returned were kept. These DNS resolutions are those observed on 14 April 2020 and may have been altered since.
4. RFC 6877: *464XLAT Combination of Stateful and Stateless Translation* https://tools.ietf.org/html/rfc6877
5. Clatd, a 464XLAT CLAT implementation for Linux: https://github.com/toreanderson/clatd

PART 2

Ensuring internet openness

CHAPTER 4

Guaranteeing net neutrality

CHAPTER 5

Devices and platforms, two structural links in the Internet access chain

CHAPTER 4

Guaranteeing net neutrality

HIGHLIGHTS

450 million European citizens are protected by the European Open Internet regulation adopted in 2015 and the guidelines on the Implementation of the Open Internet regulation.

18 months of work were needed for European regulatory authorities to revise the Open Internet regulation guidelines, which were published on June 16th, 2020.

In France, Arcep has equipped itself with several tools to ensure compliance with net neutrality: the Wehe app has been used more than **115,000 times** and **146 user reports** were filed via the "J'alerte l'Arcep" platform.

The European legislator has been protecting net neutrality since 2016, recognising the following points in particular in its Open Internet[1] Regulation:

- users' right *"to access and distribute information and content, use and provide applications and services, and use terminal equipment of their choice, irrespective of the end-user's or provider's location or the location, origin or destination of the information, content, application or service, via their Internet access service"*;
- and Internet service providers' duty to *"all traffic equally, when providing Internet access services, without discrimination, restriction or interference, and irrespective of the sender and receiver, the content accessed or distributed, the applications or services used or provided, or the terminal equipment used"*.

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

1. NET NEUTRALITY OUTSIDE OF FRANCE

The European regulation guarantees open Internet access to more than 450 million European citizens living in the 27 EU Member States. The United Kingdom's withdrawal from the European Union could alter the situation for 66 million UK citizens. The UK government adopted the *Open Internet Access (Amendment etc.) EU Exit Regulations 2018* which ensures that net neutrality will continue to be upheld, but only until the Brexit process is complete, i.e. 31 December 2020.

Net neutrality is progressing in a number of countries. In India, the Telecom Regulatory Authority of India (TRAI) adopted a series of recommendations in November 2017 designed to strengthen net neutrality. Since July 2019, these recommendations have been prerequisites for telecom operators' ability to obtain and keep their operator's licences. In a similar vein, the Korea Communications Commission (KCC) in South Korea has been requiring operators' compliance with net neutrality guidelines since 2011. Other countries are also poised to incorporate or further strengthen net neutrality provisions in their legal corpus. Prime examples include the upcoming adoption of a net neutrality law in Switzerland, and the drafting of net neutrality guidelines in Mexico.

1. Regulation (EU) 2015/2120 of the European Parliament and Council of 25 November 2015 laying down measures concerning open Internet access: https://www.arcep.fr/fileadmin/reprise/textes/communautaires/reglement-UE-2015_310-Net-Neutralite-251115.pdf

OPEN FLOOR TO ...

DAVE CHOFFNES

*Associate Professor - **Northeastern University***

NET NEUTRALITY IN THE UNITED STATES AT FEDERAL AND STATE LEVELS

In 2017, the U.S. Federal Communication Commission (FCC) relinquished all regulatory controls, including enforcement, of Internet providers in the entire country. With this order, the FCC essentially killed net neutrality protections in the U.S., permitting Internet providers to block and shape Internet traffic at their discretion, and force content providers to pay for prioritization.

While the order consisted mainly of stating what the FCC would no longer enforce, it did put in place two important requirements: Internet providers must be transparent about their net neutrality violations and no state in the U.S. can pass any regulations enforcing net neutrality at the state level. There are no reports of any auditing or enforcement of the transparency requirement. In a recent US Federal Court of Appeals case, the court threw out the exemption rule, meaning that states can indeed enact net neutrality legislation.

Despite the exemption rule being overturned, there is currently no enforcement of net neutrality laws anywhere in the U.S., and violations of net neutrality principles abound. Through our Wehe project, we found that nearly every cellular provider throttles video streaming applications to low quality resolutions. The way they single out video streaming often leads to uneven treatment for different video providers. Further, this treatment changes over time, can cause significant network inefficiency, and is applied 24/7 (not in response to network overload).

There is still hope for net neutrality laws at the state level, especially after the recent court ruling voiding preemption. However, legislatures have been slow to act on such laws --- including my home state of Massachusetts --- despite proposed legislation and overwhelming support among the public. Perhaps the best shot at net neutrality enforcement in the U.S. is the November 2020 elections, with the potential for new politicians to enact permanent net neutrality laws.

JINNY KWAK

*Chief Director of the CCDI - **KCC***

THE ISSUES OF NETWORK NEUTRALITY IN THE 5G ERA OF KOREA

Korea's net neutrality principles were established with the creation of the "net neutrality Guidelines" in 2011 and the "reasonable traffic management standards" in 2013. They prohibit blocking and unfair discrimination, and call for transparency in traffic management. The 2016 amendment to the Enforcement Decree of the Telecommunications Business Act and a notification of 2017 prohibited unfair or discriminative conditions on CPs, which clarified the basis for ex post regulation.

Ahead of the 5G launch, the Korea Communications Commission (KCC) formed a 48 member-Committee on the Coexistence and Development of the Internet (CCDI) in 2018 and began discussions on need to revise the net neutrality principles, anticipating traffic management through 5G network slicing technology.

Discussions were divided into three views: the first was that the existing net neutrality principles could be applied flexibly to 5G technology. This view considers later including health and safety services which require ultra-low latency, such as telemedicine and self-driving cars, in managed services (called "specialized service" in Europe).

The second was that the existing regulations should be strengthened. This was a view held by many CPs who pointed out the concern that if net neutrality principles are relaxed, only large CPs would survive, and the dominance of telcos could extend into the contents market. They argued that traffic management standards should be strengthened.

The third was that the net neutrality principles should be abolished except for the transparency principle. This view was shared mostly by telcos, who supported it to introduce innovative services and have large CPs share a reasonable financial burden for vast amounts of traffic.

Following 5G commercialization in April 2019, telcos have been providing B2C contents like augmented reality and virtual reality. The KCC will continue to monitor 5G services development, and cooperate with the Ministry of Science and Information and Communication Technologies as to whether net neutrality principles need to change.

OPEN FLOOR TO ...

ROBERT WELLS

*Principal Legal Adviser - **Ofcom**[1]*

NET NEUTRALITY IN THE UK IN THE CONTEXT OF BREXIT

Although the UK left the EU at the end of January, the rules on net neutrality remain the same as those in the EU, as EU law continues to apply in the UK during the transition period (until 31 December 2020). At the end of that period, the EU Regulation containing the rules on net neutrality will be converted into domestic UK law with those rules subject to only very minor changes, such as deleting references to EU laws and institutions or replacing them with their national equivalents. The basic structure of the law will remain the same, setting out the rights of end-users, restrictions on traffic management measures and the circumstances under which specialised services can be provided.

From 2021 onwards, and subject to the negotiations over the future economic relationship between the UK and EU, the UK Parliament could choose to amend or replace the law, but we are not currently aware of any such plans. Still, Ofcom, like all national regulators, continues to consider how technological changes might impact on the functioning of the existing net neutrality rules, and whether these might need to be reviewed in future. We plan to continue to exchange ideas with our European counterparts to help inform our collective thinking on the subject.

In the meantime, Ofcom remains active in monitoring compliance with the current rules. In the last couple of years, we have reviewed a number of zero-rated products and have taken enforcement action against certain traffic management practices. On the whole, the zero-rated products that we have seen in the UK market to date have not raised significant concerns. And following our enforcement programme, now that all operators are complying with the traffic management rules, we expect to spend less time on enforcement activities and more time thinking about policy issues such as the interaction between the net neutrality rules and new and evolving technologies, in particular 5G, network slicing and mobile edge computing.

1. Office of communications: UK's communications regulator.

SIDHARTH DEB

Policy & Parliamentary Counsel

APAR GUPTA

*Executive Director - **Internet Freedom Foundation***

DEMOCRATISING NET NEUTRALITY IN INDIA

After years of public advocacy led by a movement of more than a million people, in July 2018, India's Department of Telecom amended licenses for internet providers. It mandates ISPs to adhere to technical aspects of the net neutrality principle. In conjunction with a February 2016 regulation[1], which prohibited "zero rated" services, It was a victory for internet health in India.

Without enforcement however, victories can hollow out. Months after the amendment we learnt ISPs were freely discriminating against traffic. Why? Information asymmetries stymie accountability. A crowd-sourced reporting mechanism, which was hosted on SaveTheInternet.in[2], allowed us to forward 307 complaints to relevant authorities between January and May 2019[3]. In January 2020, the Telecom Regulatory Authority of India (TRAI) started a public consultation on issues like reasonable TMPs and mechanisms to monitor and detect violations.

Unfortunately many industry representatives evangelise class-based TMPs and propose revisiting net neutrality to accommodate innovation 5G networks, in particular network slicing and network functions virtualization. Worryingly, they request TRAI shun user-facing detection tools due to concerns like uneven end user environments.

We oppose this since net neutrality must be individual centric. For this, reasonable TMPs should be "as application agnostic as possible"[4]. Further, authorities should view net neutrality as a mechanism for orderly development of technologies like 5G.

Critically, regulators must chip away at asymmetries. A prerequisite towards this is a diagnostic tool. In this regard TRAI may benefit from engaging with counterparts like BEREC and ARCEP. A mobile application like Wehe could be useful in India because the Internet is mostly developing through the mobile network. In this context, Indian authorities must assume leadership one again and build tools to hold ISPs accountable.

1. *Prohibition of Discriminatory Tariffs for Data Services Regulations*, 2016
2. https://savetheinternet.in
3. https://internetfreedom.in/net-neutrality-in-india-needs-to-find-its-bearings
4. See publications of Pr. VAN SCHEWICK

Moving in the opposite direction, the Federal Communications Commission (FCC) in the US reversed course on existing regulations in December 2017, by adopting a text called *"Restoring Internet freedom"*. Coming into effect in June 2018, this decree overturns the central provisions of the *Open Internet Order* of 2015, which prohibited Internet service providers (ISPs) from blocking or throttling traffic, or charging to prioritise it. Several states reacted against this new order – the most vocal of which included California and Washington State – by reintroducing net neutrality locally, going against the FCC decision and so exposing themselves to legal proceedings. In October 2019 and in February 2020, the Federal Court of Appeal upheld the FCC's decision, while also giving States the freedom to adopt their own net neutrality rules.

Moreover, freedom of access to the Internet continues to be threatened in a number of countries. In Russia for instance, even though net neutrality has been protected by law since 2016, access to vast swaths of the Internet is occasionally blocked. This is also true in China where Internet access is filtered through the *"Great Firewall of China"* and repurposed by the *"Great Cannon of China"* – which *de facto* undermines the principle of having neutral access to content and applications. Net neutrality could also be threatened by local Internet networks being cut off from the global Internet, and so depriving end users from having complete access to the Web, as was the case in Russia last December. It could also suffer from partial or complete shutdowns which are becoming an increasingly common measure taken by national and local authorities. There was a sharp rise in the number of shutdowns [2] in India in 2019, for instance, even though the Supreme Court of India issued an order regarding these practices, and despite net neutrality being protected in that country.

5G AND NET NEUTRALITY: PROMOTING INNOVATION WHILE PRESERVING NET NEUTRALITY

5G technology promises to usher in new services thanks to substantially increased capacities, notably in terms of speed, latency, virtualisation, quality of service levels and reliability. Some of the sector's players still have concerns over whether 5G technology is compatible with net neutrality. But are those concerns justified?

In an opinion published in December 2018, BEREC offered a reminder that the Open Internet regulation and its guidelines are technologically neutral, and so pose no major obstacle to 5G technology, and apply as they do to earlier 2G, 3G and 4G technologies. The existing legal framework thus offers substantial leeway to deploy the innovations being promised by 5G, such as network slicing, different levels of quality of service or mobile edge computing.

To debunk conventional assumptions, Arcep summarised the different sides of the debate in an *ad hoc* document*, published on its website. Arcep will continue to keep a close watch over the development of 5G use cases, and to listen to players' queries regarding these use cases' compatibility with the net neutrality principle.

* https://www.arcep.fr/uploads/tx_gspublication/ARCEP_BD_5G_planche_ENG-2019.pdf

2. See lexicon.

OPEN FLOOR TO ... FELICIA ANTHONIO

*Coordinatrice de la campagne #KeepItOn - **Access Now***

INTERNET SHUTDOWNS: THE NEW GLOBAL NORM

The internet is indispensable in our everyday life: it enables rights and boosts economies. Despite this, governments across the world are shutting down the internet. Access Now, in collaboration with the #KeepItOn coalition, has been fighting against internet shutdowns since 2011.

In 2016, there were at least 75 internet shutdowns documented[1]. Fast forward to 2019; this number has tripled with at least 213 cases[2]. Between 2016-2019, through the Shutdown Tracker Optimization Project[3], the coalition documented more than 590 network disruptions. The trend shows authorities are disrupting communications during important national events, elections, protests, or crises. Shutdowns are lasting longer, affecting more people, and targeting vulnerable groups.

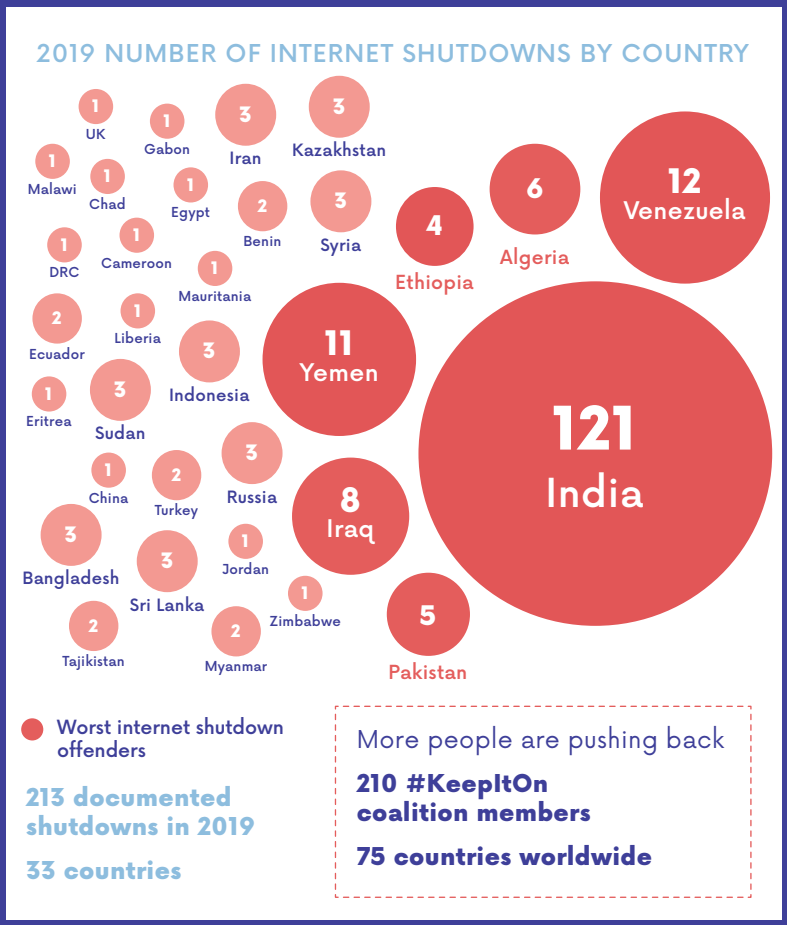
This practice violates fundamental human rights, disrupts press freedom and the free flow of information, and threatens economies. Governments justify this blatant repression by citing the need to fight "fake news", guarantee national security and public safety, or prevent cheating during exams. However, in reality, during shutdowns, netizens are unable to access information or freely express themselves, and are left with confusion and panic, while small and large businesses lose revenues, and at times, close shop.

What can service providers do?

As the implementers of government-ordered shutdowns, Internet Service Providers (ISPs) are at the center of this crisis[4]. Yet ISPs can push back, by insisting orders come in writing, from an identified official, under proper and specific legal authority. They should inform affected customers about scope, scale, duration, and reasons for the disruption.

Operators should collaborate with businesses, diplomats, and civil society to dissuade governments from ordering disruptions and end them as soon as possible. Advocates, journalists, and activists across civil society can speak publicly when ISPs may not. ISPs should join advocates who are taking governments to court to challenge these arbitrary and overbroad measures, which harm business interests and human rights.

1. https://accessnow.org/kio-2018-report
2. https://www.accessnow.org/keepiton-2019-report
3. https://www.accessnow.org/keepiton
4. https://accessnow.org/telco-action-plan



2. ARCEP'S INVOLVEMENT IN EUROPEAN WORKS

Following through on the evaluation made in 2018, Arcep and its European counterparts in BEREC devoted themselves in 2019 to clarifying the guidelines for applying the Open Internet regulation. Based on the evaluation made by BEREC in late 2018[3], the main focus of these revisions is to reduce the risk of having disparate interpretations of these texts amongst players involved the Internet's operation in France and Europe. A first version of the revised guidelines was produced after active cooperation between the national regulatory authorities (NRAs), and published for public consultation in October 2019. After having received contributions from various stakeholders – telecom operators, equipment suppliers, associations, academia and members of civil society – the revised guidelines were finalised, and were published on June 16th, 2020. They will keep the same structure as the previous guidelines, which themselves are based on that of the Open Internet regulation. The clarifications that have been brought, of which the main ones are summarised below, reflect the joint conclusions reached by European regulators.

Zero-rating refers to offers that allow subscribers to use one or more particular online services without the traffic being counted against their data allowance. These practices are not prohibited *per se* by the European regulation but they can lead to discriminatory behaviour that benefits some applications or categories of application. Using an application without having to pay for it creates an economic incentive to use it, which could eventually undermine end users' freedom of choice. The revised guidelines therefore specify the criteria for evaluating these zero-rating offers – and particularly whether a zero-rating programme is open or closed to new applications – and lists these criteria in an assessment methodology that is made available to NRAs.

The revised guidelines specify the conditions under which ISPs can create different classes of service for Internet access, and so be able to design dedicated plans, in particular for business customers. ISP marketing practices are limited by safeguards to help NRA ensure that neither the overall quality of Internet access services nor end users' rights are limited. This in turn makes it possible to continue to foster innovation while limiting the risks of creating a two-speed Internet.

The work also checked whether the criteria used to define a "specialised service"[4] fit the upcoming development of the Internet of Things (IoT) and machine-to-machine (M2M) services. These services have special requirements, notably in terms of reliability, security and energy constraints which cannot be satisfied by ordinary Internet access services. To meet these expectations, the revised guidelines clarify the notion of "specific level of quality," which is essential to the definition of specialised services, and incorporate new assessment criteria in addition to latency, jitter and packet loss. ISPs' capacity to demonstrate the need to for such a specific level of quality will determine whether these services are introduced.

REGULATORY FRAMEWORK GOVERNING NET NEUTRALITY

NOVEMBER 2015
Regulation EU 2015/2010 of the European Parliament and Council laying down measures concerning open Internet access

JUNE 2016
Public Consultation on the draft BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality rules

AUGUST 2016
BEREC Report on the outcome of the public consultation on draft BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality rules BoR (16) 128

AUGUST 2016
Adoption of BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules BoR (16) 127

MARCH 2018
BEREC Consultation Paper on the evaluation of the application of Regulation (EU) 2015/2120 and the BEREC Net Neutrality Guidelines BoR (18) 33

DECEMBER 2018
BEREC Opinion to the European Commission for the evaluation of the application of Regulation (EU) 2015/2120 and the BEREC Net Neutrality Guidelines BoR (18) 244

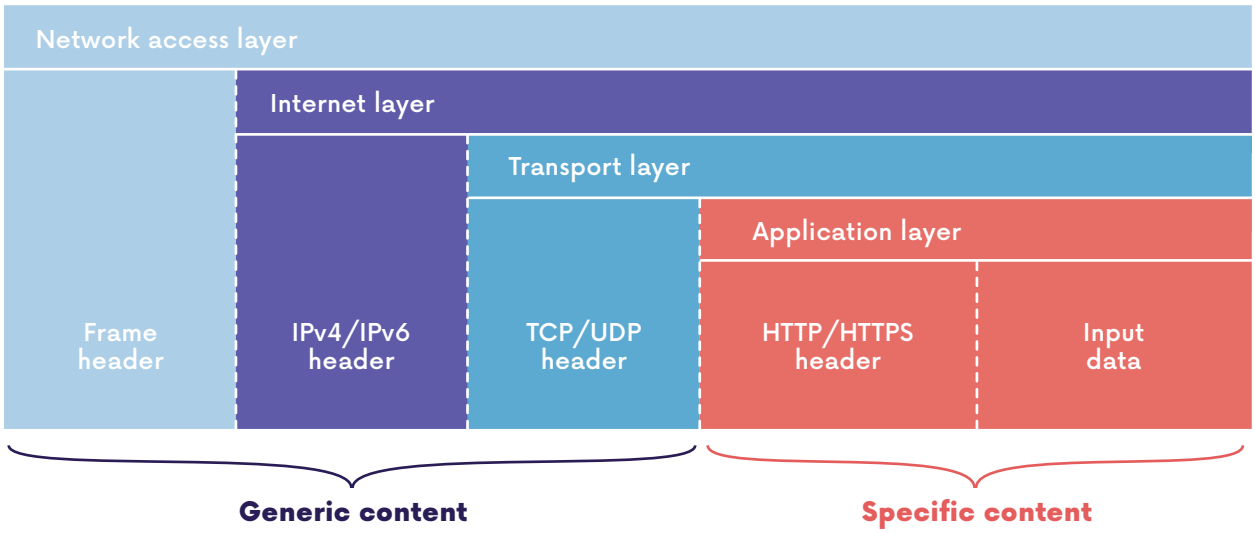
OCTOBER 2019
Public Consultation on the draft BEREC Guidelines on the Implementation of the Open Internet Regulation BoR (19)180

JUNE 2020
BEREC Report on the outcome of the public consultation on the draft BEREC Guidelines on the Implementation of the Open Internet Regulation BoR (20) 111

JUNE 2020
Adoption of the revised BEREC Guidelines on the Implementation of the Open Internet Regulation BoR (20) 112

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

EXAMPLE OF A SIMPLIFIED DIAGRAM OF THE GENERIC AND SPECIFIC CONTENTS OF ELECTRONIC COMMUNICATIONS DATA



Source: Arcep

The process of revising the guidelines also provided Arcep and its European counterparts with an opportunity to discuss the various practices that could affect the neutrality of Internet access services. NRAs thus examined the advent of new additional services (such as parental control or content filtering services) that ISPs offer alongside an Internet access service. From a broader perspective, NRAs also discussed the rules on how traffic management measures are implemented in an ISP's network. The revised guidelines specify the scope of NRAs' ability to monitor all of these issues, when these practices pose a threat to the neutrality of Internet access services.

The topic of ISPs' access to domain names (or URLs) for traffic management or billing purposes was also addressed[5]. The Open Internet regulation allows ISPs only to access the information contained in an IP packet header and in the transport layer protocol's header (e.g. TCP or UDP header) whose domain names and URL are excluded. In a public statement[6], the European Data Protection Board (EDPB[7]) – whose opinion was also solicited – specifies that the domain name and URL can be qualified as personal data and, as such, are protected by the provisions of the Privacy and Electronic Communications (ePrivacy) Directive[8] and the General Data Protection Regulation (GDPR)[9]. ISPs that use the domain name or URLs to identify traffic or for billing purposes would therefore expose themselves not only to a potential violation of the Open Internet regulation, but also a possible violation of their customers' privacy protection.

Lastly, guidelines on common approaches to identification of the network termination point[10] do have an impact on the scope of the protection afforded to end users by the Open Internet regulation. These new guidelines were designed to guide NRAs in the choice of where to locate the termination point, by taking into account the degree to which operators' boxes and their Internet access plans are technically complementary. The network termination point must thus enable a good balance between the networks' smooth operation and users' freedom to choose their device. Discussions surrounding this issue provided Arcep with an opportunity to recall the need to extend the principle of neutrality to devices, to strengthen end users' freedom in the choice and use of their device.

5. The implied issue here being ISPs' ability to access domain names and URLs as part of business practices authorised by Art. 3.2 of the Open Internet regulation
6. EDPB letter of 3 December 2019 regarding BEREC's request for guidance on the revision of its net neutrality guidelines (Ref.OUT2019-0055): https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out2019-0055_berecnetneutrality2.pdf
7. See lexicon.
8. Directive 2002/58/EC of the European Parliament and Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
9. Regulation (EU) 2016/679 of the European Parliament and Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
10. BEREC Guidelines on Common Approaches to the Identification of the Network Termination Point in Different Network Topologies, BoR (20)46: https://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/9033-berec-guidelines-on-common-approaches-to_0.pdf ; See lexicon.

OPEN FLOOR TO ... CLÉMENCE SCOTTEZ

*Head of the Department of Economic Affairs - **CNIL***

ISPS' DATA PROTECTION AND ANALYSIS OF ELECTRONIC COMMUNICATIONS

Net neutrality and data protection serve a common societal purpose. It provides citizens with a framework that enables them to express themselves freely online, without fear of discrimination or having their electronic communications spied upon by the operator that provides them with an access to these services.

It is in this spirit that Directive 2002/58/EC, commonly known as the *Privacy and Electronic Communication or ePrivacy Directive*, completes and clarifies the general framework laid out by the General Data Protection Regulation (GDPR). It states that electronic communications data contain highly sensitive information, *"allowing precise conclusions to be drawn regarding the private lives of the persons involved in the electronic communication"*[1]. From this conclusion, it establishes a general principle of prohibiting the interception, storage or monitoring of these data, with very narrow exceptions, and circumscribes the role of operator to relaying communications over the networks.

More specifically, the Directive authorises operators to process data only to guarantee the security of their services (Art. 4), to transmit the communication (Art. 5.1) or, regarding data traffic, to charge clients for their services (Art. 6). Any other operator process that does not meet these specific purposes requires them to obtain the consent of the relevant users, pursuant to Articles 5 and 6 of the above-cited Directive. Let us recall that this consent must meet the criteria set out in the GDPR, under Article 2(f); the user's consent must therefore be specific, based on clear information about the end purpose and non-prejudicial (e.g. it cannot be a condition of the conclusion of Internet access service contact). From a more general perspective, data processing must comply with the principles of transparency, fairness (users must be informed of the nature of the process, its goal, etc.), must be limited to the purpose indicated to the user, and must only use the necessary data to achieve this purpose.

On the basis of these principles, notably that of "minimisation", the European Data Protection Board (EDPB) answered BEREC's queries on the data protection issues raised by Regulation 2015/2120, in particular regarding zero-rating mechanisms. The EDPB thus underscores that the notion of *"specific content"* – whose monitoring by operators is prohibited by Article 3(3) of Regulation 2015/2120 – can be assimilated to the notion of *"communication"*, defined by the ePrivacy Directive (Art. 2) as *"any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service"*. Here, the EDPB reminds us that URLs and domain names are not *"traffic-related data"* inasmuch as they are not necessary to deliver an electronic communication on a communications network. However, they are falling within the definition of "communication" data, i.e. information that displays the content exchanged or consulted by users. Processing this information for billing purposes, as part of zero-rating schemes, therefore requires ISPs to obtain the consent of all of the users who will have the content of their communications inspected (e.g. the sender and recipient of an e-mail).

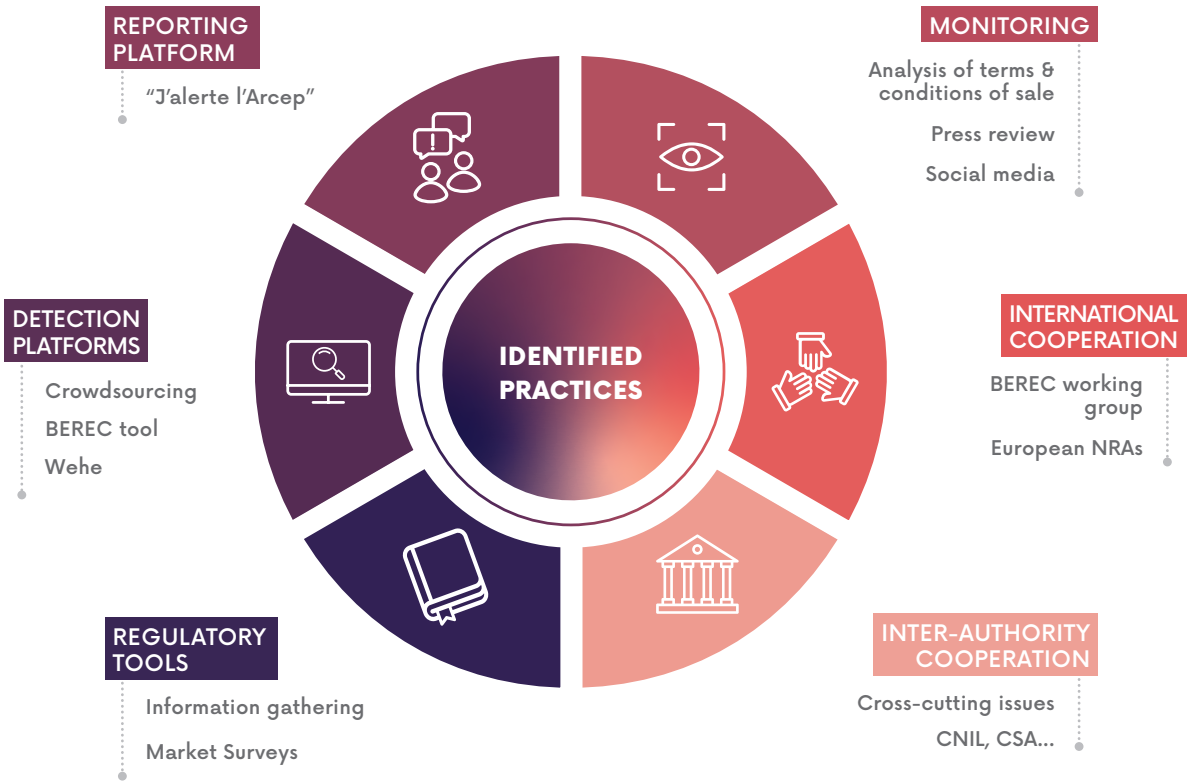
From a broader perspective, the EDPB points out that mechanisms which consist of processing domain names or URLs are tantamount to a form of network monitoring that could violate users' fundamental privacy and data protection rights, as enshrined by Articles 7 and 8 of the EU's Charter of Fundamental Rights. In addition to obtaining consent from the concerned users, the EDPB therefore encourages operators to employ less intrusive traffic management techniques, and to work together on developing standardised and interoperable techniques that are more mindful of users' personal data.

1. Recital 2 of the proposed regulation

3. DEVELOPING ARCEP'S TOOLKIT

To uphold net neutrality, Arcep has equipped itself with a toolkit that enables it to have a complete overview of market practices with respect to the Open Internet regulation's four cornerstones: business practices, traffic management, specialised services and transparency obligations.

ARCEP'S NET NEUTRALITY TOOLKIT



Source: Arcep

As part of the Authority's monitoring responsibilities, Arcep departments verify ISPs' terms and conditions of sale on a regular basis. This enables them to detect any provisions in those terms and conditions that are incompatible with net neutrality. In 2019, this monitoring work covered all of ISPs' Internet access plans, notably those sold by French overseas department operators and by companies operating in sectors other than electronic communications (cf. next section).

Arcep also has regulatory tools that enable it to gather information from ISPs on their network management rules.

In late 2017, the "J'alerte l'Arcep" reporting platform was added to the Authority's toolkit. Thanks to this platform, end users can inform Arcep about any problematic situation. Over the last year, 146 net neutrality-related reports were filed on the "J'alerte l'Arcep" website. These end-user reports in turn enabled Arcep to identify possible net neutrality infractions rapidly, and to encourage a swift resolution of the problems, which are detailed in the next section.

Arcep also maintains an ongoing dialogue with its European counterparts about the various issues encountered at the national level. This enhanced cooperation between NRAs has helped Arcep project itself into a wide range of concrete situations, question existing regulations ability to address new technologies and uses, and better understand national situations similar to those described by its fellow NRAs. Once again, the past year was punctuated by queries over zero-rating offers' compatibility with the Open Internet regulation, as the various questions for preliminary ruling brought before the Court of Justice of the European Union (CJEU) testify.

In 2019, Arcep also expanded its dialogue with other regulatory authorities in France, and particularly the National Commission on Informatics and Liberty (CNIL) regarding the scope of transport data that ISPs are allowed to access. This inter-authority cooperation creates the ability to combine each one's respective competencies to achieve a deeper regulatory analysis of common and cross-cutting issues.

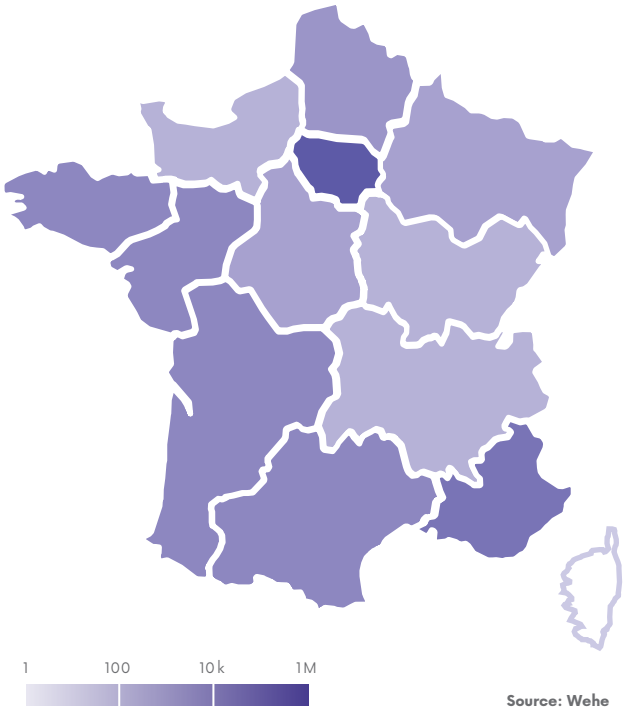
Lastly, Arcep has made a detection tool called Wehe available to the general public since November 2018. Wehe is an open source testing tool developed by Northeastern University that compares the time it takes for traffic generated by certain services to be relayed. The test is carried out in two stages. First, the tool simulates the use of a service in an ISP's network, to measure how that ISP processes actual traffic from this service. Next, the tool once again simulates this same traffic, but this time replaces the content with encrypted content that is invisible to the ISP. When there is a difference in how the two streams are treated, it

is possible to suspect that the operator has implemented traffic management measures. End users have employed Wehe close to 115,000 times since it launched and, to date, no differentiation has been detected by the application.

Available for Android and iOS, the tool is available in French to ensure that it can be accessed by as many French end-users as possible. The applications that are tested do not, however, necessarily reflect the most widely used services in France. Thanks to the partnership with Northeastern University, the list of the services tested was recently updated, to match those that are the most popular in France.

Following through on the preliminary work done in 2018, Arcep wanted the Wehe tool to be given an additional feature: the ability to detect port blocking practices. Access to certain online services or applications is obtained through a specific port[11], so any blocking, throttling or priority measures applied to that port could affect end users' ability to access that service. The test, which is still in the development phase, would enable end users to verify several of the most commonly used ports. If a malfunction is detected, end users are invited to report any issues via the new "J'alerte l'Arcep" platform, so that Arcep can examine potential incompatibilities with the Open Internet regulation on a case by case basis.

LOCATION OF WEHE TESTS PERFORMED IN FRANCE - 2019



Source: Wehe

REPLAYS TESTED BY WEHE

Source: Arcep

11. See lexicon.

FIRST QUESTIONS FOR PRELIMINARY RULING PUT TO THE COURT OF JUSTICE OF THE EUROPEAN UNION

In 2019, the Court of Justice of the European Union (CJEU) has been asked several questions for preliminary rulings on the implementing measures for the provisions of the Open Internet regulation.

In late 2018 and early 2019, the Budapest High Court questioned the CJEU on national operator Telenor's zero-rating offers for preliminary ruling (Joined Cases C-807/18 and C-39/19). The Hungarian operator sells mobile plans whereby access to certain online services is not deducted from customers' contractually-stipulated data allowance, and their connection to these services is not throttled or blocked once the data cap has been reached, unlike other online services.

Another request for preliminary ruling was brought before the CJEU in November 2019, filed by the Administrative Court of Cologne, Germany, regarding the management of zero-rating offers when roaming by the German operator Vodafone (Case C-854/19). Vodafone sells passes that keep specific services from being counted against customers' monthly data allowance. When these customers are travelling outside of Germany, however, this policy no longer applies, and traffic from the services that are normally not deducted from their contractually stipulated data allowance is deducted.

These questions for preliminary ruling are scheduled for an initial review by the Court of Justice of the European Union (CJEU) in 2020, which will provide a supplementary analysis grid to the one detailed in the revised guidelines.

4. INVENTORY OF OBSERVED PRACTICES

As a follow-up to the work performed in 2018, Arcep has addressed the issue of port blocking. Online services and applications are accessed through a port which, if blocked, prevents users from accessing the service. Arcep therefore examined the various instances reported by end users via the "J'alerte l'Arcep" platform. The first reports pertained to a mobile operator's blocking of HTTPS traffic on a specific port, which in turn prevented users from accessing some services. Arcep reported these issues that end users encountered to the operator involved, which agreed to install a mechanism that would protect end users' freedom of choice.

To keep end users informed, Arcep has made a script available that enables them to check whether a TCP port's output is operational, blocked or available but throttled. This mechanism will be further improved by the upcoming launch of a new port prioritisation test in the Wehe tool, described above.

In 2019, the competent Arcep body investigated whether the in-flight Wi-Fi services that airlines offer are compatible with net neutrality. Because an in-flight Wi-Fi service is transnational by nature, the issue was also addressed in BEREC's net neutrality expert working group. They confirmed that this type of service can be defined as being publicly available, and thus de facto subject to the provisions of Europe's Open Internet regulation, in the same way as those supplied by traditional ISPs. Placed under the heading of proactive dialogue, Arcep's action gave airlines an opportunity to take better account of the provisions of the Open Internet regulation when deploying their in-flight Internet access services. As a result, Air France adapted its offers to make them as neutral as possible, given the singular technical constraints of in-flight Internet services.

The competent Arcep body also focused its attention on Wi-Fi offers on trains. Offered to passengers, these Internet access plans, which are also considered to be publicly available, are subject to the provisions of the Open Internet regulation. In Q4 2019, Arcep thus queried national railway company, SNCF, to obtain additional information on its Internet access offer's compatibility with net neutrality and on the information provided to end users. Arcep's investigations on these products are ongoing, and Arcep is relying on SNCF to take appropriate measures to ensure that Wi-Fi services offered to railway passengers comply with net neutrality.

Arcep also paid close attention to the reports it received from end users regarding possible violations of net neutrality, via the "J'alerte l'Arcep" platform in particular. These reports led Arcep to examine the compliance of different Internet access services, e.g. recently, those offered in hospitals. These end-user reports also enabled Arcep to promptly solve issues encountered by users of a small operator's network when attempting to access certain websites (including "J'alerte l'Arcep" itself).

Lastly, Arcep worked to evaluate whether all of Internet access plans sold in French overseas markets were compatible with net neutrality. In early 2020, Arcep contacted operators in the French overseas departments and territories to establish a status report on this topic, and to invite operators to engage in a proactive dialogue with Arcep departments.

NET NEUTRALITY AND PMR SERVICES PROVIDED ON A CONSUMER 4G NETWORK

Historically, Professional Mobile Radiocommunication (PMR) networks are private, secured radiocommunication networks used chiefly for calling and short messaging services. They are designed for companies that require high availability, confidentiality or specific area coverage.

These networks long relied on specific technologies (such as TETRA) to function, but companies have been gradually urged to migrate to upgraded solutions. Two potentially complementary approaches are being considered to satisfy new expected uses: either a PMR network is deployed on an ad-hoc 4G infrastructure that is entirely separate from the 4G network used by consumers, or a PMR network is deployed within the same 4G infrastructure used by consumers. The first solution gives the user freedom in how its PMR network is deployed, but has the drawback of higher operating costs. The second solution creates the ability to share operating costs, but may also require that PMR service occasionally preempts other services being operated simultaneously on the shared 4G operators' network.

Introducing this pre-emption for PMR services on a consumer 4G operator' network is tantamount to prioritising these services over the network's general operation, including Internet access services. This second solution could therefore affect the quality of Internet access services. Arcep thus analysed this practice through the provisions of the Open Internet regulation, and concluded that deploying a PMR is allowed by the regulation, provided it satisfy a real need for availability or security, and that the overall quality of Internet access and of other services running on the same network (notably VoLTE*) do not suffer consequently. Finally, prioritising PMR services must remain very exceptional.

* See lexicon.

CHAPTER 5

Devices and platforms, two structural links in the Internet access chain

HIGHLIGHTS

On 19 February 2020, the Senate voted unanimously **(342 for, 0 against)** to adopt the bill on guaranteeing consumers' freedom of choice in cyberspace. It will give Arcep powers to ensure device neutrality and platforms' interoperability.

On 24 February 2020, Bruno Le Maire, France's Minister for Economy and Finance, and Cédric O, Secretary of State for Digital Affairs, created **an inter-ministerial working group** whose members include the main French authorities, including Arcep, and whose purpose is to submit proposed courses of action with regard to digital platforms.

In a communication released in February 2020, **the European Commission** indicated that it was examining the possibility of introducing *ex ante* regulation designed to ensure that markets dominated by structural platforms remain open and accountable.

The European Open Internet regulation enshrines users' right to access and distribute information and content online. But it applies solely to ISPs, which are only one link in the Internet access chain. Located at the end of this chain, smartphones, voice assistants, connected cars and other devices, along with their operating systems, have proven to be the weak link in achieving an open internet.

Arcep shared this conclusion in its 2018 report[1] and laid out a series of measures to guarantee an open internet, in other words one where users are guaranteed their freedom of choice. These measures include:

- Data-driven regulation, and ensuring that information is transparent and easy for consumers and business users to compare;
- Ensuring the market's liquidity and users' freedom to switch easily from one environment to another;
- Lifting certain restrictions that key device market players have imposed artificially on users and on content and service developers.

After publishing this report, Arcep continued its monitoring and communication efforts throughout 2019, working in partnership with a range of stakeholders. In addition to devices' physical components, the small number of digital platforms that influence how users access the Internet is a topic that has grown in significance.

1. DEVICE NEUTRALITY: PROGRESS REPORT

A first tool for ensuring open devices is to give users the means to make informed choices. Without waiting for more advanced regulation to be put into place, in 2019 Arcep published two factsheets for end users, providing practical tips for getting the most out of their devices. The first[2] explains how users can keep their data when switching to a new smartphone, thanks to the data portability mechanisms introduced by the GDPR. Users can port their contacts as well as their photos, message history, calendars, and certain other applications when switching from one system to another. The purpose of the second factsheet[3] is to help users configure their smartphone to be able to take the utmost advantage of available services and content. This includes instructions on how to configure certain default options (browser, search engine and choice of apps) and so help users regain control of their smartphone.

To delve deeper into its examination of this issue, Arcep also wanted to query the people of France on their freedom of choice, for the 2019 edition of the Digital Market Barometer[4]. Regarding mobile operating systems, 99% of those queried use one of the two dominant OS, namely Android or iOS. Three quarters of users

1. https://en.arcep.fr/uploads/tx_gspublication/rapport-terminaux-fev2018-ENG.pdf
2. https://www.arcep.fr/demarches-et-services/utilisateurs/terminaux-portabilite-donnees.html
3. https://www.arcep.fr/demarches-et-services/utilisateurs/terminaux-personnalisation-api.html
4. https://en.arcep.fr/news/press-releases/p/n/digital-technology-ownership-and-usage.html

said it was important to be able to port their data, which is vital when switching from one system to another, but currently find it a difficult procedure to perform. In its report, Arcep concluded that the set of apps that typically come pre-installed on new smartphones constitutes a stricture imposed on users. The survey revealed that most users adopt the pre-installed browser: fewer than 20% of smartphone owners use a browser other than the pre-installed one, and two thirds have never even tested another browser. On the other hand, of those that do test other browsers, most (55%) switch to a different one. The Barometer thus confirmed Arcep's analysis and its proposals for guaranteeing users' freedom of choice when employing their devices.

Lastly, Arcep contributed to the HADOPI/CSA report[5]: on "Voice Assistants and Smart Speakers," focusing its analysis on the additional constraints created specifically by these devices, whose use is expected to become more and more commonplace. The evolution towards increasingly intelligent devices – notably voice assistants in the home and on-board computers in cars – raises legitimate concerns that these constraints will only increase. The devices' display features (small or no screen) and the fact of having largely audio-based interaction limits the ability to access exhaustive information. As a result, users are given only a selection of information over which they have very little control, and there is often a lack of transparency about how the device makes that selection.

Device neutrality was very much in the news in 2019. After having been condemned by the European Commission's Directorate-General for Competition for abuse of dominant position in the operating systems market in 2018, Google was required to provide its Android users a choice of alternative default browsers. The choice interface that was implemented nevertheless attracted a great deal of criticism. DuckDuckGo, for instance, accused Google of taking advantage of the way that choice interface was designed to promote its own browser. Google also experienced a hail of criticism over the auction it held for search engines wanting to be presented as alternatives to Android users. This situation underscores how difficult it can be to introduce efficient behavioural remedies after the fact.

On the other side of the Atlantic, the decision in the US to ban Huawei from having any business dealings with American companies forced the Chinese equipment supplier to stop offering Google services (Search, YouTube, Chrome, Play Store, developer kits, etc.) on its devices. Instead, Huawei chose to develop its own services[6], which could eventually result in stiffer competition in the operating systems and associated products markets, but also in the creation of a third closed ecosystem with problems similar to those already observed in the other two.

The issue of the terms and conditions applied to application developers wanting access to app stores also made headlines in 2019. Following a complaint filed by Spotify, the European Commission launched an investigation into the fees charged by Apple App Store. Spotify has accused Apple of taking advantage of its vertical integration to exonerate its Apple Music app from the 30% commission applied by the App Store, which gives it a *de facto* advantage over all other music stream applications. The 30% commission that Google applies on the Play Store has also come under scrutiny. For instance, the popular Fortnite game developed by Epic is no longer available on the Play Store, as Google refused[7] to grant the company's request for an exemption.

Moreover, the question of developers' access to certain device functions has yet to be resolved. The European Commission is still debating the matter of Apple devices' NFC chip, for instance, and particularly whether restricting third parties' access to it constitutes an abuse of dominant position.

Lastly, Privacy International and more than 50 other organisations published an open letter[8] to Alphabet, asking Google to take action against pre-installed software on Android devices. The signatories draw particular attention to device manufacturers who enjoy preferred access to device functions, without informing users.

The issue of devices' openness and neutrality is now a topic of discussion within a number of institutions. At the European level, the Centre on Regulation in Europe (CERRE) addressed the issue in a report published in March 2019[9]. The report concludes that the structures that are proper to the operating systems market are conducive to abusive behaviours, which can result in consumers' freedom of choice being restricted. The report thus proposes banning certain practices, such as pre-installing apps and activating certain functions by default, when the purpose of these practices is purely commercial.

In France, a bill was presented in the Senate[10] that seeks to enshrine consumers' freedom of choice when using their devices. This bill would give Arcep monitoring and penalty tools designed to ensure that this protection is properly enforced. In particular, it seeks to prohibit practices such as users' inability to delete certain preinstalled applications from their device, their inability to install apps from alternative app stores, and unjustified restrictions on developers' ability to access devices' hardware features. The bill was adopted unanimously by the Senate.

5. https://www.csa.fr/Informer/Collections-du-CSA/Thema-Toutes-les-etudes-realisees-ou-co-realisees-par-le-CSA-sur-des-themes-specifiques/Les-autres-etudes/Etude-HADOPI-CSA-Assistants-vocaux-et-enceintes-connectees
6. https://consumer.huawei.com/en/press/news/2020/huawei-revealed-huawei-appgallery-vision
7. https://www.theverge.com/2019/12/9/21003553/google-play-store-fortnite-epic-games-30-percent-cut-dispute
8. https://privacyinternational.org/advocacy/3320/open-letter-google
9. https://cerre.eu/publications/device-neutrality-missing-link-fair-and-transparent-online-competition
10. http://www.senat.fr/espace_presse/actualites/202002/libre_choix_du_consommateur_dans_le_cyberespace.html

2. STRUCTURAL DIGITAL PLATFORMS

If consumers' freedom of choice can be hampered by restrictions tied to their devices, the powerful position enjoyed by certain online platforms may also restrict this freedom of choice. The issue of the predominance of these platforms, which can be qualified as "structural," has been the focus of a number of discussions and initiatives. In France, the bill that seeks to protect consumers' freedom of choice in cyberspace includes provisions such as guaranteed interoperability, to share the network effects from which these leading platforms benefit. Initiatives that seek to limit the power of these platforms have also been launched in other European countries, including by Germany's Ministry for the Economy, the Dutch Competition Authority. Italy and Poland, along with Germany and France, published an open letter to EU vice-president Margrethe Vestager, urging the Commission to create a dedicated framework to hem in the power of certain digital industry players who enjoy a systemic reach. Lastly, several reports – including those produced by Crémer[11] (commissioned by the European Commission's DG Competition), Furman[12] (at the request of authorities in the UK) and Scott-Morton[13] (Stigler Center in Chicago), as well as the report from Australia's Competition and Consumer Commission[14] – underscore the predominance of certain Big Tech companies. All of these works emphasise that concerns over the size of these platforms are no longer economic and competition-related, but also societal in nature.

Arcep continues to pay very close attention to the work being done on regulatory practices that seek to tackle the dissemination of hate speech and disinformation. Arcep took part in "Regulation of social networks – Facebook experiment", whose aim had been to issue recommendations for creating a framework in France for promoting accountability amongst social media sites. Published in May 2019[15], the task force's report concluded that public regulatory intervention was warranted, and proposed several avenues to explore. The impetus behind this involvement must be to achieve greater accountability from social networks, based on *ex ante* regulation, while also ensuring a balance with a repressive policy, which is vital for effectively combatting the abuses' perpetrators.

As a follow up to the *"États généraux du numérique"* assembly, Arcep contributed to the work done on identifying the Big Tech companies that would be subject to this new *ex ante* regulation. Arcep proposed an initial definition of "structural digital platform" operators that would include online platform operators and operating system suppliers which, particularly because of their role as intermediary in providing access to online content and services, and because of their size, are in a position to significantly limit users' ability to engage in a business activity and to communicate online. As an adjunct, Arcep proposed a series of criteria to determine whether a platform can be considered "structural," along with a possible balance between *ex ante* and *ex post* regulation. Today, Arcep continues to explore these issues, and is investigating tools and remedies that could prove effective in enabling public authorities to regulate the players that control all of the Internet's intersections.

At the European level, and when publishing the agenda for the Digital Services Act, the European Commission indicated that it was exploring the possibility of imposing *ex ante* regulation on a certain number of digital sector players. After a public consultation and an impact study, which are scheduled for summer 2020, the European Commission is due to present its findings before the end of the year. The purpose of this work is to examine those methods of *ex ante* regulation that can guarantee legally binding actions, fairness and freedom to innovate in digital markets, whose benefits would extend well beyond just economic considerations. To this end, the French Government has created a working group[16] whose members include representatives of all of the main authorities in France which are responsible for regulating digital platforms, which include Arcep, to continue to work on the guidelines set by the European Commission under the Digital Services Act.

11. https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf
12. https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel
13. https://research.chicagobooth.edu/-/media/research/stigler/pdfs/market-structure---report-as-of-15-may-2019.pdf?la=en&hash=B2F11FB118904F2AD701B78FA24F08CFF1C0F58F
14. https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report
15. https://www.economie.gouv.fr/remise-rapport-mission-regulation-des-reseaux-sociaux
16. https://minefi.hosting.augure.com/Augure_Minefi/r/ContenuEnLigne/Download?id=5FA62C31-70A4-4392-8526-EFC6F85FD8AD&filename=2043%20CP%20groupe%20de%20travail%20num%C3%A9rique.pdf

OPEN FLOOR TO ...

SOPHIE PRIMAS

President of the Senate economic affairs Committee

THE SENATE ADOPTS DEVICE NEUTRALITY RULES

A great deal of ink has been spilled lamenting the economic dominance of a small handful of companies who control our lives online, but the software of economic regulation seems to be a few versions out of date. If, on the other side of the Atlantic, dismantling is seen as the be all and end all, the digital economy clearly has certain singular aspects that require a fresh approach and new regulation for what can be called "core" platforms. This is what the Senate is proposing in an Act that seeks to guarantee consumers' freedom of choice in cyberspace, which was adopted on 19 February of this year.

Among other things, it enshrines people's "freedom of choice" when using their smartphone or other digital device, aka the principle of device neutrality. Here, we must pay homage to the pioneering work that Arcep has done on this issue since the early 2010s, on which the Senate was able to draw. A regulatory authority will be tasked with verifying whether practices infringe on this freedom of choice – such as the inability to uninstall an app on a device, or discriminatory behaviour towards third-party applications – are justified or not. It will need to work with stakeholders to prevent harmful practices from emerging, rather than penalising them after the fact. The Senate is thus proposing a more agile, pro-innovation regulation that re-empowers users.

While negotiations are underway at the European level, senators in France want to take action immediately at the national level, for one simple reason: the cost of waiting seems too high. The longer we wait, the longer we run the risk of letting Big Tech giants smother competition and innovation, and lock consumers inextricably into their ecosystem. There is an urgent need to hand the power back to users.

DIANE COYLE

*Bennett Professor of Public Policy - **University of Cambridge***
Member of the UK's Expert Panel on Digital Competition

EX ANTE REGULATION OF DIGITAL PLATFORMS

The view that digital markets, dominated by a small number of companies, are not working as well as they could is widespread. The concerns range from the absence of consumer choice and competition to the toxicity of "fake news" online.

The current economic crisis is likely to mean these cash-rich companies will find themselves in an even more dominant position. However, it is challenging to improve competition and consumer choice in these markets. One reason is the presence of "network effects" whereby we all benefit the more other users there are on a digital platform, and the bigger it is. So digital markets are always likely to be "winner takes all" markets.

It is for this reason that our report, the Furman Review, in the UK concluded that *ex ante* regulation of the companies concerned would need to be strengthened, along with enhanced competition policy scrutinising their behaviour *ex post.*

Currently there are few regulations governing the kinds of conduct or outcomes specific to digital platforms. These include behaviours such as self-preferencing – dominant platforms prioritising their own services above those of other suppliers – or frequent unannounced changes in long and obscure terms and conditions, or in APIs. We recommended a digital markets unit be set up to introduce and enforce a code of conduct for platforms with market power; the UK government has established a task force at the Competition and Markets Authority to do this.

We also called for specific regulation of data, a key driver of concentration and barrier to entry. Data mobility and interoperability will be essential to drive competition. It might also be necessary to mandate more open access to some of the data held by the digital giants. This is not only to help make the markets more open to competition; it could also become a social necessity at a time of unparalleled economic crisis. Many people are asking why a few large companies are allowed to retain all the value from hoards of data provided for free by their users, and demanding that it be used for social as well as private benefit.

PART 3

Tackle the digital technology's environmental challenge

CHAPTER 6

Integrate digital tech's environmental footprint into the regulation

CHAPTER 6

Integrate digital tech's environmental footprint into the regulation

HIGHLIGHTS

The forward-looking framework of the "Future Networks" cycle of inquiry created an opportunity for Arcep to begin the work of assessing the impact that various network developments, and increasing use of those networks, have on digital technology's carbon footprint, which culminated in the publication of a brief **on 21 October 2019.**

The Body of European Regulators for Electronic Communications (BEREC) created three new expert working groups **on 6 March,** including one devoted to sustainable development of which Arcep is the co-chair.

On 6 April 2020, Arcep added an environmental dimension to its tool for collecting information from telecom operators, to gain a deeper understanding of the sector's environmental issues and challenges, and to be able to keep public policymakers and users informed on the impact of their usage.

Back in 2018, as part of its "Future Networks" cycle of inquiry, and surrounded by a Scientific Committee, Arcep began the work of assessing the impact that various network developments, and increasing use of those networks, have on digital technology's carbon footprint. After publishing a first brief on the topic in October 2019, Arcep remains committed to pursuing its work on environmental protection.

1. CURRENT STATUS

A growing amount of attention is being paid to digital technology's environmental impact. The Digital Market Barometer that Arcep published in 2019 underscores this growing societal awareness, and reveals that, although people in France have a positive view of the role that digital technology plays in their daily lives, they also have growing concerns about its impact on the environment. Thirty eight percent of people in France view digital technology as having a positive impact on the environment, compared to 53% in 2008. While 69% are willing to change their behaviour, 45% say they still do not have enough information on digital technology's environmental impact[1].

According to sources[2], digital technology currently accounts for 3% to 4% of the world's greenhouse gas (GHG) emissions, giving it a carbon footprint equal to the airline industry. If this percentage is still small compared to other sectors, the ongoing annual increase in the use of digital technology (volume of data, devices, etc.) should give us pause[3].

2. ARCEP'S INITIAL WORK, THROUGH ITS "FUTURE NETWORKS" CYCLE OF INQUIRY

Back in 2018, as part of its "Future Networks" cycle of inquiry, and surrounded by a Scientific Committee, Arcep began the work of assessing the impact that various network developments, and increasing use of those networks, have on digital technology's carbon footprint. To this end, Arcep queried experts from civil society, industry players as well as public sector actors in an attempt to identify the key issues surrounding the digital world's carbon footprint, and to provide some preliminary responses.

This work made it possible to draw several conclusions, of which the main ones can be found here[4].

1. CREDOC, survey on "Standards of living and Aspirations," June 2019.
2. Shiftproject, "Lean ICT: Towards Digital Sobriety", October 2018; GreenIT, "Environment footprint of the digital world", September 2019.
3. Regarding the digital world's GHG emissions, in a Senate hearing on 29 January 2020, Hugues Ferreboeuf, head of the Shift Project, stated at that, at the current rate of increase, these emissions could triple digital tech's 2015 global footprint by 2025.
4. For more detailed conclusions see the Arcep brief on "Digital tech's carbon footprint" of 21 October 2019, available here: https://www.arcep.fr/uploads/tx_gspublication/reseaux-du-futur-empreinte-carbone-numerique-juillet2019.pdf

First, if networks' energy consumption is a major source of operators' GHG emissions, digital technology's GHG emissions include the entire value chain, from datacentres to devices, of which the latter are primary cause of digital tech's carbon footprint. According to sources, devices (smartphones, tablets, displays, smart speakers, etc.) are responsible for more than half of digital technology's GHG emissions, and particularly their production phase which accounts for around 80% of the emissions attributed to them. In addition to GHG emissions, one must also factor in the consumption of resources (notably rare earths and water) used in the production of devices. Telecom operators in particular may have an incentive to make their networks and datacentres more energy efficient, as a way to decrease their energy bill. A rough estimate puts French operators' energy bills at between several dozen and several hundred million euros[5] depending on their size and the price they pay for electricity. For mobile operators, for instance, energy consumption represents 15% to 20% of their operating costs[6].

Second, new uses and their increasingly massive adoption – which are enabled, among other things, by improvements to the networks and devices – are driving up data consumption. This in turn is creating a rebound effect[7], whereby a technological development which enables a reduction in GHG emissions, at constant rates of use, is in fact likely to result in an overall increase in emissions because of the increased number of uses or applications it enables. This phenomenon is therefore driving up energy consumption. It emerged from interviews that Arcep conducted when preparing its brief on "Digital tech's carbon footprint" that, in the specific case of mobile networks – whose power consumption depends heavily on their use – an antenna can consume up to three times more power during peak traffic times as when it is idle. The power consumption of equipment located in operators' core network also increases apace with traffic. Conversely, technological improvements can improve energy efficiency and help reduce consumption per traffic unit. Regarding fixed network use, for instance, one player stated that, on average, fibre consumes just over 0.5 watt (W) per line, or three times less than ADSL (1.8 W) and four times less than PSTN (2.1 W) on the access network[8]. The way in which these two phenomena are combined will ultimately determine how overall energy consumption evolves.

Finally, if some players along the chain (network and datacentre operators, for instance) have an incentive to reduce their carbon footprint – notably to contain their infrastructure-related costs[9] – the environmental footprint tied to the use of digital services remains invisible to most consumers. For instance, the majority of digital technology's energy consumption derives from: consumers (20%), datacentre production and use (19%), network production and use (16%), and by the production alone of computers (17%), smartphones (11%) and televisions (11%)[10]. There is therefore a real need to inform citizens and businesses of these facts, based on stakeholders' shared metrological benchmarks.

5. Estimate based on operators' CSR reports and regulated electricity tariffs.
6. https://www.mobileworldlive.com/ict-ee-18-news/global-ict-energy-efficiency-summit-paves-way-for-5g
7. The rebound effect refers to the increased consumption induced by the different technological innovations (i.e., decreased costs, improved energy efficiency, etc.). It was laid out for the first time by W. Stanley Jevons ("The Jevons Paradox") and later updated by economists Daniel Khazzoom and Leonard Brookes ("The Khazzoom-Brookes postulate"). The paradox lies in the fact that any development of an application or a technology that improves an activity's energy efficiency must, a priori, involve a reduction of this activity's overall energy impact. However, if this improvement engenders (or produces) a parallel decrease in the cost of producing that good or service, this decrease then makes it possible to produce a greater quantity of the good or service at a lower price, and thereby stimulates demand.
8. The power consumed by these wireline technologies depends relatively little on how heavily they are used, so this evolution has translated into gains in the absolute value of consumption.
9. These incentives do not, however, necessarily carry over to digital technology's entire environmental footprint (notably the hardware production and recycling stages).
10. See footnote 7.

3. THE REGULATOR'S COMMITMENT TO MEETING THE ENVIRONMENTAL CHALLENGE

Galvanised by these initial conclusions, Arcep is proposing an approach to tackling this issue that is strongly rooted in data-driven regulation, and whose aim is to provide end users with relevant information on the environmental impact of using digital technology. Defined as a regulatory objective in Article L.32-1 of the French Postal and Electronic Communications Code (CPCE)[11], environmental protection is indeed an area in which Arcep – which is committed to fostering debate based on objective facts and with no preconceived notions – wants to expand its work, in particular to deepen its awareness and to transmit clear and accurate information to end users. This approach could lead to a "Green Barometer" for digital technology. Here, Arcep is beginning the process of gathering information from operators on the environmental impact of telecoms networks and devices. The collected indicators pertain to the main operators' greenhouse gas emissions, and to the energy consumed by the Internet and set-top boxes they provide to their customers.

In early 2020, Arcep, along with other French regulators, contributed to the publication of a brief that testified to their growing awareness, and the role that regulators can play in tackling the climate challenge. In the same vein, Arcep and ADEME are set to further their actions with a joint study on environmental concerns, and by working together on the implementation of the Circular Economy Act which requires Internet service providers to keep their customers informed about their consumption and the associated greenhouse gas emissions.

Arcep also suggested to its European counterparts that this issue be included in the work being done by BEREC in the coming months and years, after being contacted by several national telecom regulators following the publication of its brief on "Digital tech's carbon footprint". To this end, European regulators working within BEREC created three new expert working groups on 6 March of this year, including one devoted to sustainable development which will focus on the environmental impact of telecom networks in their broadest sense, and on exploring ways to reduce it. Arcep's Anaïs Aubert is the co-chair of this working group, along with Dr. Panos Karaminas, who is the BEREC Office's Head of Programme Management.

These plans are in sync with the trend underway at the European level, as the European Commission has made digital technology's carbon footprint one of the areas of focus in the European Green Deal which is set to be published in the coming months. As part of its digital strategy, it announced the target of having carbon neutral telecommunications networks and datacentres by 2030. The Radio Spectrum Policy Group (RSPG) has also added an environmental dimension to its work programme for 2020 and 2021. The dedicated RSPG sub-group plans on tackling three topics: including environmental considerations in the terms of frequency licences, protecting meteorological services, notably in the millimetre wave bands, and giving power companies access to frequencies.

SOME BASIC TIPS FOR REDUCING DIGITAL TECHNOLOGY'S ENVIRONMENTAL FOOTPRINT:

1. Choose the most energy efficient network, depending on the use case

- Fibre is a more energy efficient fixed network than copper, for instance
- Switch your phone to Wi-Fi when at home (instead of continuing to use 3G or 4G)
- Download content to be consumed when on the go before leaving home, using a fixed network Wi-Fi connection

2. Become more digitally sober

- Turn off all network boxes at night and when away from home
- Only download apps and videos that you are sure to use/watch
- Reduce video picture quality if possible
- Limit the number of e-mail attachments and clean up your inbox on regular basis

3. Optimise connected objects' lifespan

- Only buy a new smartphone when the old one no longer works (same for other devices: computers, displays, tablets, etc.)
- Opt for refurbished devices, and recycle your phone when it reaches the end of its life.

11. In tandem with the Ministers responsible for health and the environment.

OPEN FLOOR TO ...

ARNAUD LEROY

*President - **ADEME***

INTERNET AND THE GREEN TRANSITION

I am delighted to be penning this contribution on a topic that is becoming a source of concern for more and more of our fellows, both in France and in many countries across the globe. They are all beginning to wonder about the internet and, by extension, digital tech as a whole: is it an entirely positive transition accelerator, or are there also negative aspects to this growing digitisation?

The sector symbolises the paradoxes underlying the green transition's implementation. The recently passed law on the circular economy also marks an important milestone in society's questioning of the greenhouse gas emissions of our internet-driven lives, at a time when the sector's GHG emissions are skyrocketing.

The lockdown proved how vital it is to have network infrastructures that work during times of crisis as, today more than ever before, data traffic is a major issue in our society. As crucial as they are, these data that allow us to stay in touch, to continue to work, to stay informed, to educate our children and to be entertained, must not result in our activities creating an even greater carbon footprint.

So we need to continue to make our networks more energy efficient, as is the case with optical fibre rollouts, to inform users of the greenhouse gas emissions that their use of digital services generate, and to offer solutions for all of the stakeholders working to achieve "digital sobriety".

If the current trajectory of technological developments is reducing the size of and energy consumed by devices, we are also seeing the impact being transferred over to those stages for which available data are less reliable: extraction of non-renewable resources, end of life processing for devices and internet usage.

HUGUES FERREBOEUF

Project leader and co-author of the report:
*"Lean ICT – Towards digital sobriety" - **The Shift Project***

DIGITAL TECH AND THE ENVIRONMENT: A VITAL NEED FOR CONGRUENCE

The digital transition that is currently underway is advancing apace with a massive surge in the carbon footprint left by the services, devices and infrastructures that make that transition possible, but without any real hope as yet of stepping up the process of decarbonising the enabling sectors. This is deeply concerning.

The main reasons for this situation are not technological but rather systemic[1], and remedying them would require consumers and their suppliers to become more digitally sober, both quickly and dramatically, if we really hope to tackle the environmental emergency. But only the adoption of a dedicated regulation will create the ability to make these changes at the pace and on the scale that are needed.

Which is why the Shift Project considers Arcep's involvement in this issue as not only welcome but also totally necessary, mobilising its sector-specific expertise to inform public policies, and as the overseer of regulatory mechanisms.

To guarantee efficient action that is equal to the task at hand, it will be vital to achieve utmost consistency between choices made with environmental imperatives in mind, and those designed to uphold other principles (e.g. net neutrality) or when deploying new technologies (5G, IoT...).

Finally, given the existence of the sector's USA – China duopoly, it is of course crucial that similar catalysts be implemented on a European scale, which will require awareness and mobilisation as much from national regulators as from the European Commission and Parliament.

1. The Shift Project – "Lean ICT – Towards digital sobriety" report, 2018

Lexicon

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

A

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

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.

Anycast: an addressing and routing technique used to reroute data to the closest test server.

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.

AS (autonomous system): a collection of IP networks and routers that is controlled by a single entity, such as an internet service provider (ISP).

B

BEREC (Body of European Regulators for Electronic Communications): independent European body created by the Council of the European Union and the European Parliament, and which assembles the electronic communications regulators from the 27 European Union Member States.

BGP (Border Gateway Protocol): a protocol designed to exchange routing, used on the internet network in particular.

Buffer: (aka data buffer) refers to a virtual memory area or a region of physical memory storage on a computer's hard drive used to store data temporarily.

C

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

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

CDN: Internet Content Delivery Network

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

CPU (Central Processing Unit): a computer's processor or microprocessor, responsible for executing computer programmes' instructions.

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

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

D

DHCP (Dynamic Host Configuration Protocol): network protocol whose role is to ensure automatic configuration of a machine's IP parameters.

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

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

DWDM (Dense Wavelength Division Multiplexing): wavelength multiplexing that enables several signals to travel over a single fibre.

E

EDPB (European Data Protection Board): an independent European authority whose purpose is to ensure consistent application of the GDPR across Europe, and to promote cooperation amongst the EU's data protection authorities.

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

EVPN: Ethernet VPN is a technology for carrying layer 2 Ethernet traffic a a virtual private network, using wide area network protocols.

F

Firewall: a hardware or software security mechanism used to filter and/or block traffic streams based on predetermined security rules.

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

G

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

H

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

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

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

I

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

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

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-enabled: which actually transmits and receives traffic using IPv6 routing, either thanks to activation by the customer or activation performed by the operator.

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.

ISP: Internet Service Provider

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

L

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

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

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

M

macOS: operating system developed by Apple for its computers.

MPLS (MultiProtocol Label Switching): data transport mechanism based on switching the labels that are inserted at the MPLS network entry point and removed at the exit.

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

N

NAP (Network Access Point): a public peering location that provides a marketplace on which users can buy and/or sell traffic capacity to other players.

NAS (Network Attached Storage): autonomous file storage server that is attached to a network.

NAT: Network Address Translation mechanism for remapping one IP address space to another, used in particular to limit the number of public IPv4 addresses being used.

Network termination point: the physical location at which a user gains access to public electronic communications networks.

NFC (Near-Field Communication) chip: very short-range, high frequency wireless technology used to exchange information between peripherals, typically within a range of around 10 centimetres.

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

O

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

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 CAPs provide over the internet.

P

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

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.

PoP: an operator's physical point of presence.

Port: every internet connection emanating from an application is associated with UDP or TCP session, which is identified by a port number using a 16-bit coding scheme.

Q

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

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

R

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

RFC (Request For Comments): official memorandum that describes the technical aspects and specifications that apply to the working of the internet or to different computer hardware.

RPKI (Resource Public Key Infrastructure): designed to secure internet routing infrastructure.

S

Sandbox: a computer security mechanism based on isolating software components.

SD-WAN (Software-Defined Wide Area Network): IP packet transport technology separating the network hardware from the software, thereby creating the ability to control and perform a centralised and automated deployment on heterogeneous equipment.

SIEM: a Security Information and Event Management approach.

Specialised service: electronic communication service(s) that are distinct from internet access services, and which require specific quality of service levels.

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

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

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

Shutdown: intentional interruption of electronic communications services, making them inaccessible or unavailable, either to an entire population or in a specific location (e.g. nationally or locally).

T

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

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

Tier 1: a network capable of interconnecting directly with any internet network (i.e. via peering) without having to go through a transit provider. There were 18 Tier 1 operators in 2019: AT&T, CenturyLink/Level 3, Cogent Communications, Deutsche Telekom AG, Global Telecom & Technology, Hurricane Electric, KPN International, Liberty Global, NTT Communications, Orange, PCCW Global, Sprint, Tata Communications, Telecom Italia Sparkle, Telxius/Telefónica, Telia Carrier, Verizon Enterprise Solutions and Zayo Group.

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

Transit provider: company that provides transit services.

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

Tunnel broker: service providing global IPv6 connectivity to a machine with an IPv4 connection, by tunnelling over that IPv4 connection to an IPv6 host.

U

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

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

V

VLAN: Virtual Local Area Network that groups together a set of machines virtually but not physically. This concept makes it possible to create several independent networks which, by default, cannot communicate with one another.

VoLTE (Voice over LTE): main voice transport technique used on 4G LTE mobile telephone networks.

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

VXLAN (Virtual eXtensible Local Area Network): network virtualisation technology whose functions are similar to those of VLAN and which encapsulates Layer 2 Ethernet frames in Layer 3 UDP packets, with the goal of isolating the maximum number of virtual machines.

W

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

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

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

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

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

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.

#

4G: the fourth generation of mobile telephony standards. It is defined by 3GPP Release 8 standards.

5G: the fifth generation of mobile telephony standards. It is defined by 3GPP Release 15 standards.

Annexes

ANNEX 1

Parameters provided by the API

The following parameters are taken from the Decision Arcep adopted in late October 2019[1] and whose implementing order was published in the *Journal Officiel* of 16 January 2020.

1. MAIN PARAMETERS

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

Presence requirement	JSON tree	Parameter name	Unit	Parameter details	Format/ accepted values
Mandatory	Root	ApiVersion		Version de API	64-bit signed integer
Optional	Gateway	Model		Customer IAD (“box”) name	text
Optional	Gateway	SoftwareVersion		Software version	text
Mandatory when defined and existing	SubscriptionSpeed	DownloadMin	Kbit/s	Minimum guaranteed download speed	64-bit signed integer
Mandatory when defined and existing	SubscriptionSpeed	UploadMin	Kbit/s	Minimum guaranteed upload speed	64-bit signed integer
Mandatory	SubscriptionSpeed	DownloadMax	Kbit/s	Maximum guaranteed download speed	64-bit signed integer
Mandatory	SubscriptionSpeed	UploadMax	Kbit/s	Maximum guaranteed upload speed	64-bit signed integer
Mandatory when defined and existing	SubscriptionSpeed	DownloadNormally	Kbit/s	Guaranteed “normally available” download speed (if it exists)	64-bit signed integer
Mandatory when defined and existing	SubscriptionSpeed	UploadNormally	Kbit/s	Guaranteed “normally available” upload speed (if it exists)	64-bit signed integer
Mandatory	Wan	Technology		WAN technology used by the IAD (“box”)	[«ftth»;»adsl»;«vdsl»;»gfast»; »cable»;»satellite»;»2g»;»3g»; »4g»;»5g»;»other»]
Mandatory if FttH is the WAN technology	Wan/SpeedOnt	Download	Kbit/s	FttH only: Ethernet downlink speed between the ONT and IAD. Optional: if PLC detected on the WAN port: raw speed provided by PLC	64-bit signed integer
Mandatory if FttH is the WAN technology	Wan/SpeedOnt	Upload	Kbit/s	FttH only: Ethernet downlink speed between the ONT and IAD. Optional: if PLC detected on the WAN port: raw speed provided by PLC	64-bit signed integer
Mandatory if FttH is the WAN technology	Wan/SpeedOnt	Duplex		FttH only: Ethernet mode between the ONT and IAD	[«half»;»full»]
Mandatory if xDSL is the WAN technology	Wan/ SpeedSynchro	Download	Kbit/s	xDSL only: downstream synchronisation speed	64-bit signed integer
Mandatory if xDSL is the WAN technology	Wan/ SpeedSynchro	Upload	Kbit/s	xDSL only: upstream synchronisation speed	64-bit signed integer
Mandatory	Wan	Aggregation		“No” secondary active WAN technology: absence of aggregation or aggregation not activated	[«no»;»ftth»;»adsl»;«vdsl»; »gfast»;»cable»;»satellite»; »2g»;»3g»;»4g»;»5g»;»other»]

N.B.: The “maximum speed” indicated for WAN FttH, cable and satellite access lines must always be the customer’s advertised speed. For other WAN technologies, it should only be filled in if the connection has a guaranteed maximum speed. n’est à remplir que si l’accès possède un débit maximum.

1. https://www.arcep.fr/uploads/tx_gsavis/19-1410.pdf

Presence requirement	JSON tree	Parameter name	Unit	Parameter details	Format/ accepted values
Mandatory	Lan	ConnectionType		Technology used by the API requesting device to reach the IAD. Note: PLC detection on the LAN is optional.	[«wifi»;»ethernet»; »cpl» ; «other»]
Mandatory	Lan/SpeedLan	DownloadMax	Kbit/s	Interface's maximum theoretical speed. Ethernet/PLC: capacity of the Ethernet port on the box where the API request originates. Wi-Fi: maximum theoretical speed provided by the box's Wi-Fi connection.	64-bit signed integer
Mandatory	Lan/SpeedLan	Download	Kbit/s	LAN downlink speed (Ethernet / Wi-Fi / PLC) negotiated by the API requesting device PLC: raw speed supplied by the PLC connected to the Ethernet port from which the API request is sent	64-bit signed integer
Mandatory	Lan/SpeedLan	UploadMax		Interface's maximum theoretical speed. Ethernet/PLC: capacity of the Ethernet port on the box where the API request originates. Wi-Fi: maximum theoretical speed provided by the box's Wi-Fi connection.	64-bit signed integer
Mandatory	Lan/SpeedLan	Upload	Kbit/s	LAN (Ethernet / Wi-Fi / PLC) uplink speed negotiated by the API requesting device	64-bit signed integer
Mandatory if the LAN connection is Ethernet	Lan/SpeedLan	Duplex		Ethernet half-duplex or full-duplex	[«half»;»full»]
Mandatory if the LAN connection is Wi-Fi	Lan/Wifi	IeeeMax		Highest Wi-Fi IEEE 802.11 standard compatible with the box.	Positive integer (802.11a=>1 802.11b=>2 802.11g=> 3 802.11n=>4 802.11ac=>5 802.11ax=>6)
Mandatory if the LAN connection is Wi-Fi	Lan/Wifi	Ieee		Wi-Fi IEEE 802.11 standard negotiated between the IAD and the API requesting device.	Positive integer (802.11a=>1 802.11b=>2 802.11g=> 3 802.11n=>4 802.11ac=>5 802.11ax=>6)
Mandatory if the LAN connection is Wi-Fi	Lan/Wifi	RadioBand		Wi-Fi radio band used by the API requesting device. 2.4 GHz frequency block or 5 GHz frequency block.	Positive integer: 2.4 GHz band => 2 5 GHz band => 5
Mandatory if the LAN connection is Wi-Fi	Lan/Wifi	Rssi	dBm	Received radio signal strength Indication. It is the API requesting device's RSSI.	64-bit signed integer
Optional	Miscellaneous	Other[1…n]		Any other parameters that the operator wants to transmit to the measuring tools.	

N.B.: Some PLC[2] adapters cannot be detected by the IAD. The same is true with Wi-Fi connections initiated at an outside access point that is connected to the IAD via Ethernet.

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

2. CROSS-TRAFFIC PARAMETERS

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

- immediately after the customer has launched the test for measuring internet quality of service;
- immediately after the measurement tool has completed the internet quality of service test.

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

One optional measure is to install a LAN cross-traffic meter. It creates the ability to detect cross-traffic that can affect the LAN.

Presence requirement	JSON tree	Parameter name	Unit	Parameter details	Format/ accepted values
Mandatory	TimeStamp	ApiCallTime		Time stamp that corresponds to the time when the API is called	64-bit signed integer
Mandatory	TimeStamp	LastUpdate		Time stamp for the WAN port meter's latest update (meter is read in real time LastUpdate = ApiCallTime)	64-bit signed integer
Mandatory	Wan/ByteCounter	Download	Bytes	WAN port downstream traffic meter reading (internet => IAD)	64-bit signed integer
Mandatory	Wan/ByteCounter	Upload	Bytes	WAN port upstream traffic meter reading (IAD => internet)	64-bit signed integer
Optional	Lan/ByteCounter	Download	Bytes	LAN port downstream traffic meter reading (IAD => User device)	64-bit signed integer
Optional	Lan/ByteCounter	Upload	Bytes	LAN port upstream traffic meter reading (User device => IAD)	64-bit signed integer

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

If "non-internet" traffic (chiefly TV/VoD traffic) falls outside the scope of the Internet speed test, with dedicated bandwidth, then cross-traffic meters only measure the bytes tied to Internet traffic.

If "non-internet" traffic affects maximum speeds on the Internet, which correspond to an overall bandwidth pool used for one or the other, then cross-traffic meters measure the bytes on the WAN port, including TV/VoD traffic.

ANNEX 2

Tests servers provided by the different quality of service measurement tools

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

1. NPERF

Sponsor, as listed on nPerf	City	Region	IPv6 (web, Windows application)	IPv6 (Android / iOS application)	Connection capacity	Port used	Hosting company	AS
RRT	Compiègne	Hauts-de-France	IPv4 only	IPv4 only	10 Gbit/s	443	Renater	AS2200
Orange	Paris	Île-de-France	IPv4 or IPv6	IPv4 only	10 Gbit/s	443	Orange	AS3215
Orange	Puteaux	Île-de-France	IPv4 or IPv6	IPv4 only	10 Gbit/s	443	Orange	AS3215
Orange	Rennes	Bretagne	IPv4 or IPv6	IPv4 only	10 Gbit/s	443	Orange	AS3215
Orange	Lille	Hauts-de-France	IPv4 or IPv6	IPv4 only	10 Gbit/s	443	Orange	AS3215
Orange	Strasbourg	Grand-Est	IPv4 or IPv6	IPv4 only	10 Gbit/s	443	Orange	AS3215
Orange	Lyon	Auvergne-Rhône-Alpes	IPv4 or IPv6	IPv4 only	10 Gbit/s	443	Orange	AS3215
Orange	Marseille	Région Sud	IPv4 or IPv6	IPv4 only	10 Gbit/s	443	Orange	AS3215
Orange	Bordeaux	Nouvelle-Aquitaine	IPv4 or IPv6	IPv4 only	10 Gbit/s	443	Orange	AS3215
Bouygues Telecom	*Anycast*	Île-de-France (Paris) Hauts-de-France (Lille) Auvergne-Rhône-Alpes (Lyon) Région Sud (Marseille) Nouvelle-Aquitaine (Bordeaux)	IPv4 or IPv6	IPv4 only	10 Gbit/s	443	Bouygues Telecom	AS5410
Bouygues Telecom	Paris	Île-de-France	IPv4 or IPv6	IPv4 only	10 Gbit/s	443	Bouygues Telecom	AS5410
Bouygues Telecom	Lille	Hauts-de-France	IPv4 or IPv6	IPv4 only	10 Gbit/s	443	Bouygues Telecom	AS5410
Bouygues Telecom	Lyon	Auvergne-Rhône-Alpes	IPv4 or IPv6	IPv4 only	10 Gbit/s	443	Bouygues Telecom	AS5410
Bouygues Telecom	Marseille	Région Sud	IPv4 or IPv6	IPv4 only	10 Gbit/s	443	Bouygues Telecom	AS5410
Bouygues Telecom	Bordeaux	Nouvelle-Aquitaine	IPv4 or IPv6	IPv4 only	10 Gbit/s	443	Bouygues Telecom	AS5410

Sponsor, as listed on nPerf	City	Region	IPv6 (web, Windows application)	IPv6 (Android / iOS application)	Connection capacity	Port used	Hosting company	AS
Phibee Telecom	Aubervilliers	Île-de-France	IPv4 or IPv6	IPv4 only	10 Gbit/s	8443	Phibee Telecom	AS8487
Online	Vitry-sur-Seine	Île-de-France	IPv4 only	IPv4 only	4 Gbit/s	443	Scaleway – Online	AS12876
Wangarden	Pontoise	Île-de-France	IPv4 only	IPv4 only	1 Gbit/s	443	Scaleway – Online	AS12876
SFR	*Anycast*	Île-de-France (Courbevoie) Auvergne-Rhône-Alpes (Vénissieux)	IPv4 only	IPv4 only	10 Gbit/s	443	SFR	AS15557
SFR	Courbevoie	Île-de-France	IPv4 only	IPv4 only	10 Gbit/s	443	SFR	AS15557
SFR	Vénissieux	Auvergne-Rhône-Alpes	IPv4 only	IPv4 only	10 Gbit/s	443	SFR	AS15557
OVH	Gravelines	Hauts-de-France	IPv4 or IPv6	IPv4 only	10 Gbit/s	443	OVH	AS16276
OVH	Roubaix	Hauts-de-France	IPv4 or IPv6	IPv4 only	10 Gbit/s	443	OVH	AS16276
OVH	Strasbourg	Grand-Est	IPv4 or IPv6	IPv4 only	10 Gbit/s	443	OVH	AS16276
Axialys	Courbevoie	Île-de-France	IPv4 only	IPv4 only	1 Gbit/s	443	Axialys	AS16363
Corexpert	Paris	Île-de-France	IPv4 only	IPv4 only	5 Gbit/s	443	Amazon AWS	AS16509
Ikoula	Reims	Grand-Est	IPv4 or IPv6	IPv4 only	1 Gbit/s	8443	Ikoula	AS21409
Eurafibre	Douai	Hauts-de-France	IPv4 only	IPv4 only	20 Gbit/s	8443	Eurafibre	AS35625
Videofutur	Paris	Île-de-France	IPv4 only	IPv4 only	10 Gbit/s	443	Reunicable	AS37002
CMIN	Lucé	Centre-Val de Loire	IPv4 only	IPv4 only	1 Gbit/s	443	CMIN	AS39271
SHPV France	Toulouse	Occitanie	IPv4 or IPv6	IPv4 only	4 Gbit/s	443	SHPV France	AS41652
Proceau	Paris	Île-de-France	IPv4 only	IPv4 only	1 Gbit/s	8443	Proceau	AS43424
Alsatis	Paris	Île-de-France	IPv4 only	IPv4 only	10 Gbit/s	443	Alsatis	AS48072
Muona	Lyon	Auvergne-Rhône-Alpes	IPv4 only	IPv4 only	1 Gbit/s	443	Muona	AS50818
Metro Optic	Paris	Île-de-France	IPv4 only	IPv4 only	1 Gbit/s	443	Metro Optic	AS57902
DataPacket	Paris	Île-de-France	IPv4 only	IPv4 only	10 Gbit/s	443	DataCamp	AS60068
System-Net	Montpellier	Occitanie	IPv4 only	IPv4 only	1 Gbit/s	443	System-Net	AS60427
Rezopole	Lyon	Auvergne-Rhône-Alpes	IPv4 or IPv6	IPv4 only	1 Gbit/s	443	Rezopole	AS199422
AOC Telecom	Clermont-Ferrand	Auvergne-Rhône-Alpes	IPv4 only	IPv4 only	200 Mbit/s	443	AOC Telecom	AS202328
Neyrial	Cébazat	Auvergne-Rhône-Alpes	IPv4 only	IPv4 only	1 Gbit/s	443	Neyrial informatique	AS203352
Telicity	Bordeaux	Nouvelle-Aquitaine	IPv4 only	IPv4 only	10 Gbit/s	443	Telicity	AS204355
Alpesys	Grenoble	Auvergne-Rhône-Alpes	IPv4 only	IPv4 only	10 Gbit/s	8443	Alpesys	AS206120
Azylis	Besançon	Bourgogne-Franche-Comté	IPv4 only	IPv4 only	1 Gbit/s	443	Azylis	AS207151

2. UFC-QUE CHOISIR SPEEDTEST

City	Region	IPv6	Connection capacity	Port used	Hosting company	AS
Saint-Denis	Île-de-France	IPv4 only	20 Gbit/s	443	Zayo France	AS8218

3. FIXED SPEED TESTS DEVELOPED BY QOSI (5GMARK / DÉBITEST 60 / NETGMARK ZD-NET)

Domain name	City	Region	IPv6	Connection Capacity	Port used	Hosting company	AS
dedi3.5gmark.com	Saint-Ouen-l'Aumône	Île-de-France	IPv4 only	1 Gbit/s	8443	Scaleway – Online	AS12876
dedi5.5gmark.com	Vitry-sur-Seine	Île-de-France	IPv4 only	2.5 Gbit/s	8443	Scaleway – Online	AS12876
dedi6.5gmark.com	Saint-Ouen-l'Aumône	Île-de-France	IPv4 only	1 Gbit/s	8443	Scaleway – Online	AS12876
paris.4gmark.com	Vitry-sur-Seine	Île-de-France	IPv4 only	400 Mbit/s	8443	Scaleway – Online	AS12876
paris2.4gmark.com	Vitry-sur-Seine	Île-de-France	IPv4 only	400 Mbit/s	8443	Scaleway – Online	AS12876
paris3.4gmark.com	Vitry-sur-Seine	Île-de-France	IPv4 only	400 Mbit/s	8443	Scaleway – Online	AS12876

4. MOBILE SPEED TESTS DEVELOPED BY QOSI (5GMARK / BECOVER+ / DÉBITEST 60 / GIGALIS / KICAPTE / QOSBEE / TU CAPTES ? / RÉSOMÈTRE)

Sponsor, as listed on the application	City	Region	IPv6	Assumed connection capacity	Port used	Hosting company	AS
Bouygues Telecom	Nanterre	Île-de-France	IPv6 only*	10 Gbit/s	443	Bouygues Telecom	AS540
Orange Montsouris	Paris	Île-de-France	IPv6 only*	10 Gbit/s	443	Orange	AS3215
Orange Lyon	Lyon	Auvergne-Rhône-Alpes	IPv6 only*	10 Gbit/s	443	Orange	AS3215
Azure Network	Paris / Marseille	Île-de-France / Région Sud	IPv6 only*	600 Mbit/s	443	Microsoft Corporation	AS8068
OneProvider Paris	Vitry-sur-Seine	Île-de-France	IPv4 only	400 Mbit/s	443	Scaleway – Online	AS12876
OneProvider Paris2	Vitry-sur-Seine	Île-de-France	IPv4 only	400 Mbit/s	443	Scaleway – Online	AS12876
Dedibox Paris3	Saint-Ouen-l'Aumône	Île-de-France	IPv4 only	1 Gbit/s	443	Scaleway – Online	AS12876
SFR	Courbevoie	Île-de-France	IPv4 only	10 Gbit/s	80	SFR	AS15557
OVH 5GMARK	Roubaix	Hauts-de-France	IPv4 only	1 Gbit/s	443	OVH	AS16276
QoSi.eu	Roubaix	Hauts-de-France	IPv6 only*	1 Gbit/s	443	OVH	AS16276
AWS	Paris	Île-de-France	IPv6 only*	1 Gbit/s	443	Amazon Web Services	AS16509
Azure Akamai	multiple locations	multiple locations	IPv6 only*	1 or 10 Gbit/s**	443	Akamai International	AS20940
Ikoula	Reims	Grand-Est	IPv6 only*	1 Gbit/s	443	Ikoula	AS21409
Adeli	Saint-Trivier-sur-Moignans	Auvergne-Rhône-Alpes	IPv6 only*	1 Gbit/s	443	Adeli	AS43142
Mediactive Network	Paris	Île-de-France	IPv6 only*	10 Gbit/s	80	Mediactive Network	AS197133

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

** Depending on the Akamai content distribution solution used.

5. IPv6-TEST

Sponsor, as indicated on IPv6-test	City	Region or country	IPv6	Connection capacity	Port used	Hosting company	AS
LaFibre.info	Paris	Île-de-France	IPv4 and IPv6	10 Gbit/s	443 or 80	Bouygues Telecom	AS5410
OVH	Limbourg	Allemagne	IPv4 and IPv6	100 Mbit/s	443 or 80	OVH	AS16276
ZeelandNet	Zélande	Pays-Bas	IPv4 and IPv6	1 Gbit/s	80 only	ZeelandNet	AS15542
ServerHouse	Portsmouth	Royaume-Uni	IPv4 and IPv6	1 Gbit/s	81 only	ServerHouse	AS21472
EBOX	Longueuil	Canada	IPv4 and IPv6	1 Gbit/s	82 only	EBOX	AS174

6. OOKLA SPEEDTEST.NET

Sponsor, as indicated on Speedtest	City	Region	IPv6	Download connection capacity**	Upload connection capacity**	Port used	Hosting company	AS	ID***
fdcservers.net	Paris	Île-de-France	IPv4 only	2 Gbit/s	10 Gbit/s or +	8080	Cogent	AS174	6027
Orange	Lyon	Auvergne-Rhône-Alpes	IPv6 only*	10 Gbit/s or +	10 Gbit/s or +	8080	Orange	AS3215	24394
Orange	Rennes	Bretagne	IPv6 only*	10 Gbit/s or +	10 Gbit/s or +	8080	Orange	AS3215	23282
Orange	Strasbourg	Grand-Est	IPv6 only*	10 Gbit/s or +	10 Gbit/s or +	8080	Orange	AS3215	29543
Orange	Lille	Hauts-de-France	IPv6 only*	10 Gbit/s or +	10 Gbit/s or +	8080	Orange	AS3215	29544
Orange	Puteaux	Île-de-France	IPv6 only*	10 Gbit/s or +	10 Gbit/s or +	8080	Orange	AS3215	23884
Orange	Paris	Île-de-France	IPv6 only*	10 Gbit/s or +	10 Gbit/s or +	8080	Orange	AS3215	24215
Orange	Bordeaux	Nouvelle-Aquitaine	IPv6 only*	10 Gbit/s or +	10 Gbit/s or +	8080	Orange	AS3215	29542
Orange	Marseille	Région Sud	IPv6 only*	10 Gbit/s or +	10 Gbit/s or +	8080	Orange	AS3215	29545
GTT.net	Paris	Île-de-France	IPv4 only	4 Gbit/s	2 Gbit/s	8080	GTT	AS3257	24386
LaFibre.info	Lyon	Auvergne-Rhône-Alpes	IPv6 only*	10 Gbit/s or +	10 Gbit/s or +	8080	Bouygues Telecom	AS5410	2023
LaFibre.info	Douai	Hauts-de-France	IPv6 only*	10 Gbit/s or +	10 Gbit/s or +	8080	Bouygues Telecom	AS5410	4010
TestDebit.info	Massy	Île-de-France	IPv6 only*	10 Gbit/s or +	10 Gbit/s or +	8080	Bouygues Telecom	AS5410	2231
LaFibre.info	Bordeaux	Nouvelle-Aquitaine	IPv6 only*	10 Gbit/s or +	10 Gbit/s or +	8080	Bouygues Telecom	AS5410	21415
TestDebit.info	Marseille	Région Sud	IPv6 only*	10 Gbit/s or +	10 Gbit/s or +	8080	Bouygues Telecom	AS5410	4036
Sewan	Paris	Île-de-France	IPv4 only	10 Gbit/s or +	10 Gbit/s or +	8080	Sewan	AS8399	24130
Vialis	Colmar	Grand-Est	IPv4 only	6 Gbit/s	4 Gbit/s	8080	Vialis	AS12727	24059
ONLINE	Vitry-sur-Seine	Île-de-France	IPv4 only	10 Gbit/s or +	10 Gbit/s or +	8080	Scaleway – Online	AS12876	5022
Sirius Media Group	Paris	Île-de-France	IPv4 only	2,5 Gbit/s	2,5 Gbit/s	8080	Scaleway – Online	AS12876	10676
DFOX	Nice	Région Sud	IPv4 only	1 Gbit/s	1 Gbit/s	8080	Scaleway – Online	AS12876	8195
CCleaner	Paris	Île-de-France	IPv4 only	1 Gbit/s	1 Gbit/s	8080	Scaleway – Online	AS12876	16676
SFR	Lyon	Auvergne-Rhône-Alpes	IPv4 only	10 Gbit/s or +	10 Gbit/s	8080	SFR	AS15557	27852
SFR	Vénissieux	Auvergne-Rhône-Alpes	IPv4 only	10 Gbit/s or +	5 Gbit/s	8080	SFR	AS15557	30993
SFR	Trappes	Île-de-France	IPv4 only	10 Gbit/s or +	10 Gbit/s or +	8080	SFR	AS15557	31993

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

** Assumed connection capacity on the internet, outside the operator's network.

*** The ID is used to select the server with the Speedtest CLI command line interface app.

Sponsor, as indicated on Speedtest	City	Region	IPv6	Download connection capacity**	Upload connection capacity**	Port used	Hosting company	AS	ID***
SFR	Mitry	Île-de-France	IPv4 only	10 Gbit/s or +	10 Gbit/s or +	8080	SFR	AS15557	27984
SFR	Paris	Île-de-France	IPv4 only	10 Gbit/s	4 Gbit/s	8080	SFR	AS15557	12746
SFR	Bordeaux	Nouvelle-Aquitaine	IPv4 only	10 Gbit/s or +	5 Gbit/s	8080	SFR	AS15557	32438
Stella Telecom	Paris	Île-de-France	IPv4 only	1 Gbit/s	1 Gbit/s	8080	Stella Telecom	AS16211	26387
Stella Telecom	Courbevoie	Île-de-France	IPv4 only	1 Gbit/s	200 Mbit/s	8080	Stella Telecom	AS16211	14821
Rocho DataCenter	Chambéry	Auvergne-Rhône-Alpes	IPv6 only*	1 Gbit/s	1 Gbit/s	8080	OVH	AS16276	11457
OVH Cloud	Gravelines	Hauts-de-France	IPv6 only*	3 Gbit/s	10 Gbit/s or +	8080	OVH	AS16276	25985
ITDATA Telecom	Roubaix	Hauts-de-France	IPv4 only	500 Mbit/s	600 Mbit/s	8080	OVH	AS16276	29243
StreamRadio	Roubaix	Hauts-de-France	IPv4 only	200 Mbit/s	200 Mbit/s	8080	OVH	AS16276	32230
Ikoula	Reims	Grand-Est	IPv6 only*	1 Gbit/s	1 Gbit/s	8080	Ikoula	AS21409	5813
Axione	Paris	Île-de-France	IPv4 only	1 Gbit/s	4 Gbit/s	8080	Axione	AS31167	28308
Keyyo	Paris	Île-de-France	IPv4 only	10 Gbit/s or +	2 Gbit/s	8080	Keyyo	AS34659	27961
Hexanet	Reims	Grand-Est	IPv4 only	5 Gbit/s	5 Gbit/s	8080	Hexanet	AS34863	17225
Networth Telecom	Clichy	Île-de-France	IPv4 only	1 Gbit/s	1 Gbit/s	8080	Networth Telecom	AS35283	28073
Eurafibre	Lille	Hauts-de-France	IPv4 only	1 Gbit/s	10 Gbit/s or +	8080	Eurafibre	AS35625	16913
FullSave	Toulouse	Occitanie	IPv6 only*	10 Gbit/s	3 Gbit/s	8080	FullSave	AS39405	29032
Orne THD	Rombas	Grand-Est	IPv6 only*	2 Gbit/s	1 Gbit/s	8080	Orne THD	AS41114	17349
Enes Hag	Hagondange	Grand-Est	IPv4 only	1 Gbit/s	1 Gbit/s	8080	Vialis	AS42487	31081
Regivision	Nilvange	Grand-Est	IPv4 only	1 Gbit/s	1 Gbit/s	8080	Vialis	AS42487	31082
Enes	Hombourg-Haut	Grand-Est	IPv4 only	1 Gbit/s	1 Gbit/s	8080	Vialis	AS42487	21268
Fibragglo	Forbach	Grand-Est	IPv4 only	1 Gbit/s	1 Gbit/s	8080	Vialis	AS42487	16232
RIV54	Saulnes	Grand-Est	IPv4 only	1 Gbit/s	700 Mbit/s	8080	Vialis	AS42487	14372
Regie Talange	Talange	Grand-Est	IPv4 only	1 Gbit/s	1 Gbit/s	8080	Vialis	AS42487	16876
REFO Falck	Falck	Grand-Est	IPv4 only	1 Gbit/s	1 Gbit/s	8080	Vialis	AS42487	21216
Vialis	Woippy	Grand-Est	IPv4 only	1 Gbit/s	200 Mbit/s	8080	Vialis	AS42487	13661
Via Numérica	Archamps	Auvergne-Rhône-Alpes	IPv4 only	10 Gbit/s or +	2 Gbit/s	8080	Via Numérica	AS44494	3596
Naitways	Paris	Île-de-France	IPv4 only	10 Gbit/s or +	10 Gbit/s or +	8080	Naitways	AS57119	16476
ColocationIX 10G	Paris	Île-de-France	IPv4 only	10 Gbit/s or +	5 Gbit/s	8080	ColocationIX	AS61955	28994
HarryLafranc	Paris	Île-de-France	IPv4 only	1 Gbit/s	1 Gbit/s	8080	Netrix	AS62000	10176

Sponsor, as indicated on Speedtest	City	Region	IPv6	Download connection capacity**	Upload connection capacity**	Port used	Hosting company	AS	ID***
Mediactive	Paris	Île-de-France	IPv6 only*	10 Gbit/s or +	10 Gbit/s or +	8080	Mediactive	AS197133	31895
iBlooPro	Rennes	Bretagne	IPv4 only	10 Gbit/s or +	1 Gbit/s	8080	Blue Infra	AS201808	31656
Enes	Creutzwald	Grand-Est	IPv4 only	1 Gbit/s	1 Gbit/s	8080	ENES Creutzwald	AS204645	24052
Telerys	Paris	Île-de-France	IPv6 only*	10 Gbit/s or +	3 Gbit/s	8080	Telerys	AS205344	31725
Alpesys	Grenoble	Auvergne-Rhône-Alpes	IPv4 only	1 Gbit/s	700 Mbit/s	8080	Alpesys	AS206120	25041
AS208196	Paris	Île-de-France	IPv6 only*	1 Gbit/s	10 Gbit/s or +	8080	Dorian GALIANA	AS208196	32367
Tubeo	Bitche	Grand-Est	IPv4 only	1 Gbit/s	1 Gbit/s	8080	CC Pays de Bitche	AS208574	31083
La Regie	Reichshoffen	Grand-Est	IPv4 only	1 Gbit/s	1 Gbit/s	8080	La Regie Reichshoffen	AS208719	14043

This document was drafted by Arcep

Jean Cattan, *advisor to the Chairman*
Cécile Dubarry, *director-general*

DIRECTORATE FOR INTERNET, PRINT MEDIA, POSTAL AND USERS

Loïc Duflot, *director*

"Open Internet" unit
Aurore Tual, *head of unit*
Samih Souissi, *deputy head of unit*
Vivien Guéant and Emmanuel Leroux, *advisors*

"Data-driven regulation" unit
Pierre Dubreuil, *head of unit*

"Operators and legal obligations" unit
David Epelbaum, *head of unit*
Hélène Bartyzel, *advisor*

DIRECTORATE FOR ECONOMY, MARKETS AND DIGITAL AFFAIRS

Stéphane Lhermitte, *director*
Laurent Toustou, *advisor to the director*

"Economic analysis and digital intelligence" unit
Anaïs Aubert, *deputy head of unit*
Chiara Caccinelli, Arthur Dozias, Adrien Haïdar and Nisrynne Nahhal, *advisors*

DIRECTORATE FOR MOBILE AND INNOVATION

Anne Laurent, *director*
Maxime Forest, *deputy director*

"Mobile coverage and investments" unit
Guillaume Decorzent, *head of unit*
Audrey Goffi and Corentin Golly, *advisors*

DIRECTORATE FOR COMMUNICATIONS AND PARTNERSHIPS

Clémentine Beaumont, *director*
Anne-Lise Lucas, *advisor*

DIRECTORATE FOR LEGAL AFFAIRS

Elisabeth Suel, *director*

"Mobile market and scarce resources" unit
Aurore Martinat, *head of unit*
Annabel Gandar, *deputy head of unit*

"Infrastructures and open networks" unit
Rémy Maecker, *deputy head of unit*
Théotime Gélineau, *advisor*

Thank you...

All the people who were consulted, interviewed or who took part in Arcep's co-construction efforts devoted to Internet quality of service or to the IPv6 task force, for their energy and invaluable contribution to this report.

Publication
Arcep
14, rue Gerty d'Archimède – 75012 Paris
Directorate for communications
and partnerships: com@arcep.fr

Design
Agence Luciole

Translation
Gail Armstrong

Photos' credits
Pages 20, 30 and 79: Adobe Stock
Page 53: Ikoula

June 2020

NETWORKS AS A COMMON GOOD ARCEP MANIFESTO

Internet, fixed and mobile telecom, postal and print media distribution networks constitute the “Infrastructures of freedom”. Freedom of expression, freedom to communicate, freedom to access knowledge and to share it, but also freedom of enterprise and innovation, which are key to the country’s ability to compete on the global stage, to grow and provide jobs.

Because it is essential in all open, innovative and democratic societies to be able to enjoy these freedoms fully, national and European institutions work to ensure that these networks develop as a **“common good”**, regardless of their ownership structure, in other words that they meet high standards in terms of accessibility, universality, performance, neutrality, trustworthiness and fairness.

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

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

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

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