2022
EDITION

REPORT

The state of the Internet in France

TOME 3

arcep

French Republic - June 2022

2022 REPORT

The state of the Internet in France

arcep

Editorial

By Laure de La Raudière,
President of Arcep

ACHIEVING DIGITAL SUSTAINABILITY

Every act of our daily lives today plays out in a world where digital technology is ubiquitous.

This revolution in the ways the Internet is used has nevertheless given rise to new societal issues. The first challenge is of course guaranteeing superfast access for everyone and everywhere, so that nobody finds themself on the wrong side of the digital divide. These are the objectives of the National superfast access scheme and New Deal for Mobile, whose progress Arcep measures on a regular basis.

The second is guaranteeing inclusion in all of the daily uses of digital, so that no one will be excluded or disadvantaged by an insufficient mastery of digital tools.

The third, and by no means lesser, challenge is tackling the environmental impact of the explosion in new uses of digital technology.

The climate emergency that we are facing demands that we rethink, both individually and collectively, how we travel, consume, assess and choose.

This is further complicated by the fact that digital technology in fact has two opposite effects on the environment. On the one hand, digital can help reduce other sectors' carbon footprint: videoconferencing can reduce the need to travel; reducing inputs in farming thanks to the use of connected sensors; saving paper by storing documents digitally, etc.

On the other hand, the digital sector itself currently accounts for 2.5% of France's total carbon footprint, a figure that could rise to 7% (i.e. grow by 60%) between now and 2040, in particular due to the massive surge in the number of connected objects.

Aware of this challenge, Arcep has been taking a constructive approach to tackling these issues since 2019, to help inform the choices made by industry stakeholders, public policymakers and users.

After having published a report on "Achieving digital sustainability" in 2020, this commitment continued and deepened through a number of workshops and workstreams. In October 2021, Arcep hosted a webinar for all of the associations, institutions, operators, tech companies and experts who helped author this report, to deliver a state of the art. An event that gave me the opportunity to reaffirm Arcep's ambition of reconciling the growing use of digital tech and reducing its environmental footprint.

In 2022, thanks to data collected from operators in 2020 and 2021, Arcep published the first edition of its "Achieving digital sustainability" annual survey. Analyses of these data revealed several preliminary findings, including: mobile networks consume twice as much energy as fixed ones, and fiber networks consume four times less energy per subscriber than copper ones.

The Act of 23 December 2021 aimed at reinforcing environmental regulation of the digital sector expands Arcep's data collection powers to include other digital sector players (data centers, device manufacturers, etc.) which will enable us to enhance future editions of our annual survey.

Arcep has also been a driving force on environmental issues since 2020 within the Body for European Regulators for Electronic Communications (BEREC), and is co-chair of the "Sustainability" working group. It was thanks to this action that, on 16 March of this year, BEREC presented its draft report on "Environmental sustainability," and invited stakeholders to contribute to the resulting public consultation.

Among the many other challenges to arise from the digital revolution is the omnipresence of Big Tech. These companies have the power to determine what content and services can be made available online, and the conditions under which users can access them. Arcep has been warning for several years about the role of gatekeepers, to the Internet and beyond, enjoyed by a small handful of Big Tech companies, and the need to regulate them.

"Reconciling the growing use of digital tech and reducing its environmental footprint"

4

This is why Arcep has been so deeply involved, notably within BEREC, in contributing to the work done on Europe's Digital Markets Act. The Authority welcomes its recent adoption, and the ability it creates to establish *ex ante* obligations for digital gatekeepers.

More than ever, Arcep and its teams are working to ensure that users have high quality Internet access, and to provide them with all available and reliable information, notably on the digital environmental footprint.

Table of contents

2021 ARCEP HIGHLIGHTS

23 FEBRUARY

Environment

The Government's "Digital and the Environment" roadmap tasks the Authority with producing a report on mobile device replacement and examining ways for taking environmental considerations into account when awarding 26 GHz band frequencies.
It reaffirms Arcep's role in working to achieve digital sustainability with the ADEME/Arcep report on measuring the sector's environmental footprint (Parts 1 and 2 published in January 2022) and the creation of a Environmental Barometer.

SPRING

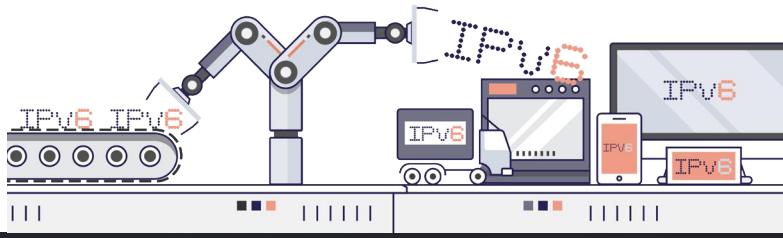
Regulating platforms

Within the Body of European Regulators for Electronic Communications (BEREC), Arcep hosts and moderates two workshops on the Digital Markets Act (DMA) with high-level representatives of the European Commission, the European MP serving as the DMA rapporteur, along with a panel of experts, and representatives of rival platforms, business users, consumer associations and civil society. Around 250 participants are in attendance.

19 MAY

Transition to IPv6

The Body of European Regulators for Electronic Communications (BEREC) hosts a public workshop on IPv6 deployment in Europe. An opportunity to show the tremendous disparities in IPv6 adoption levels across Europe, and why it is so important to accelerate the transition, to achieve better connectivity, to future-proof digital markets and keep them open, and to empower end users.



7 JULY

Internet quality of service

Upon the publication of its report on the State of the Internet in France, Arcep publishes the list of players involved in QoS testing that have declared themselves compliant with the Code of conduct on Internet quality of service that Arcep published in 2020.

12 JULY

Environment

Arcep submits a report to the Government on how smartphone distribution models influence their replacement rate.

17 JULY

Internet quality of service

The top four operators in France present Arcep with the design for their boxes with the "Access ID card" API installed, in accordance with Arcep Decision No. 2019-1410.

2 SEPTEMBER

Open Internet

The Court of Justice of the European Union hands down three decisions providing an interpretation of zero-rating practices' compliance with the Open Internet Regulation.

30 SEPTEMBER

Regulating platforms

BEREC publishes proposals on the *ex ante* regulation of so-called "gatekeeper" platforms in a report, with the goal of promoting competition between platforms, protecting the interests of end users, treating identified issues in a proportionate and tailored fashion, and ensuring the regulation's efficient implementation through a system of reinforced oversight. These proposals are submitted to public consultation, and are met largely with support from the different stakeholders.

SEPTEMBER

Open Internet

Arcep participates in the review of BEREC guidelines, following the rulings from Court of Justice of the European Union. The new guidelines are published in June 2022.

SEPTEMBER TO DECEMBER

Mobile quality of service

Arcep conducts its 2021 mobile quality of service audit in the French overseas departments and territories, performing more than 400,000 tests in Guadeloupe, Guiana, Martinique, Mayotte, Réunion, Saint-Barthélemy and Saint-Martin, on the services of some dozen operators in all. The findings were published in March 2022.

4 OCTOBER

Environment

Arcep hosts a webinar for its “Achieving digital sustainability” platform participants. Invited to this status update: associations, institutions, operators, tech companies and experts.

19 NOVEMBER

Mobile quality of service

Arcep publishes the findings of its 2021 QoS audit: a significant improvement in mobile Internet quality of service, with 2G/3G/4G downlink speeds reaching an average 71 Mbit/s, and in web browsing and streaming performances, with especially noticeable progress in rural areas. Arcep performs QoS tests on 5G plans and handsets for the first time.

29 NOVEMBER

Transition to IPv6

Arcep posts the 2021 edition of the Barometer of the transition to IPv6: France has risen in the global and European IPv6 adoption rate rankings. Arcep also publishes the second handbook from the IPv6 task force: “A business’s guide to the IPv6 transition”.

23 DECEMBER

Environment

The Act on strengthening environmental regulation of the digital sector by Arcep is adopted. It expands Arcep’s environmental data collection powers to include a range of stakeholders: device manufacturers, CAP, operating system providers, data center operators and network equipment suppliers.

LATE 2021

Data interconnection

Thanks to its regular information gathering on data interconnection and routing, Arcep publishes an update of its Barometer of interconnection in France.

LATE 2021

Open Internet

In 2021, the Wehe app that Arcep has made available to users to detect Internet traffic throttling and port blocking has been used more than 144,000 times, and 295 net neutrality-related reports were sent to Arcep via the “J’alerte l’Arcep” platform.

PART 1

Ensuring the Internet functions properly

CHAPTER 1

IMPROVING INTERNET QUALITY OF SERVICE MEASUREMENT

What you need to know

In summer 2022, operators will have deployed the **"Access ID card" API** in almost all the recent boxes.

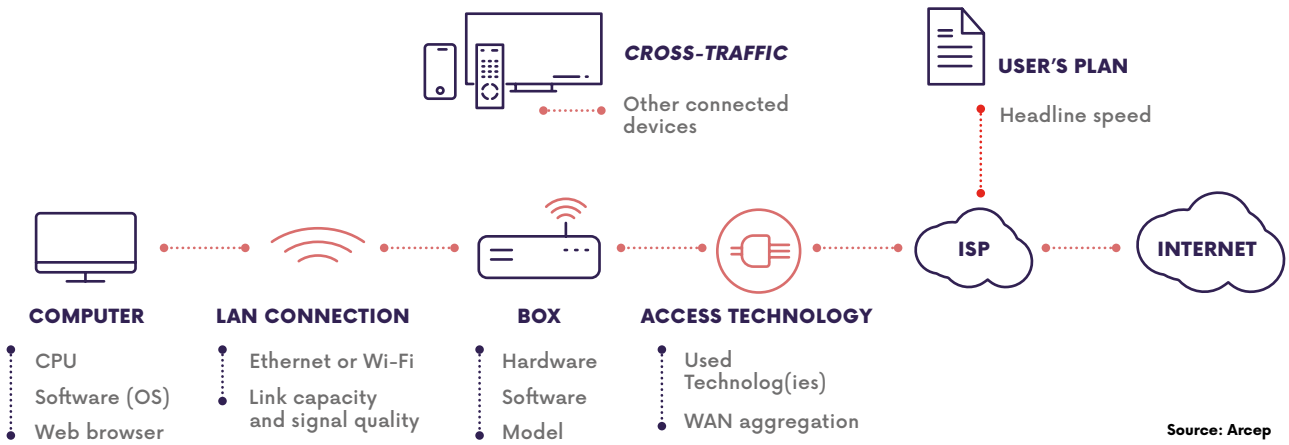
19 testing tools have declared themselves compliant with the 2020 version of the Code of conduct on Internet quality of service.

The quality of mobile data services improved significantly again this year: average speeds in Metropolitan France reached **71 Mbit/s** in 2021.

Internet quality of service depends, first, on infrastructures' ability to provide increasingly high speeds, notably by deploying fiber on fixed networks and 4G and 5G technologies on mobile. To empower users to make informed choices about their operator, Arcep created the "Ma connexion Internet" (My Internet connection) tool which allows them to see the technologies and speeds available at any given address in France.

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.

CARACTERISTICS 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 server'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

2.1. Presentation of the "access ID card" API

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, fiber, etc.) being used on the tested line. This lack of user environment characterisation 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 approach[1] 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 access boxes to transmit the information that make up the "Access ID card".

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 overall quality of their Internet connection. 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.

From July 2022, the API will be implemented and activated in the following boxes:

- **Bouygues Telecom:**
  - Bbox Wi-Fi 6E FttH (*Bbox F@st 5688b-v2*) starting in September 2022
  - Bbox Wi-Fi 6 FttH (*Bbox F@st 5688b*)
  - Bbox Wi-Fi 5 FttH /xDSL (*Bbox F@st 5330b-r1*)
  - Bbox Wi-Fi 4 FttH /xDSL (*Bbox F@st 5330b*)
- **Free:**
  - Freebox Pop FttH /xDSL (Wi-Fi 5)
  - Freebox Delta FttH /xDSL (Wi-Fi 5)
  - Freebox One FttH /xDSL (Wi-Fi 5)
  - Freebox mini 4K FttH /xDSL (Wi-Fi 5)
  - Freebox Révolution r3 FttH /xDSL (Wi-Fi 5)
  - Freebox Révolution r2 FttH /xDSL (Wi-Fi 4)
  - Freebox Révolution r1 FttH /xDSL (Wi-Fi 4)
- **Orange:**
  - Livebox v6 FttH (Wi-Fi 6E)
  - Livebox v5 FttH (Wi-Fi 5)
  - Livebox v4 FttH /xDSL (Wi-Fi 5)
- **SFR:**
  - SFR Box 8X Wi-Fi 6 FttH XGS-PON (*NB8 XGSPON*)
  - SFR Box 8 Wi-Fi 6 FttH GPON (*NB8 FTTH*)
  - SFR Box 8 Wi-Fi 6 Docsis (*NB8 Docsis*)
  - SFR Box 8 Wi-Fi 6 xDSL (*NB8 xDSL*)
  - Box Plus or "SFR Box 7" Wi-Fi 5 FttH /xDSL (*NB6VAC*)
  - Modem THD AC Wi-Fi 5 Docsis (*F@st 3686*)
  - La Box THD 4K or "La Box Fibre Zive" Wi-Fi 5 Docsis (*La Box V3*)
  - La Box THD V2 or "La Box by Numericable V2" Wi-Fi 5 Docsis (*La Box V2*)
  - Box Évolution VDSL or "Neufbox 6V" Wi-Fi 4 FttH /xDSL (*NB6V et NB6V2*)
  - Box Évolution or "Neufbox 6" Wi-Fi 4 FttH /ADSL (*NB6*)

The updated list of boxes that are compatible with the API of is available on Arcep website.

Arcep encourages implementation of the API by operators that are not subject to the Decision (operators with fewer than a million customers, business market operators, etc.).

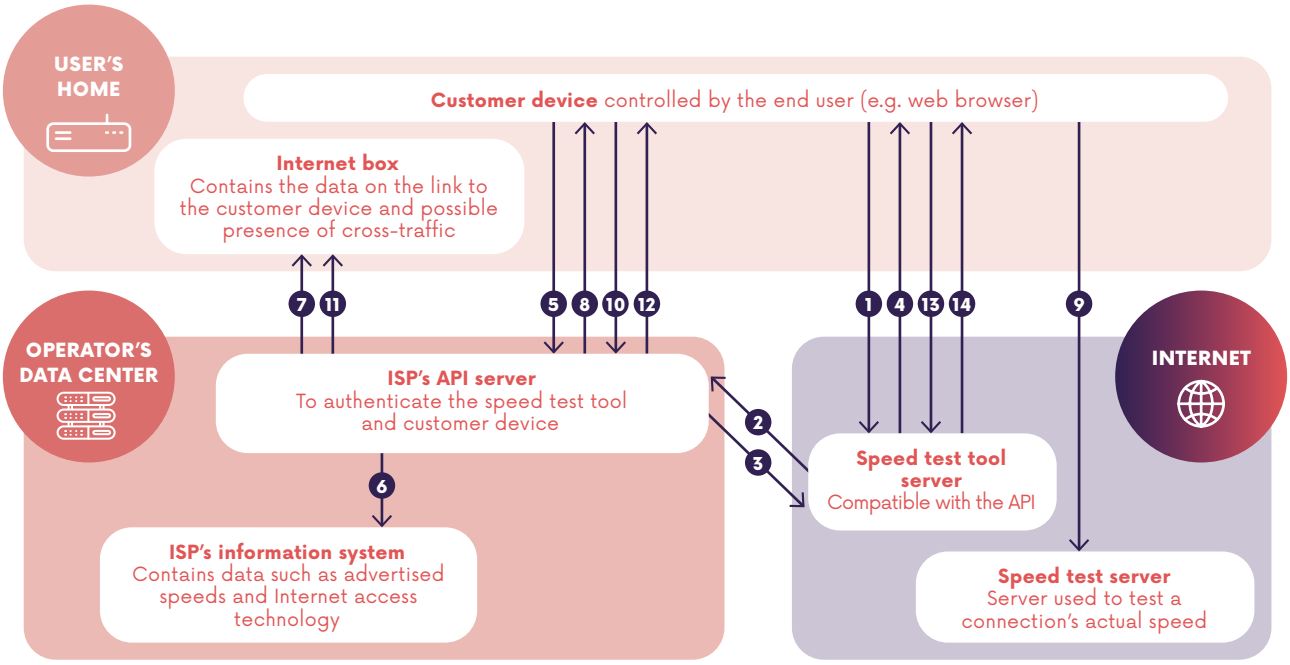
The API's operating rules take users' privacy protection concerns and demands fully into account. First, the data collected by the API are not transmitted to Arcep. The API will not transmit any information on the user's identity (user ID, name, location, etc.) to the measurement tools, thereby ensuring 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.

1. Description of the API co-construction process. Click here.
2. 2020 edition of the quality of service Code of conduct. Click here.

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.

HOW THE "ACCESS ID CARD" API WORKS



1. The user goes to a website to test their line's speed and authorises an API call
2. The speed test tool authenticates itself and requests a token from the ISP, authorising the user to query the API
3. The ISP delivers a token to the tool, which enables the customer device to query the API, while limiting the request to the customer's IP address and to only a few minutes
4. The customer device collect the token from the tool
5. The user's browser software connects to its ISP's API, which checks the token's validity
6. The API queries the information system to retrieve some of the data
7. The API queries the user's box, to retrieve the rest of the data
8. The data from the API are sent to the user device
9. The user's browser software launches the speed test on a test target: a server dedicated to this purpose
10. The user's browser software connects to the API for the second call, to check whether there was cross-traffic on the line
11. The API queries the user's box, to retrieve cross-traffic data
12. Data from the API's second call are sent to the user device
13. The user's browser software transmits the speed test results and API data to the speed test tool's server
14. The tool delivers the enhanced information to the user

Source: Arcep

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. Two calls are made to the API: the first right before the test and the second right after. The purpose of these calls is to retrieve the different indicators to be able to characterise the link between the user device and the Internet, while ensuring there was no cross-traffic, in other words traffic other than what was being tested (e.g. traffic from another PC or smartphone, TV box or another test programme on the computer). To achieve this, the testing tool will compare the quantity of data that it sent and received on the Internet and the quantity of data that was transmitted on the Internet by the box, between the API's first and second call.

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.

Is the API accessible from the Internet?

No, the API can only be accessed from the end user's local network. The API's call must be made on the ISP's server from the customer's IP address. Requests from other IP addresses will be rejected, to ensure the system's security. It is therefore only the tool used to run the test on the customer's device that can call the API. 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 ID Card API will be implemented and activated in almost all the boxes concerned by Arcep's decision.

API DEPLOYMENT SCHEDULE

Source: Arcep

2.2. Co-construction work continues within the API supervising committee

Since publishing its decision, Arcep has met regularly with operators and measurement tools within a supervising committee for the development of the API, to establish the specifications. Five working groups were created to this end:

1. API implementation methods (architecture, authorisation mechanisms, etc.);
2. Definition of the API access process for testing tools;
3. API design;
4. Quality of the data supplied by the API;
5. Implementing GDPR and ePrivacy rules.

The API supervising committee will continue to meet to monitor the API's launch with the testing tools. Talks could also continue on improving the information provided to users and the publications of aggregate data enabled by the API.

3. Achieving even more transparent and robust measurement methodologies

3.1. Presentation of Arcep's 2020 Code of conduct

In addition to the characteristics of the user environment, testing methodologies too have a tremendous influence on QoS test results. Indeed, it is equally vital to have a clear understanding of the kind of tests these tools perform and of their limitations, but also of how their findings are presented, so that users can conduct these tests under the best possible conditions, and properly interpret the results.

In 2017, Arcep identified the need for greater transparency on measurement methodologies. In December 2018, it published a Code of conduct for stakeholders involved in quality of service measurement[3].

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 co-construction approach taken to drafting the 2018 Code of conduct continued to be used to produce this new version. To this end, Arcep hosted a series of bilateral and multilateral meetings with some twenty stakeholders, including the publishers of crowdsourcing testing and measurement tools, consumer protection organisations, operators and members of academia. The 2020 Code of conduct is the fruit of this work[4]. This updated Code of conduct keeps the same two-part structure as the 2018 version:

- 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, as well as the other tests the tool offers, and the information that it provides to end users;
- the second part concerns aggregate data 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.

3. 2018 edition of the Code of conduct on Internet quality of service. Click here.
4. 2020 edition of the Code of conduct on Internet quality of service. Click here.

Several aspects have been strengthened in the new version of the Code of conduct, to provide the QoS measurement ecosystem with ongoing support to continue to develop their knowledge and abilities. In particular, QoS testing and measuring tools are being required to:

- provide users with information on the different factors that might affect the measurement, such as the use of and properties of Wi-Fi, and the model and version of their operating system and web browser, all of which can have a considerable influence on quality of service measurement;
- display a median value for certain parameters, notably latency. This information is more relevant than averages in reflecting the user experience, particularly in cases where the measured results contain extreme values;
- introduce a minimum capacity for test servers, to ensure that the servers will not hamper testing;
- specify the capacity for test servers conducting tests in IPv6, as the protocol used can impact the outcome of speed tests.

This Code of conduct also underscores a number of potential sources of bias that must be made clear in measurement and testing tools' aggregate publications. Lastly, it takes greater account of the specific considerations when measuring Internet quality of service on mobile networks.

3.2. Tools compliant with 2020 edition of the Code of conduct

Arcep published a new version edition of the quality of service Code of conduct on 14 September 2020, and by early 2021 several tools had already declared themselves in compliance. The tools that were already compliant with the 2018 version have renewed their declaration of compliance, and new tools have expressed their interest in joining Arcep's co-construction approach.

Tools that declared themselves to be in compliance with the 2020 edition of the Code of conduct

The tools for measuring fixed Internet quality of service that declared themselves to be in compliance with the 2020 version of the Code of conduct on Internet quality of service are:

- 5GMark, developed by QoSi (Mozark group);
- DébiTest 60, the connection tester from *60 Millions de consommateurs* developed by QoSi (Mozark group);
- IPv6-test: the IPv4 and IPv6 QoS test, developed by IPv6-test;
- nPerf, developed by nPerf;
- Speedtest UFC-Que Choisir, developed by UFC-Que Choisir;
- Speedtest, developed by Ookla*;
- TestADSL.net, developed by SpeedChecker*.

The tools for measuring mobile Internet quality of service which have declared themselves to be in compliance with the 2020 version of the Code of conduct on Internet quality of service are:

- 5GMark, developed by QoSi (Mozark group);
- DébiTest 60, the connection tester from *60 Millions de consommateurs* developed by QoSi (Mozark group);
- Gigalis: the connection tester from the region *Pays de la Loire*, developed by QoSi (Mozark group)*;
- KiCapte: the connection tester from the department *Ille-et-Vilaine*, developed by QoSi (Mozark group)*;
- nPerf, developed by nPerf;
- QuelDébit: the connection tester from the association *UFC-Que Choisir*, developed by QoSi (Mozark group)*;
- Speedtest, developed by Ookla*;
- Tadurezo: the connection tester from the region *Bourgogne-Franche-Comté*, developed by QoSi (Mozark group)*;
- Tu Captes ?: the connection tester from the region *Hauts-de-France* and the Departments of the *Aisne, Nord, Oise, Pas-de-Calais* and *Somme*, developed by QoSi (Mozark group)*;
- The crowdsourcing tool Tutela, developed by Tutela*.

Although they do not offer testing solutions aimed at end users, the following tools also declared themselves in compliance with the Code of conduct:

- Whitebox probes developed by SamKnows*;
- The Eyes'ON solution developed by SoftAtHome*.

Other speed test tools do exist, but have not yet been declared compliant with the 2020 Code of conduct. The updated list of tools that declared themselves to be in compliance with the Code of conduct is available on Arcep website.

* Tools that were not declared compliant with the 2018 edition, but have been declared compliant with the 2020 edition of Code of conduct on Internet quality of service.

3.3. Towards a new version of the Code of conduct

As indicated when it was published, the 2020 edition of the Code of conduct on Internet quality of service was due to evolve once again with the introduction of the "Access ID card" API.

Arcep thus relaunched a workstream with all of the stakeholders involved in measuring QoS (ISPs, testing tools, consumer protection organisations and academics). The goal is to improve the accuracy and reliability of QoS testing, by working to strengthen the new version of Code of conduct on several fronts.

Below are a few examples of the topics explored during the work carried out on this new version of the Code of conduct:

- The need for the QoS testing tools to display the data delivered by the API, notably headline speed, LAN speed, etc. in addition to the test results;
- Whether to increase the minimum percentage of test servers that are IPv6-compatible;
- Whether to factor in the data sent by the API during the data's post-processing and aggregation process:
  - Deletion of individual tests when Wi-Fi is the limiting factor or when there is cross-traffic;
  - Definition of several categories of aggregation, notably by technology (xDSL, cable, FttH);
- The need to publish information that is more specific to the user on factors that can introduce bias.

Arcep will invite testing and measurement tools wanting to declare themselves compliant with this new version of the Code of conduct to do so, and will publish a list of the players involved in testing that have declared themselves compliant with this new version.

Taking the features provided by the "Access ID card" API into account should also help increase the accuracy not only of QoS tests but also of testing tools' aggregate data publications. Naturally, these changes will be made in concert with stakeholders.

Work done by BEREC: Supporting NRAs in the implementation of measurement tools and updating the QoS testing methodology

The tool developed by BEREC is an open-source tool for measuring Internet quality of service which is available on Git Hub: https://github.com/net-neutrality-tools/nntool. This tool is made available to national regulatory authorities (NRAs) in the different Member States, who are free to adopt it or not.

BEREC created a working party to coordinate the different national projects devoted to the quality of service measuring tools that have been created. In addition to providing experts with a forum for discussion and sharing experiences and best practices, BEREC will also catalogue all of the national initiatives and monitor European NRAs' different projects to develop new tools.

Furthermore, in December 2021 BEREC launched a public consultation on updating the QoS measurement methodology recommended by BEREC in 2017 (BoR (17) 178). This update seeks to take the latest technological developments into account, specifically for quality of service measurement indicators, and speed in particular. This update will also draw on the guidelines that BEREC published in 2020, detailing the quality of service parameters (BoR (20) 53). A report on the methodology will be published by mid-2022, and could help inform the next edition of Arcep's Code of conduct.

From a more general perspective, the work done within BEREC should facilitate the adoption of a measurement tool that could eventually become a diagnostic tool for Arcep, in the areas of quality of service and net neutrality.

4. Importance of choosing the right test servers

The choice of test servers – i.e. the server that the QoS testing 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 server'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 a throughput of only 1 Gbit/s.

The 2020 Code of conduct already set a minimum capacity of 1 Gbit/s for test servers, along with a set of 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.

4.2. Impact of test servers' congestion-avoidance algorithm

The results of QoS and speed tests also depend on the test servers' technical characteristics, and notably their congestion-avoidance algorithms. These algorithms are used on the data transmission side to decide packet transmission speed. There are multiple congestion-avoidance algorithms, and these algorithms evolve over time. Today, most of the Internet uses Cubic, created in 2006, which relies on packet loss as the signal to reduce speed. Cubic remains the default TCP implementation in Linux, Android and MacOS.

In 2016, Google developed the BBR (Bottleneck Bandwidth and Round-trip propagation time) congestion-avoidance algorithms that use a different model based on maximum bandwidth and round-trip time. This approach gives BBR the ability to provide faster speeds and lower latency than algorithms like Cubic, based on packet loss. Some of the top Internet companies are starting to deploy BBR on their services, notably on HTTP/3-compatible servers (i.e. the new, third generation HTTP standard).

Some test servers use Cubic and others BBR, while still others use a different congestion-avoidance algorithm, which means that the speed test performed with the latter will not be representative of Internet use.

The Code of conduct invites all testing tools to indicate which congestion-avoidance algorithm their different test servers use, as the speed that is measured can differ depending on the algorithm employed, especially if packet loss is frequent.

4.3. 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. Aside from the latency tied to the access technology, most of the route travelled between a customer and a server is over optical fiber. The round-trip latency is around 1.2ms per 100 Km of optical fiber[5].

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 server can be in different locations:

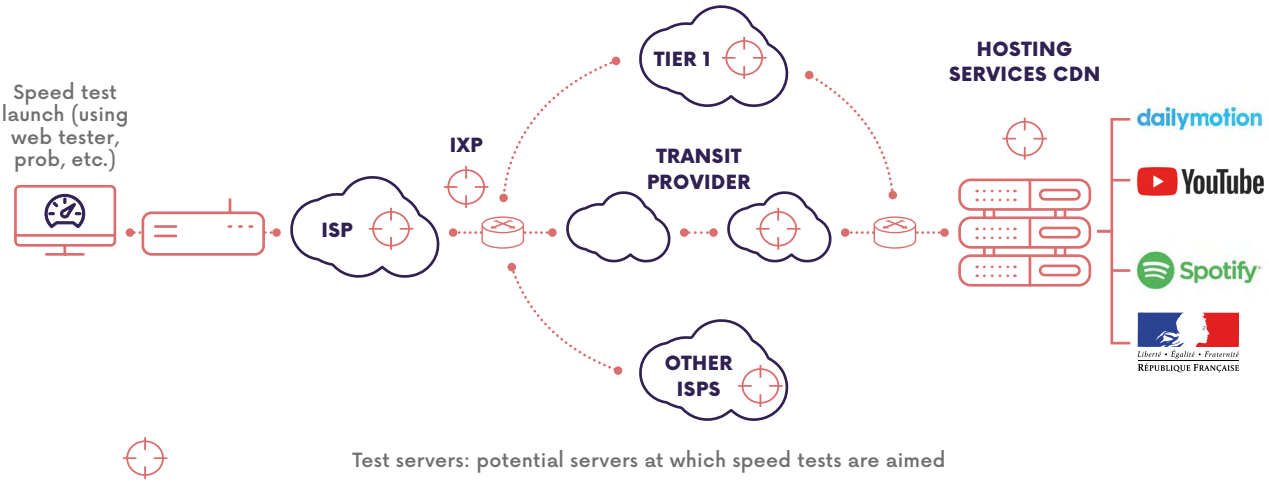
- on the user's ISP's network: the results of the test depend only on the ISP but it is not terribly representative of the actual experience of using Internet services, which are often hosted outside this simple network;
- on another ISP's network directly interconnected (via peering) with the user's 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 entirely 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 only represent quality of service towards a specific point on the Internet;
- on a Tier 1 network[6]: 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 servers 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.

5. The speed of light in a silica core is 200,000,000 m/s, or 5 microseconds per km, to which must be added the latency introduced by the chromatic dispersion compensation coils, when they are present, which create an additional distance of 1/7th. New generation WDM equipment (100 Gb/s class-coherent) no longer requires chromatic dispersion compensation coils.

6. See lexicon.

THE TEST SERVER'S LOCATION: A CHOICE THAT HEAVILY IMPACTS RESULTS



Source: Arcep

5. Technical parameters that influence speed

On the Internet, a server transmitting data has no knowledge of the speeds available end to end. Despite which, it is fundamental that the right quantity of data be transmitted: sending them at too high a speed runs the risk of overloading a low-speed connection. Sending too few would make inefficient use of fiber connections' bandwidth. A congestion avoidance algorithm is therefore used to estimate the capacity of the link between server and client, based on latency and packet loss. Algorithm, latency and packet loss are three crucial factors to ensure the availability of a decent speed.

5.1 Latency

Latency is the time it takes for information travel from one point on the network to another. Latency is shaped by three factors:

- **Latency tied to the length of optical fiber.** The speed of light in a silica core is 200,000,000 m/s, or 5 microseconds per km of optical fiber. This figure must be doubled to calculate the round trip. To which must be added:
  - 5% for coiled lengths (excess cable stored in coils) in the different telecoms installations;
  - 1/7th additional latency if the fiber is equipped with coils of chromatic dispersion compensation fiber.

This gives a round-trip latency of exactly 1.2 milliseconds for 100 km of optical fiber. N.B.: the optical fibre used does not typically go in a straight line, unlike a microwave link.

- **Latency tied to the Internet access technology.** Below is the typical additional latency by technology:
  - FttH fiber (GPON, XGS-PON or 10G-Epon technologies): < 1 millisecond;
  - Cable network (Docsis 3.0): between 6 and 7 milliseconds;
  - 4G mobile network: between 15 and 30 milliseconds;
  - 3G mobile network: between 25 and 50 milliseconds;
  - Copper network (xDSL technologies): between 5 and 45 milliseconds depending on the interleaving[7] configuration. Removing the interleave will enable low latency, but the line is no longer protected, and a large amount of packet loss (CRC errors) will damage the connection. A 16 millisecond interleave delay will protect the line against impulse noise, but will generate an additional latency of 32 milliseconds (16ms there + 16ms back). Noisy lines require greater protection. Some operators give customers the ability to choose their level of protection.
- **Latency tied to buffers, notably when there is congestion.** When a link receives more data than it can process, the excess packets awaiting transmission are stored in a buffer memory. When the buffer is full, any additional incoming packets are deleted. Setting the size of buffers on telecom equipment is a complex operation:
  - If the buffer is too small, packets will be quickly deleted without the congestion avoidance algorithm having time to determine available capacity on the link. Speeds will therefore be abnormally low.
  - If the buffer is too big, the congestion avoidance algorithm might not compute that the link is saturated. And it will only begin to take corrective measures (lowering transmission speed) once the buffer memory begins to overflow, and packets are deleted. Taking the example of a one-second buffer, all of the packets will need to wait one second before being relayed over the congested link: buffers use the First In First Out (FIFO) rule. Large data transfers and video streaming will be little affected by this significant latency, whereas interactive applications (loading

7. See lexicon.

web pages, network gaming, remote control of an apparatus, etc.) will be slowed considerably, if not rendered inoperable. This abnormally high latency caused by excess buffering of packets is called bufferbloat.

The right size buffer is therefore the smallest that will allow the congestion avoidance algorithm to understand the link's speed limit. For a high-capacity link aggregating the connections of thousands of users, a buffer must contain only the absolute minimum of data to be able to fill the link during saturation. If the number of bytes in the buffer never dips below a certain threshold, it means the buffer can be reduced by that much. This maintains performance while reducing latency caused by bufferbloat as much as possible.

5.2 Packet loss

Packet loss occurs when packets do not reach their destination. Loss is expressed in the percentage of packets lost compared to the number sent. The two causes of packet loss are:

- **An unreliable network** which can lead to packet loss. This is especially true of wireless networks (Wi-Fi, 4G, 5G, etc.) which are sensitive to radio interference. Interference or an overly weakened signal can result in the corruption or loss of packets in transit. Packet loss is measured by BER (Bit Error Rate). Packet loss is normal on a Wi-Fi network: 0.1% is a typically acceptable loss rate. An ADSL connection may also lose packets if the line is noisy and interleaving delays reduced. A network's unreliability can also be due to damaged equipment, a software bug or poor quality cable.
- **Network congestion** can also result in packet loss. Once the buffer memory is full, any additional incoming packets will be deleted. This is a healthy mechanism for handling congestion, as storing too many packets in the buffer will cause bufferbloat.

5.3 Congestion avoidance algorithms

Cubic and BBR are the most widely use congestion avoidance algorithms on servers.

- **Cubic:** most Internet services today use Cubic. Created in 2006, it uses packet loss as the signal to reduce speed. Cubic is the congestion avoidance algorithm used by default in Linux (which runs most of the Internet's servers) as well as Android and macOS.
- **BBR:** in 2016 Google developed BBR (Bottleneck Bandwidth and Round-trip propagation time) which uses a different model, based on maximum bandwidth and round-trip time. When there is packet loss on a connection, this approach enables BBR to deliver significantly higher speeds than those provided by packet loss-based algorithms like Cubic. Today, some of the top Internet companies are starting to deploy BBR on their servers. But BBR has not yet been widely adopted online, largely due to RTT fairness issues. On a link where bandwidth is shared between users (e.g. mobile network frequencies or a fiber link) BBR connections will "take the place" of Cubic connections. BBR v2 is currently being developed to improve the current version and achieve better cohabitation with Cubic.

How latency, packet loss and the congestion control protocol affect speed

Test protocol

The following tests were conducted in a laboratory. A server, installed for this purpose is dedicated to the tests and connected directly to its client by a two-metre 1 Gbit/s Ethernet cable. Latency and packet loss are added using NetEm software, integrated into the Linux kernel. The protocol used is the one employed by Arcep's mobile QoS audits: a 250 MiB file is downloaded over HTTPS. The test stops once the 250 MiB are reached or when 10 seconds have elapsed. The test server settings are contained in the following document: server configuration for Arcep 2022 mobile QoS audit[2]. To ensure the reliability of the results, each test is carried out several hundred times. In total, more than 58,000 tests[3] were conducted.

1. MiB = a mebibyte which is equal to 1024 KiB (Kibibytes) = 1024 x 1024 or 1,048,576 bytes. A Mb (megabyte) equals 1000 Kb or 1,000,000 bytes.
2. One exception: the version of Ubuntu used is Ubuntu server 22.04 LTS.
3. Details of the tests conducted (OpenDocument file, can be read with spreadsheet software).

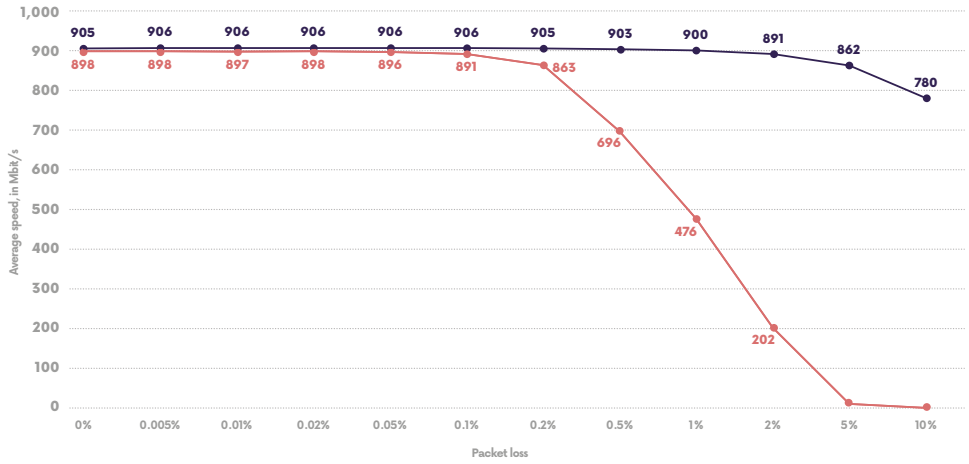
Speed depending on packet loss for round-trip latency of 1 millisecond

This extremely low latency is found chiefly in business settings, when customers and servers are in the same location.

Note that with the Cubic congestion avoidance algorithm speeds decrease far more significantly than with BBR, starting at 0.2% packet loss.

Round-trip latency of 1 ms: speed depending on packet loss

Typical situation: internal enterprise network (customer and server in same location)
Congestion avoidance algorithm: ● BBR ● Cubic



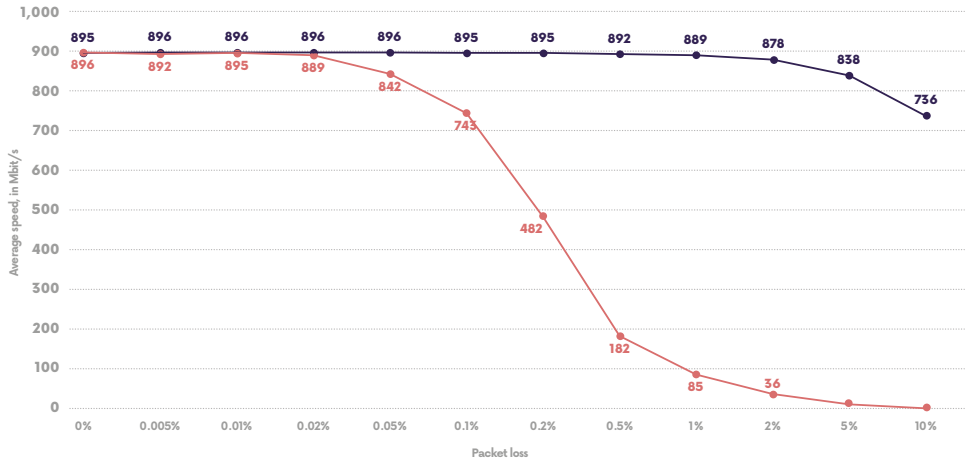
Speed depending on packet loss for round-trip latency of 4 milliseconds

This level of latency is found chiefly on FttH networks, when customer and server are in the same region, and the customer is on the same network as the server (or peering between the two networks also takes place in the region – this applies mainly to Parisian users using a Parisian server, with peering in the Paris region).

Note that with the Cubic congestion avoidance algorithm speeds decrease much more significantly than with BBR, starting at 0.05% packet loss, and drops below 100 Mbit/s when packet loss exceeds 1%.

Round-trip latency of 4 ms: speed depending on packet loss

Typical situation: fiber connection with server very close by (customer and server in the same region, local peering) Congestion avoidance algorithm: ● BBR ● Cubic



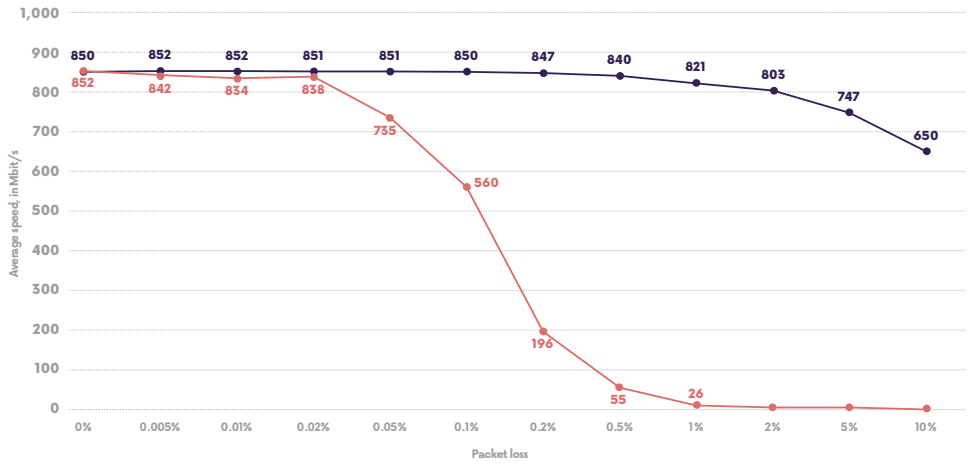
Speed depending on packet loss for round-trip latency of 16 milliseconds

This level of latency is found chiefly on FttH networks, when customer and server cross several regions. For instance, latency can be 16 milliseconds for a customer in the Auvergne-Rhône-Alpes region using a server located near their home, if the server's network is interconnected with the customer's network in Paris. The route taken can be: "customer" => "Lyon (customer network)" => "Paris (customer network)" => "point of peering" => "Paris (server network)" => "Lyon (server network)" => "Server".

Note that with the Cubic congestion avoidance algorithm speeds decrease more significantly than with BBR, starting at 0.05% packet loss. Speeds with 0.5% packet loss max out at 55 Mbit/s with Cubic, compared to 840 Mbit/s with BBR.

Round-trip latency of 16 ms: speed depending on packet loss

Typical situation: fiber connection with nearby server (optical signal travelling across several regions)
Congestion avoidance algorithm: ● BBR ● Cubic



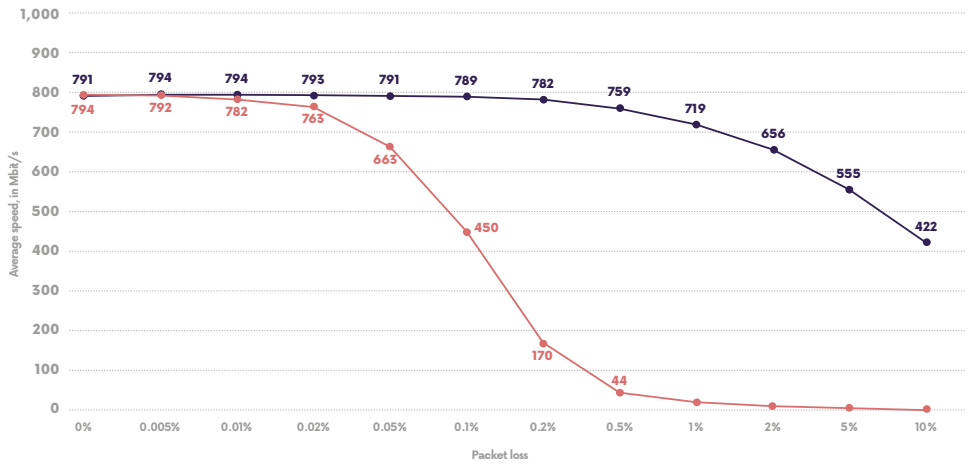
Speed depending on packet loss for round-trip latency of 32 milliseconds

This level of latency is found chiefly on 4G networks with a nearby server, or on FttH networks when the server is located outside of France (but still in Europe).

Speeds with 0.5% packet loss max out at 44 Mbit/s with Cubic, compared to 759 Mbit/s with BBR.

Round-trip latency of 32 ms: speed depending on packet loss

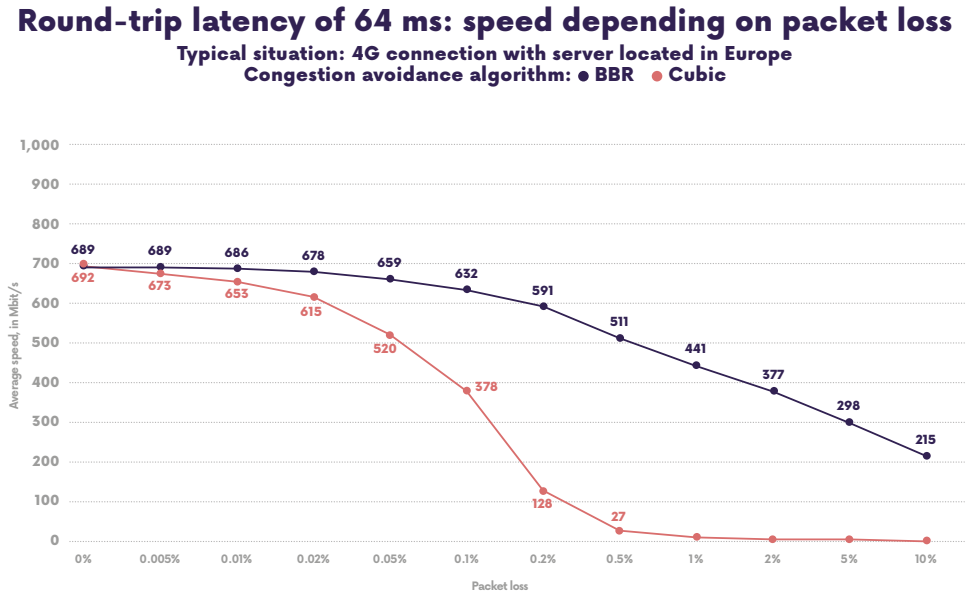
Typical situation: fiber connection (server located in Europe)/4G connection with nearby server
Congestion avoidance algorithm: ● BBR ● Cubic



Speed depending on packet loss for round-trip latency of 64 milliseconds

This level of latency is found chiefly on 4G networks when the server is located outside of France (but still in Europe).

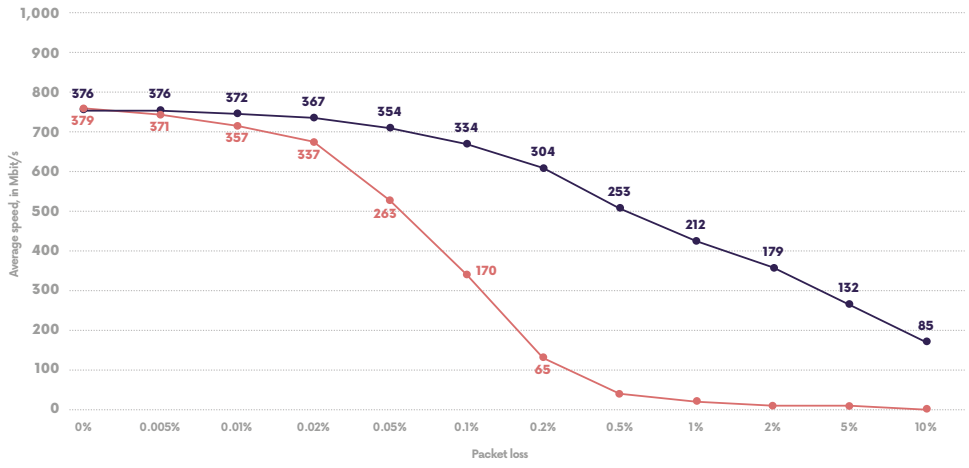
Note that with the Cubic congestion avoidance algorithm speeds decrease more significantly than with BBR, starting at 0.02% packet loss, and drop below 100 Mbit/s when packet loss exceeds 0.3%.



Speed depending on packet loss for round-trip latency of 128 milliseconds

This level of latency is found chiefly on 4G networks when the server is located overseas.

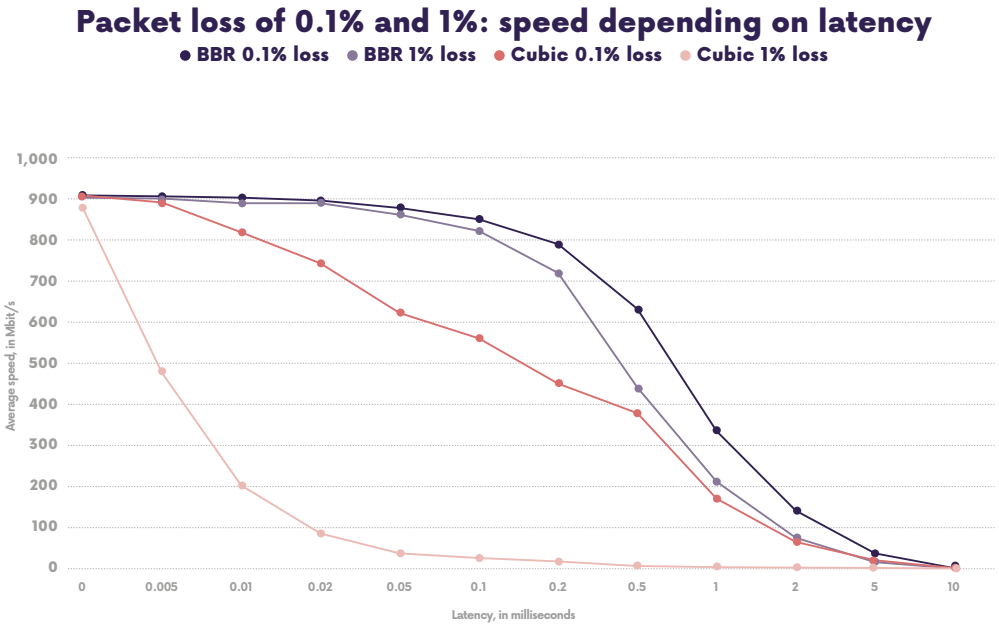
Speed drops to 9 Mbit/s with Cubic, when there is 0.5% packet loss.



Speed depending on latency for a packet loss of 0.1% and 1%

Packet loss of 0.1% can easily occur on Wi-Fi networks and of 1% on a network experiencing congestion.

Note that speed depends heavily on latency and the congestion avoidance algorithm.



6. Arcep's monitoring of mobile Internet quality

If mobile operators' coverage maps – which are produced based on operators' digital simulations and verified by Arcep – provide necessary information on the entire country, they also only give a simplified picture of mobile services' availability. Arcep does work continually on enhancing and improving them, notably by increasing the reliability threshold for coverage maps, which was increased from 95% to 98% in 2020 – but they will never perfectly represent reality[8]. 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 2021, more than a million measurements were taken from May to September on 2G, 3G, 4G and, for the first time, on 5G systems in every department across the country (both indoors and outdoors) and on transportation systems (metro, TGV, roadways).

In 2017, Arcep launched an interactive mapping tool called "monreseamobile.fr" (my mobile network), which allows users to view mobile operators' coverage maps along with 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.

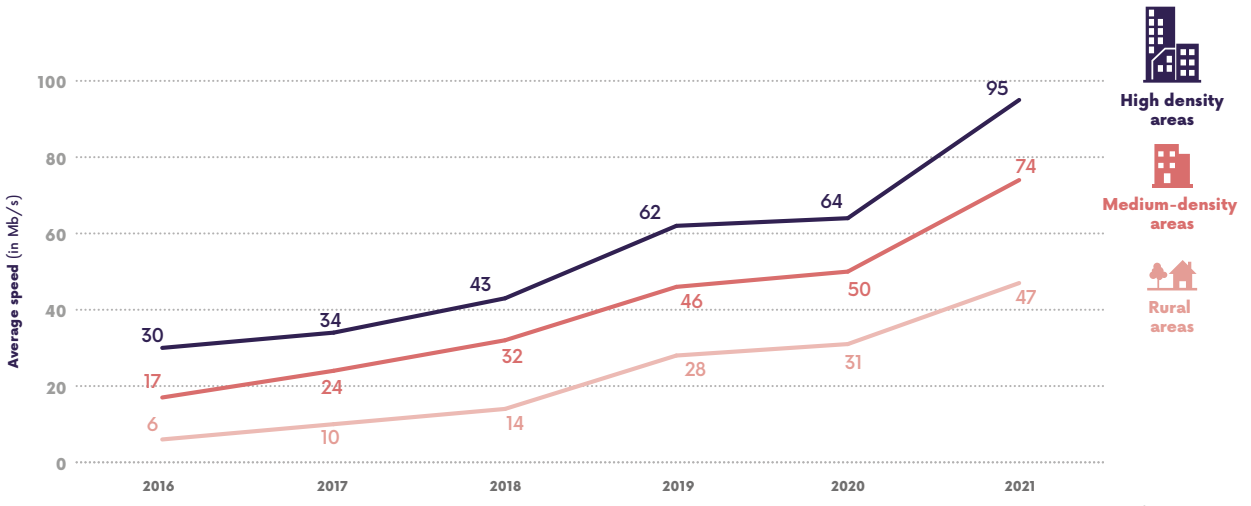
6.1. In Metropolitan France, quality of service continues to improve significantly after a 2020 marked by the public health crisis.

In November 2021 Arcep published the results of its 22nd annual audit evaluating the quality of the services provided by mobile operators in Metropolitan France.

The quality of every operator's mobile Internet services (data metrics) improved significantly, and this in every type of area: rural, medium-density and high-density.

Downlink speeds on 2G/3G/4G networks reached an average 71 Mbit/s, compared to 49 Mbit/s last year, which marks a steady increase after the decline in average connection speeds in 2020 due to the Covid-19 crisis.

PROGRESSION IN AVERAGE DOWNLOAD SPEEDS, BY TYPE OF AREA



Source: Arcep

8. Up until recently, Arcep considered a coverage map to be accurate if its rate of reliability, which corresponds to the success rate of a test performed in areas that operators declare as being covered, is equal to or above 95%. Arcep increased this threshold to 98% in a Decision adopted in March 2021, and which came into effect in Q4. More specifically, the decision sets the "overall" reliability threshold for maps at 98%. As an adjunct, this requirement is broken down locally: 98% for all areas of more 1,000 km² and 95 % for all areas of more than 100 km².

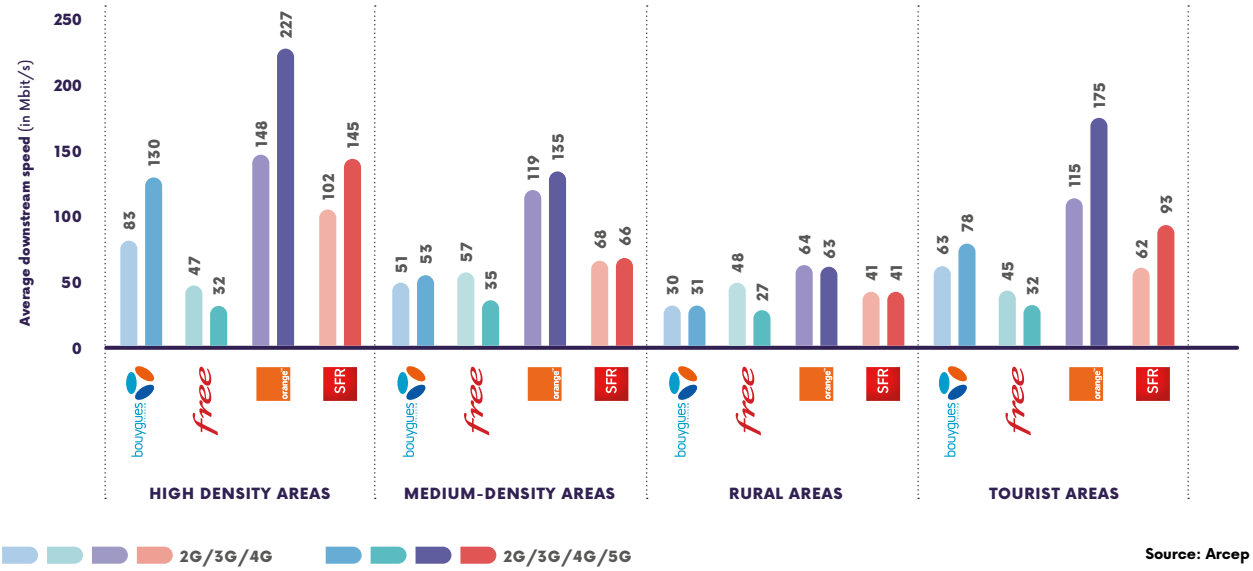
For the first time, Arcep has implemented a protocol that creates the ability to test quality of service for a user with a 5G-compatible plan and phone, and so measure downstream and upstream speeds. The indicator being published here presents the average speed obtained with 5G-compatible tests across the whole of France, to measure the speeds that a user can expect to have for their daily use, regardless of whether they are connected to a 5G cell tower.

Orange provides the fastest downstream speeds, with an average of 142 Mbit/s across the whole of France. Orange 5G users in high-density areas, where most of the operator's 5G cell sites are deployed, have access to an average connection speed of 227 Mbit/s. This is followed by SFR, with 84 Mbit/s on average in the whole of France and 145 Mbit/s in high-density areas, then Bouygues Telecom (71 Mbit/s on average, 130 Mbit/s in high-density areas). Free is in last place with 31 Mbit/s on average, with little difference in the speeds provided in high-density, medium-density and rural areas.

Regarding voice calls and texting, the quality of service in 2021 is comparable to 2020; in 2021, Arcep added a new published indicator by measuring call setup time – i.e. the time between the moment when the caller places the call and when they hear the first ringtone.

Finally, on transport corridors, the quality of service on "Intercités", "Transiliens" and "RER" railway lines was measured once again in 2021, after having been impossible to perform in 2020 due to Covid-19. The gaps between operators' quality of service on roadways continue are narrowing on most of transport corridors.

AVERAGE DOWNSTREAM SPEEDS FOR USERS WHO DO NOT HAVE ACCESS TO 5G AND THOSE WHO HAVE A 5G-COMPATIBLE MOBILE PHONE AND PLAN



Source: Arcep

6.2. Disparities in the progress of Internet quality of service in the overseas departments

The results of its quality of service audit in the French overseas departments and territories, published on 31 March 2022 shows a moderate improvement, whether for Internet services, voice calls and texting. The progress varies a great deal from operator to operator.

One change worth noting: Orange began providing Voice over LTE services on its overseas networks this year. This feature provides a better quality of calls, shorter call setup time and the ability to have a high-speed connection during the call.

Lastly, in 2021, Arcep tweaked the methodology employed to test video streaming services in Reunion and in Mayotte. Up until now, tests had been performed with a resolution set at 720p. In 2021, to reflect users' actual experience more accurately, resolution is no longer blocked at 720p but, rather, is adaptative. Streaming can therefore be performed using different resolutions.

A video stream is considered to be of decent quality if it meets the following criteria:

- 95% of streaming time with a resolution of >=360p;
- Load time of under 15 seconds;
- Disturbance that lasts fewer than 5 seconds.

A video stream is considered to be of perfect quality if it meets the following criteria:

- 95% of streaming time with a resolution of >=720p;
- Load time of under 10 seconds;
- Disturbance that lasts fewer than 0.5 seconds.

6.3. 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 toolkit 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. Arcep has been engaged in an ongoing dialogue with these players and, since April 2020, "Mon réseau mobile" has been further enhanced by the measurements obtained by different regions. Many regions were involved in this initiative and particularly: Bourgogne-Franche-Comté, Auvergne-Rhône-Alpes or Pays-de-la-Loire. Departments such as Haute-Loire or Cher also took such actions.

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 (see section 3 of this chapter).

Since February 2022, SpeedChecker and Mozark speed test results have been published on the "Mon réseau mobile" site in a tab dedicated to crowdsourced testing. These data represent 100 times the number of measurements taken as part of Arcep's classic annual QoS audit, conducted in living spaces (which concern 2,000 test points), and have the advantage of being able to be conducted anywhere in the country and at any time of day or night. Crowdsourced measurements must, however, be interpreted very carefully, due to the uncontrolled variable conditions at play when running the tests, such as the inability to know for certain whether a user performed the test indoors or out. Arcep has also published an instructional document that details these precautions to take when interpreting the data.

This publication is part of Arcep's data-driven approach to regulation, which aims to empower users by providing them with accurate and personalised information, whether it comes from users themselves, via crowdsourcing solutions, local authorities' measurement campaigns or collected from operators by Arcep.

Arcep would like to thank Mozark and SpeedChecker for agreeing to be part of this process, and invites any players wanting to continue to enhance "Mon réseau mobile" to join them. Users too can contribute by conducting tests using these applications, whose results will then be posted on "Mon réseau mobile" apace with the regular updates.

Open floor to

FRÉDÉRIC LASOROSKI

*Head of Network Performance – **Bouygues Telecom***

TREMENDOUS IMPROVEMENT IN THE QUALITY OF MOBILE SERVICES OVER THE PAST FEW YEARS

Voice services, which are essential to our customers, and for which there is an expectation of irreproachable QoS, continue to improve. VoLTE, launched by Bouygues Telecom in 2015, has become the standard for voice calls, with its virtually instantaneous call setup time and increased voice quality.

Meanwhile, data speeds have skyrocketed. Between 2016 and 2021, average download speeds all operators combined, as measured during an annual mobile QoS audit, increased close to eightfold in rural areas, going from 6Mbit/s to 47Mbit/s, and more than fourfold in high-density areas, going from 30Mbit/s to 133Mbit/s with the start of 5G deployment.

Download speeds are now so fast that disparities between operators no longer reflect a significant quality of experience gap for customers on the most common applications. A download speed of over 3Mbit/s is enough to sustain standard mobile Internet uses: web browsing, social media and streaming videos in 480p or 720p without any major lag.

Climate change has made the push for digital sobriety crucial. Putting an end to the race to deliver ever higher speeds, which offers no real advantage to customers, will help optimise the sector's carbon footprint.

Operators and Arcep need to assess whether measuring download speeds is still relevant. The mobile QoS audit should focus on indicators that measure the quality of the services that customers use every day.

Added to which, a fast connection alone is not enough to deliver optimal service. The network needs to be reliable, optimised and provisioned from end to end: wireless, transport, core network, interconnection with Internet companies. The emergence of 5G and new services and (notably industrial) uses will introduce new criteria for differentiating networks, such as latency, and represent new challenges for operators.

MARIE-GEORGES BOULAY

*Deputy Secretary-Genera - **Altice France/SFR***

QUALITY OF SERVICE: A CORE ISSUE FOR SFR

When delivering the results of the mobile QoS audit for 2021, Arcep once again ascertained that quality levels had progressed across the board, with a clear improvement from every operator and in every type of area (rural, medium-density and high-density). The progress in mobile Internet quality is especially welcome news. The quality of service provided on our mobile networks is a central focus for SFR, driven by a commitment to improving both voice and Internet access quality: which has resulted in a 46% increase in download speeds compared to those measured in 2020, significant progress across all strata of the country, an improvement in the rate of calls with perfect voice quality…

Quality of service depends on technological choices and investments. It differentiates competitors and influences consumers' choices.

This quality has now reached very high levels on 4G networks, for both voice and data services, with high success rates on services of over 90%. It therefore makes sense to reduce the number of criteria monitored by the regulator's annual audit. Attention to quality now appears to be increasingly present with 5G. SFR thus believes that consumers should be provided instead with more information on 5G performance on the different frequencies, as part of the annual QoS audits. The latest audit revealed that 4G and 5G cohabitation on the same frequency band could degrade 5G performance, with some operators' 5G speeds being slower than their 4G ones. This information warrants being further detailed to demonstrate to consumers the performance delivered by 5G in the 3.5 GHz band, as opposed to other frequencies.

The aim of the regulator's quality of service audits of mobile networks is to deliver a snapshot of the diversity of users' experience under the most common conditions. SFR plays close attention to the ways that crowdsourcing tools contribute to measuring this quality of service. While these tools provide interesting information thanks to the sheer volume of their input, they cannot replace measurement campaigns conducted in a controlled environment. These tools can introduce major statistical biases in terms of representativeness (geography, user device, behaviour…). They cannot replace tests carried out using well-defined protocols, which guarantee the same objective measurements on every network.

Open floor to

MAXIME LOMBARDINI
President - Free Mobile

MEASURING THE QUALITY OF MOBILE SERVICES

Arcep's mobile quality of service audits adhere strictly to a complex protocol. More than 200 usage and coverage indicators are measured each year, at tens of thousands of locations, then aggregated into layers to form the indicators. The details behind the results of these audits remain unclear for members of the public, and even for specialised journalists. It is also amusing to see that, after each audit, every operator declares itself number one on this or that criterion.

We believe that the current mechanism is far too complex and unclear. Added to which the highlighted findings do not necessarily express the reality of the user experience. Journalists, like Arcep itself, tend to focus heavily on downstream speeds, which is a very flawed way to reflect ease of use. Indeed, once connections exceed around 10 Mbit/s, download speed is rarely an issue when running most applications (watching a video, sending photos, receiving email…).

By far the most questionable aspect of the entire quality of service audit, however, is the protocol Arcep uses to measure download speeds. A brief (and rather technical) public controversy in fact occurred after the publication of the 2021 results, and could happen again this year.

It is a simple matter of common sense. There are a great many speed test platforms, such as 5G mark and Nperf. Rankings can vary from platform to platform, and over time, but the four operators' speed indicators are generally comparable, and variations between first and last place speeds rarely reach a factor of two. Arcep's test protocol is the only one to have measured differences of a factor of three between certain operators' speeds in 2021. A disparity of this size leads one to question the reliability of Arcep's protocol, when compared to the findings obtained by other platforms.

To produce relevant and reputed QoS audits, we believe the regulator needs to hold an open and transparent debate, after having defined its objectives and the procedure for communicating its findings. This debate must lead to the definition of a test protocol and methodology that are accepted by all of the players.

Orange chose not to respond to Arcep's invitation to contribute to this section.

Methodology of the mobile QoS assessment protocol

The protocol used for the annual assessment of mobile operators' quality of service is designed to measure a mobile quality of service that is representative of the user experience. The speeds measured by Arcep can differ substantially from those obtained by certain crowdsourced speed testing tools, as some tools measure the link's capacity (the speed on the link between the device and the Internet) whereas Arcep seeks to obtain a speed that is representative of actual use of the Internet. The main differences between certain crowdsourced speed tests and the Arcep protocol are detailed below.

Single connection vs. Multi-connection

Single connection: a single connection speed test measures the speed of a single connection, and therefore a speed that is representative of actual Internet use. At any given moment, the vast majority of Internet applications use a single, high-speed connection. For a great many online services, several connections are open, but in the overwhelming majority of cases, at any given moment, only one connection is used at a time to transfer most of the data. For instance: a transfer will begin with connection «A» before switching over to connection «B» then «C» before returning to connection «A». Certain small elements may be transferred in parallel, but this is a minor occurrence and, overall, most uses of the Internet match the behaviour of a single connection speed test.

Multi-connection: a multi-connection speed test measures Internet connection speed by adding together the speeds of multiple simultaneous connections. A number of speed tests conduct a transfer on 16 simultaneous connections, for example. These multiple connections create the ability to estimate the link's maximum speed, but are unable to detect certain speed restrictions on TCP connections. These restrictions, which heavily affect a single TCP connection but multiple parallel ones only marginally, can include packet loss and/or saturation and/or excessive latency.

Arcep's choice: Arcep's protocol is single connection to be more representative of most customers' Internet use. In 2022, however, an experimental multi-connection trial (limited to 50 testing locations) will be conducted, to obtain additional information on the tested links' capacity.

Cubic vs BBR

The results of QoS and speed testing also depend on the technical characteristics of the test servers, and particularly their congestion avoidance algorithms (CAA). These algorithms are used on the data sender side to determine packet transmission speed. A number of congestion avoidance algorithms exist, and these algorithms are evolving.

Cubic: Most Internet services today use Cubic. Created in 2006, it uses packet loss as the signal to reduce speed. Cubic is the congestion avoidance algorithm used by default in Linux (which runs most of the Internet's servers) as well as Android and macOS.

BBR: In 2016 Google developed BBR (Bottleneck Bandwidth and Round-trip propagation time) which uses a different model, based on maximum bandwidth and round-trip time. When there is packet loss on a connection, this approach enables BBR to deliver significantly higher speeds than those provided by packet loss-based algorithms like Cubic. Today, some of the top Internet companies are starting to deploy BBR on their servers. But BBR has not yet been widely adopted online, largely due to RTT fairness issues. On a link where bandwidth is shared between users (e.g. mobile network frequencies or a fiber link) BBR connections will "take the place" of Cubic connections. BBR v2 is currently being developed to improve the current version and achieve better cohabitation with Cubic.

Which congestion avoidance algorithms are used in speed test apps? These applications can use Cubic, BBR, or other congestion avoidance algorithms which may be particularly aggressive, and so potentially creating the ability to achieve very high speeds, but which are not representative of regular daily use. Arcep is working to promote more transparency by encouraging speed test tools to list their congestion avoidance protocol. If the settings on certain speed test servers make it possible to display speed records, this does not necessarily influence the speeds that a single end user will obtain for their daily use.

Arcep's choice: The Arcep protocol seeks to reflect users' regular use of the Internet and, in 2022, 75% of the tests will be conducted with Cubic and 25% with BBR. The experimental multi-connection trial (limited to 50 testing locations) will be conducted entirely in BBR, to obtain a sample similar to the results of crowdsourced speed testing tools.

HTTP vs HTTPS

The Internet has evolved over time, and in a matter of years has switched from an HTTP protocol (unencrypted and on port 80) to the HTTPS protocol (encrypted on port 443). Most mobile speed tests are still conducted over HTTP. For some applications, neither port 80 nor port 443 is employed, which creates representativeness issues. Arcep is urging greater transparency, and asking testing tools that comply with the 2021 Code of conduct to indicate which port they use, and whether or not the speed test connections are encrypted.

Arcep's choice: In 2022, all tests performed using the Arcep protocol will employ the HTTPS protocol on port 443.

IPv4 vs IPv6

The Internet's transition to IPv6 is underway and, according to Arcep's 2021 IPv6 Barometer, 62% of the most visited web pages (Alexa data on top 730 for France) support IPv6. Some speed test tools have chosen to offer only IPv4 tests by default, whereas others use IPv6 as soon as the server and customer both have IPv6 connectivity. Arcep is urging greater transparency, and asking testing tools that comply with the 2021 Code of conduct to indicate if their test servers support the IPv6 protocol.

Arcep's choice: Under the Arcep protocol, 50% of tests are conducted in single stack IPv4 and 50% in dual-stack IPv4/IPv6.

Average speed vs maximum speed

The speeds displayed by testing tools can differ depending on the tool:

- maximum speed, reached for a short duration during the test;
- established speed (speed at the end of the test);
- average speed, after removing the slow start (first few seconds of the test);
- average speed, between the file request and receiving the last packet.

To increase transparency on this aspect of testing, Arcep is asking testing tools that have declared themselves compliant with the 2021 Code of conduct to list the indicators displayed at the end of the test. Testing tools must also indicate the length of the test, when the maximum volume is not reached and the maximum volume of data transferred (size of the downloaded file).

Arcep's choice: Speed is calculated by incorporating all of the stages, namely DNS resolution, TCP connection, Transport Layer Security (TLS) encryption and transfer of a 250 MiB[1] file. The transfer stop as soon as the file has been fully downloaded, or after a 10-second delay expires. If difficulties occur during the DNS request or server connection stages, the test will not be interrupted before the 10 seconds are up.

Configuration of the test servers used

In the interests of transparency, Arcep is publishing a document that recaps the parameters of the test servers used: server configuration for Arcep 2022 mobile QoS audit.

Open floor to

THOMAS SCHREIBER
RTR-NetTest team – Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR-GmbH)

DIETMAR ZLABINGER
ÉRTR-NetTest team – Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR-GmbH)

TEN YEARS OF RTR-NETTEST

Back in 2011 RTR, the Austrian regulatory authority, started to investigate how end users could be empowered regarding the quality of Internet access. Consequently, RTR-NetTest was launched in spring 2012. It provides users with a tool to test the speed and quality of their Internet connection – reliably and independently. Thus advertised or contractual performance can be easily compared against actual quality.

RTR-NetTest is available for Android, iOS and browsers, where it can be found in the app stores of Android and iOS as in the web under https://www.netztest.at/.

RTR-NetTest measures different parameters, including download and upload speed, ping (latency), signal strength and technology (depending on the device used). The test results are depicted in a map and can be shared with others. The tool allows for a certified measurement where the result is available as PDF and can be used as "prima facie proof" in proceedings.

Besides information for end users, aggregated results of RTR-NetTest are also used for regulatory purposes and RTR's publications, e.g. the quarterly published "Internet Monitor" which provides key figures about Internet supply and demand.

All data that is not personal data is published by RTR under the Creative Commons Attribution (CC BY 4.0) licence as Open Data. This allows private entities, research companies and universities to re-use this data in their projects and conduct further analysis. The code of RTR-NetTest is Open Source and is published on GitHub under the permissive Apache 2.0 Licence.

This year, when RTR-Nettest is celebrating its tenth anniversary, its popularity is still growing, counting more than 14.000 measurements per day. In total, more than five million measurements are conducted each year.

VOLKER SYPLI
Technical Officer - Federal Network Agency in Germany (Bundesnetzagentur)

ENABLING END USERS TO CHECK INTERNET ACCESS SERVICE PERFORMANCE

The Bundesnetzagentur provides a monitoring mechanism, the "Breitbandmessung" broadband speed checker, which allows consumers to monitor the quality and performance of their broadband Internet access. An installable version (desktop app) can be used for fixed-line broadband and an app-based one (Android and iOS) for mobile connections. Also, for testing the performance when surfing the Internet, a browser-based test is available.

"Breitbandmessung" measures the data transmission rate in both the download and upload directions. Results are presented as absolute values and as relative values for the contractually agreed speed. Thus, the broadband speed checker allows the data transmission rate actually measured of a broadband connection to be compared with the data transmission rate contractually agreed.

The desktop app constitutes a certified monitoring mechanism according to Article 4(4) Regulation (EU) 2015/2120. Specific care is taken in order to avoid influences of the end user environment on the measurement results by technical means, end user declaration and accompanying user-friendly technical education.

The broadband speed checker is also used to collect test samples via crowdsourcing. The results are presented in an annual broadband speed test report. A browser-based map displaying these is also available showing validated test results broken down by region and other criteria, such as provider and/or bandwidth category, and is updated on a daily basis.

Open floor to

JOHAN FOLDØY

*Head Engineer - **Norwegian Communications Authority (NKOM)***

INTERNET MEASUREMENTS: EMPOWERING END-USERS AND MONITORING THE DEVELOPMENTS

Internet as a service platform is a wonderful thing: deeply affecting our daily lives whether we look for entertainment, business opportunities or education. The development in available content, as well as the underlying technologies being used to deliver it to our device, continues to amaze.

Norwegian Communications Authority (Nkom), as a regulator, has several responsibilities when it comes to Internet. One of them is to understand and monitor the development of Internet access quality and availability, and to enable end-users to do the same. Therefore, Nkom already in 2009 developed and released our measurement tool nettfart.no, providing the domestic Internet users with a possibility to verify their connection quality and understand what might affect the measurement results.

Our way of connecting to the Internet has changed from copper to fiber, and from 2G, 3G and 4G, to 5G. Applications and services has taken us from static content to augmented reality. This means Nkom needs to pay close attention and make sure the tools we offer will provide reliable measurement results, but also: present relevant information for the users.

An example on this can be found in our mobile app: in the map view, we focus more on which mobile **technology** was available in a certain location, rather than simply the measured speed or latency. Not because they're unimportant, but because we expect that 5G access in itself will be key to realize a plethora of services, in the coming years.

KLAUS NIEMINEN

*Chief expert - **Finnish Transport and Communications Agency (Traficom)***

A NEW MEASUREMENT TOOL TO EMPOWER END-USERS

Our goal is to promote the understanding of Finnish Internet users about the quality of the service (QoS) they receive and to help them make informed decisions. The QoS information is also important in the light of our regulatory task for example in the areas of coverage obligations and universal service.

Therefore, in 2022, Traficom will publish its Bittimittari.fi QoS measurement service supporting measurements via Android and iOS applications and web browsers.

Our new measurement tool will be a certified monitoring mechanism according to the Article 4(4) of the Open Internet Regulation enabling the detection of the potential significant discrepancy between actual and contractual performance for fixed network subscriptions and trigger the remedies available to the consumer in accordance with national law.

Our measurement tool is based on the NetTest code and we have been developing it further especially in two aspects. We have limited the need to process and collect personal data for example by storing the measurement history locally in the measurement client. We are also targeting to elaborate further what the measurement results mean for the particular user's needs. We'll also conduct an extensive security review for the service.

I would also like to voice our sincere thanks for our NRA colleagues and the good collaboration done within BEREC's Open Internet working group.

CHAPTER 2

SUPERVISING DATA INTERCONNECTION

What you need to know

Inbound traffic to the main ISPs in France increased by more than 25% in a single year, to reach **35.6 Tbit/s at the end of 2021.**

51% of traffic to the customers of France's main ISPs come from **5 providers:** Netflix, Google, Akamai, Facebook and Amazon.

In 2021, video streaming accounted for more than **53% of global IP traffic** transiting on electronic communications networks, according to Sandvine[9].

Interconnection[10] 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[11].

1. Video delivery

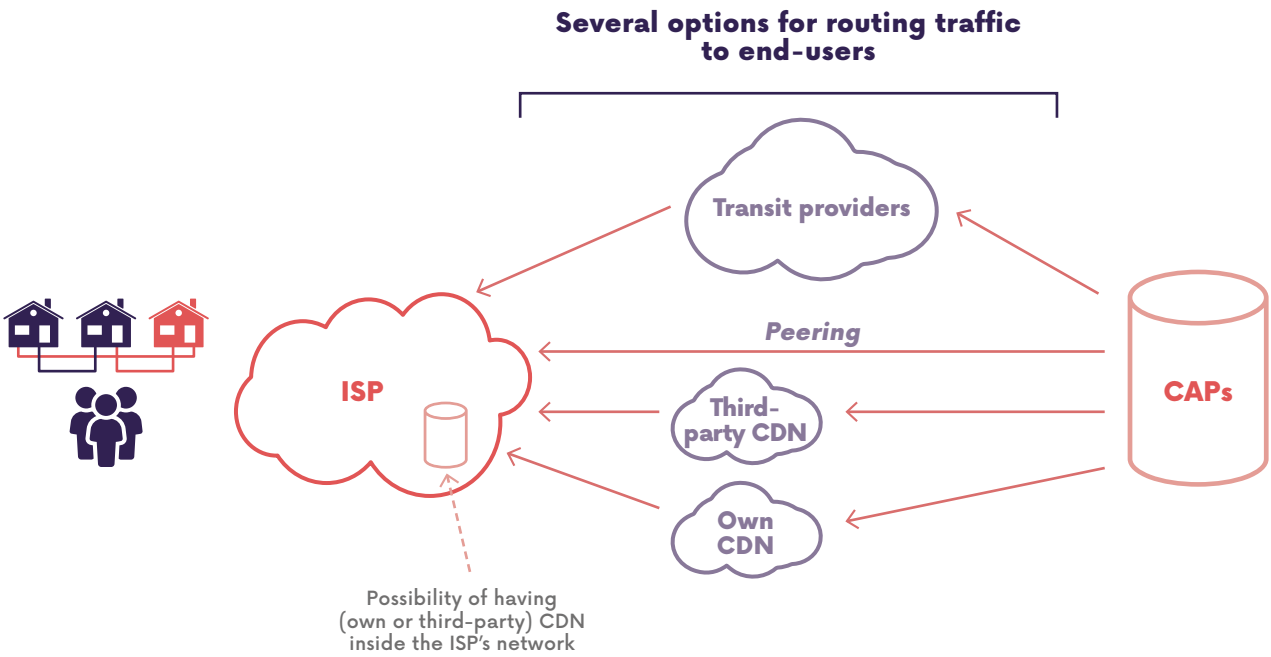
In 2021, video streaming accounted for 53.72% of global IP traffic transiting on electronic communications networks, according to Sandvine[12]. Video content is also found in other categories in this ranking, including social media which accounts for 12.69% of global traffic, online gaming (5.67%) and messaging solutions such as WhatsApp, Zoom, Microsoft Teams, Messenger, etc. (5.35%). Video's substantial share of total online traffic can be attributed to the proliferation of sources (live/linear viewing online, replay and catch-up services, subscription video on demand services, social media, video chats on instant messaging, widespread use of video advertising, etc.). It is also due to the overall increase in the quality of online videos[13].

France is no exception here, and is part of this global trend. As indicated in the Barometer of data interconnection in France, the main content providers are Netflix, YouTube, Akamai, Facebook and Amazon whose video content consumes a great deal of bandwidth.

As to interconnection methods and to reach end users, video content providers can contract the services of transit providers, in the same way that content and application providers (CAPs) do. This was the main option available in the early days of the Internet. In a matter of only a few years, however, as traffic increased alongside the need to improve quality of service and the quality of the user experience, the Internet's architecture evolved and several alternatives to transit emerged, starting with peering. Peering, which can be private or public, enables CAPs to do away with transit providers and interconnect directly with ISPs.

9. Sandvine, the global Internet phenomena report, January 2022. Click here.
10. Definitions of the technical terms related to interconnection that are employed here can be found in the Barometer of data interconnection in France.
11. 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.
12. Sandvine, the global Internet phenomena report, January 2022.
13. Streaming content in UHD generates eight times more data traffic than high definition (HD) streaming, using identical encoding levels. Source: CGE, Reducing digital's energy consumption, December 2019.

INTERNET TRAFFIC ROUTING



Source: Arcep

To improve quality of service by bringing content as close to end users as possible, video content providers will often use content distribution networks (CDNs) which replace long distance transport with local data storage on cache servers[14]. Some of the largest CAPs – such as Google, Netflix and Facebook – have the means to develop and own their own long-distance transport infrastructure, as well as their own CDNs which gives them the ability to optimise the delivery of their content. ISPs too are deploying their own content delivery networks.

Another major trend to emerge over the past several years is the advent of internal or on-net CDNs[15]. These servers are managed by the company that owns them (CAP, CDN or ISP) but are installed inside the ISP's network. To improve quality of service by getting as close to end customers as possible, CAPs create partnerships with ISPs to have their content hosted on cache servers inside operators' network. The on-net CDNs can belong to the operator that hosts them, or to a third party. The most notable examples are the Netflix OCA (Open Connect Appliance) and Google Global Cache (GGC) servers. By bringing content closer to end users, the use of an on-net CDN installed inside an ISP's network creates the ability to upload video content to servers during off-peak times, instead of waiting to satisfy user requests for it during peak hours.

In addition to developments in interconnection methods, another path to optimising video stream delivery involves the use of codecs[16] to reduce the size of the content without damaging its intrinsic qualities. By using powerful codecs, CAPs give users the ability to access more content within the same volume of data traffic.

In addition, leading video content providers often choose to encode a video file with multiple quality settings to be compatible with the different user devices' capacities (including the oldest devices) and their client Internet access services' bandwidth capacity. Encoding with several resolution settings, along with choosing the quality provided for ultimate viewing, notably its optimisation according to the device, also contribute to reducing the digital carbon footprint. Combined with an adaptive streaming mechanism, the user device can automatically, and in real time, choose the video quality best suited to available bandwidth. The device is able to continually adapt to the available video quality as the access environment changes, by downloading the video file that corresponds to the highest possible resolution. This helps minimise timeouts and lags, and so improve the overall viewing experience.

14. See Lexicon.
15. See 2.5. Traffic breakdown by interconnection type, page 42.
16. See Lexicon.

Codecs and their role in video stream delivery

Online video streams are compressed using codecs. A codec is a device or computer program that encodes and decodes a digital data stream. It will help drastically reduce the size of this stream by encoding only the differences between the frames. Fixed images are transmitted in full at regular intervals (compression of these images can be similar to jpeg, used for photos). The other frames are described by the differences between the previous and/or following frame. A frame where only a person's mouth moves will require little data if the encoder is able to vary the speed according to the scene being encoded. On the other side of the spectrum, a camera installed on a motorbike filming the Tour de France will probably produce frames that are more complicated to encode and require high speeds to preserve picture quality. A maximum speed is typically assigned to the encoding to keep from exceeding a threshold.

It typically takes several years for a codec to be developed and widely adopted, as it first needs to be implemented in the different software and hardware where it will be used. If a web browser can be updated to be compatible with new codecs that it will decode using microprocessor-powered software, on other peripherals such as televisions decoding is performed by hardware, in which case it is impossible to provide a new codec through a software update.

Most global Internet traffic is composed of compressed video, and H.264/AVC is by far the most widely used video codec on the web. There are new generation codecs that make it possible to cut the size of a video stream in half. But H.264/AVC remains the most popular because more powerful codecs create incompatibility issues with some customers. It is therefore impossible to offer a single encoding process: videos often need to be encoded and stored in two or three different codecs for each resolution. The cost of these different encodings means that only a small handful of major players can afford to handle it themselves. They generally do not encode every video in AV1, which is a more powerful codec than H.264/AVC, but use artificial intelligence to encode only the most popular videos in different formats.

A list of the main video codecs is available in the Annex to this report.

Tutorial

How to find out which codec is being used?

Here is the method for the two main players that use multiple video codecs:

- YouTube on a web browser: Click right on the video and select "Stats for nerds": if "avc1" is listed on the "Codecs" line it means that the video being played uses the H.264/AVC codec. A video with "av01" is encoded in AV1. "vp9" means the video is encoded in VP9.
- YouTube on a smartphone: open the YouTube app, click on the user account icon at the top right, then tap "Settings" then "General". Scroll to the bottom and tap "Advanced". When the video is played, one can then show/hide «Stats pour nerds» via the video player's three-dot "More" button.
- Netflix on a web browser: Press the "Ctrl" + "Shift" + "Alt" + "Q" keys simultaneously. The video codec is listed at the end of the "Video Track" line.
- Netflix on a TV: Connect a USB keyboard to the TV and press "Q" in the Netflix app.

Open floor to

ÉRIC RENARD
CTO - Molotov

THE CHALLENGE OF ONLINE VIDEO STREAMING

Streaming services need to carry a very large data streams from their servers up to customers' devices. These customers' demand for high quality, combined with increased average Internet connection speeds have only increased these streams over time. Today, 1080p has become the *de facto* standard for a fee-based service, and standard codecs such as H264 make it possible to live stream at that quality at speeds of around 4-5 Mbps per customer. For a service like Molotov, which serves over 300,000 simultaneous viewers a day, this represents a required outgoing stream of more than 1 Tbps with, of course, a need for continuity of service and decent latency.

To ensure this quality of service, every streaming service works with CDN (Content Delivery Network) providers. A CDN is an infrastructure capable of reliably delivering massive amounts of data. For six years now, Molotov has been working with multiple CDNs (Akamai, CloudFront, Fastly…) to ensure the best quality of service for its customers.

Optimisation at the codec level

For a service such as Molotov, optimising video bandwidth is absolutely fundamental for two reasons: providing the same streaming quality over lower bandwidth creates the ability to open the service up to households that are not yet equipped with a superfast fiber connection, and to mobile customers using a less powerful network and, naturally, to improve the company's economic equation. Video distribution fees represent a very large percentage of a streaming service's operating costs, so reducing bandwidth requirements has an extremely significant financial impact.

Today, H264 remains the king of codecs. It allows for decent compression rates; it is universally compatible with every device (which is crucial for a service like Molotov that wants to be universal and ubiquitous) and it carries no licensing issues. For several years now, we have been seeing new codecs appear, promising superior results on both video file size and quality: HEVC, VP9, AV1… Unfortunately, none of these codecs currently provides coverage of all of the devices on which Molotov is run, and employing multiple codecs leads to financial cost issues. Trials nevertheless continue, and the world of video is a constant state of development, so nobody doubts that development at this level are to be expected.

Another level of optimisation lies in the choice of CBR (constant bitrate on all video) and VBR (variable bitrate, depending on the complexity of the scene). Traditionally, live streaming is performed using CBR, which helps ensure constant quality, while on-demand services are delivered using VBR as the elimination of the constraints of live streaming create the ability to optimise video in several stages, and to reduce bitrates substantially without losing quality.

Over the past several years, we have also seen encoding solutions appear that are based on machine learning technologies, as a way to optimise streaming bitrates further still.

The new challenges

As streaming becomes French people's favourite way of watching TV, demands on service quality are rising. We have several key sources of concern for the coming years.

First, video quality and ultra-HD resolution, such as 4K. Even if sources are still rare today, 4K will eventually become the norm and create even more data transfer issues. A decent 4K stream today requires a bandwidth of close to 15 Mbps, or three times more than a 1080P stream.

Latency is of course a topic that arises on a regular basis. It is the Achilles' heel of the streaming world, which is still struggling to keep the live delay under 45 seconds, compared to several seconds for satellite and DTT. The technology to narrow this gap does exist, but requires massive adaptations at every step along the chain: encoding, packaging, CDN, video player, etc.

Lastly, sound quality is also becoming an issue for French viewers. Streaming is being done more and more on the living room television, using high quality audio equipment – equipment which is often underused as virtually all live streams are currently confined to simple stereo.

Open floor to

CHRISTIAN KAUFMANN
*Vice President Technology - **Akamai***

THE INTERNET IN FRANCE FROM A CDN AND CLOUD COMPANY VIEW

Akamai is operating the largest and most distributed edge platform, which just peaked at 250 Tbps in April 2022, this said Akamai also has a long history and strong presence in France itself.

The Internet Infrastructure in France is very centralized, most of it is deployed in data center in the Paris metro area, this is equally true for local eyeball operators or carriers but also for international cloud and content companies.

When it comes to the highest Interconnection density in data centers, we even just talk about three locations in Paris, covering the majority of traffic in France - Telehouse and Equinix followed by Interxion.

In the recent years there where some efforts to decentralize these dependencies on Paris with Marseille leading the way.

This led to some of the traffic in the south of France staying in Marseille and beind exchanged there, instead of going to Paris and therefore twice through the country which has negative implications to round trip times but also the throughput.

But to equal parts Marseille also attracted more foreign providers and carriers from North Africa, the Middle East and even Asia because of the submarine cable landing station and its two Internet Exchanges.

In the recent years, especially with the merger of Rezopol and FranceIX we also have seen some traction in the Lyon market, so we are hopeful to get a third Interconnection point in France for local and international players.

But despite or probably because of this centralization in France Akamai delivers more then 90% of the content for French end users from inside the country.

For this Akamai uses its Akamai Accelerated Network Partner Program (AANP), with Akamai server deployed in the eyeball network as well as extensive PNIs (Private Network interconnect) or the various Internet Exchanges like FranceIX.

In the past Akamai relied on the public Internet as a delivery method to connectivity between its own server cluster. In the last couple of years, Akamai built its own global backbone for performance but also for economic reasons. This global backbone also has pops in Paris and Marseille where it connects to the rest of Europe but also to the US and to Asia.

All these above-mentioned delivery methods allow low latency and high throughput as it is needed for time sensitive applications as well as HD and 4k video delivery.

Looking at the end user behavior regarding video delivery we see a change in the last couple of years, we see Video on demand overtaking the Video Live Streaming in traffic volume.

Another trend which is worth to mention is the IPv6 adoption rate of France.

Akamai serves approximately 25% of the traffic volume in France via IPv6 by now, this said there is quite a difference between the various eyeball providers.

Free/Proxad has the highest rate with approximately 50% of its traffic being received via IPv6 on one side and SFR with just 10% on the other side of the spectrum. Other providers like for example Orange Telecom are somewhere in the middle with around 30% of its traffic received via IPv6.

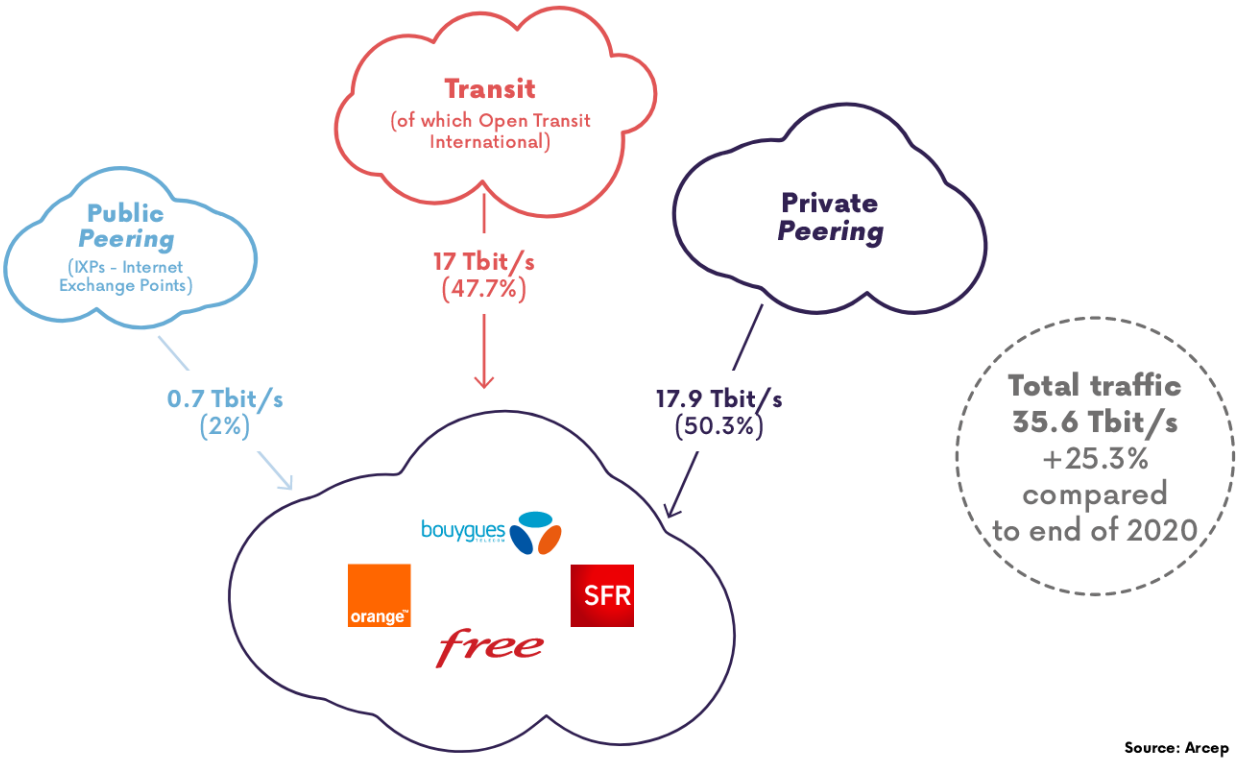
2. State of interconnection in France

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 2021. For confidentiality reasons, the published findings[17] are the aggregated results only of the main ISPs in France (Bouygues Telecom, Free, Orange, SFR)[18].

2.1. Inbound traffic

Inbound traffic to the four main ISPs in France increased from more than 28.4 Tbit/s at the end of 2020 to 35.6 Tbit/s at the end of 2021, which translates into more than 25% increase in a single year. Almost 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 2021)

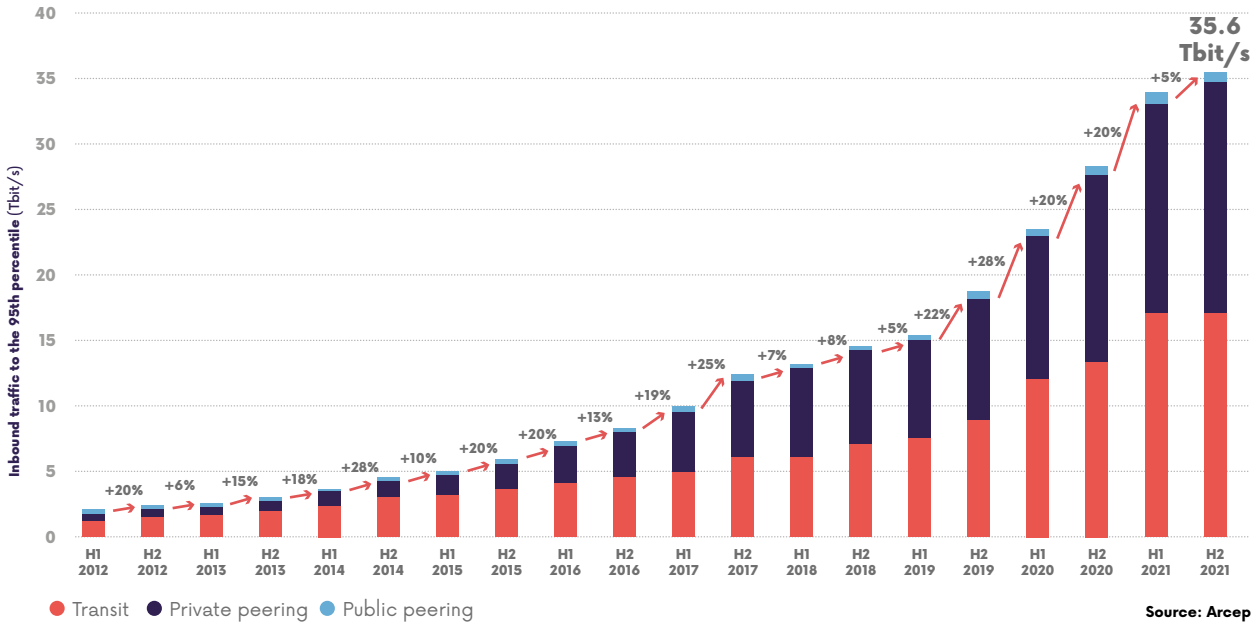


Source: Arcep

17. 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.

18. Figures for H2-2020 were amended slightly compared to 2020 figures following a change in methodology.

INBOUND TRAFFIC TO THE MAIN ISPs IN FRANCE, FROM H1-2012 TO H2-2021

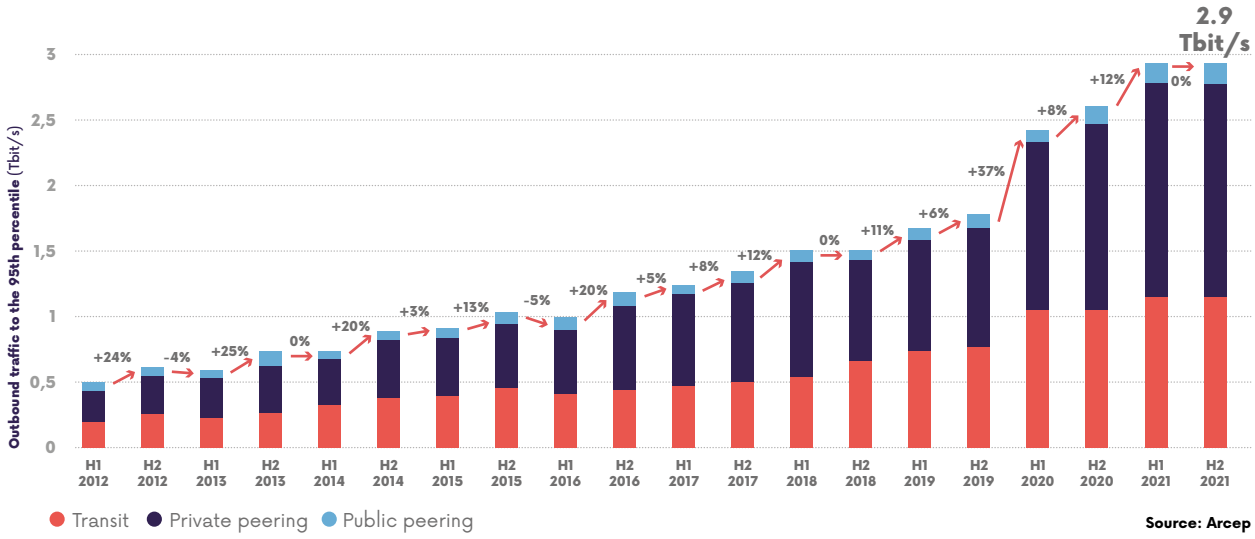


Source: Arcep

2.2. Outbound traffic

By the end of 2021, outbound traffic on the networks of France's four main ISPs stood at around 2.9 Tbit/s, or 12.5% more than at the end of 2020. This traffic multiplied sixfold between 2012 and 2021.

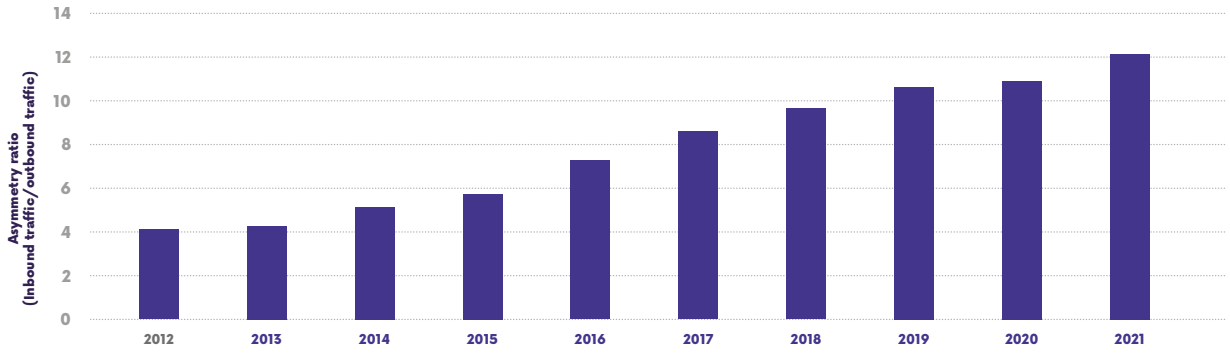
OUTBOUND TRAFFIC FROM THE MAIN ISPs IN FRANCE, FROM H1-2012 TO H2-2021



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 1:12 in 2021. 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 THE INTERCONNECTION LEVEL FOR THE MAIN ISPs IN FRANCE BETWEEN 2012 AND 2021



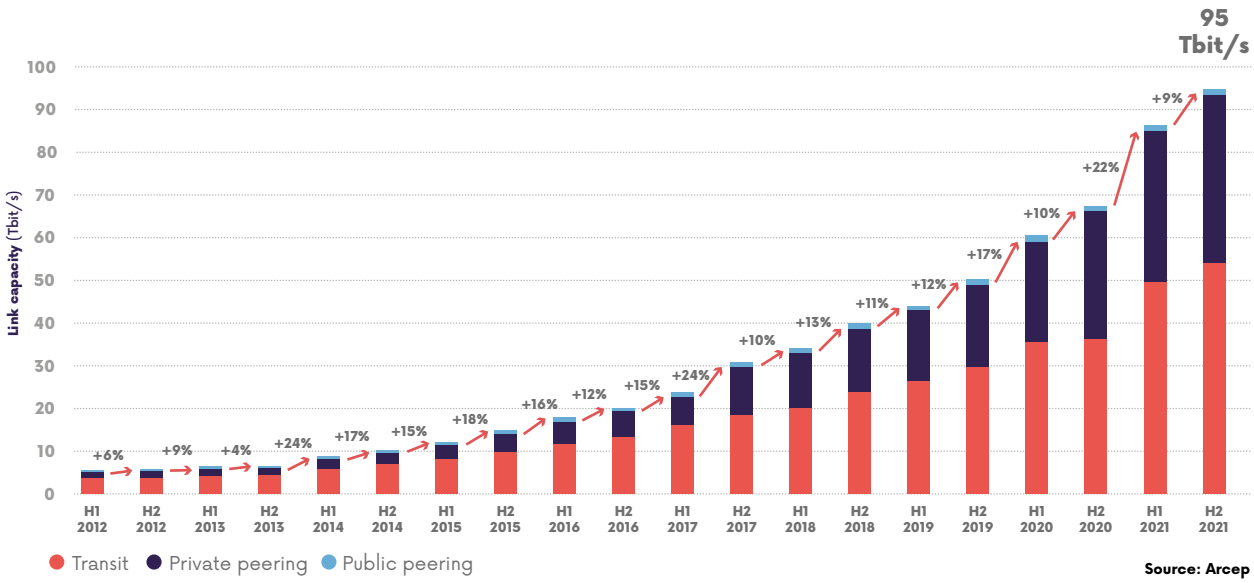
Source: Arcep

2.3. Evolution of installed capacities

Installed interconnection capacities have increased at the same pace as inbound traffic. Installed capacity at the end of 2021 is estimated at 95 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 H2-2021



Source: Arcep

2.4. Evolution of interconnection methods

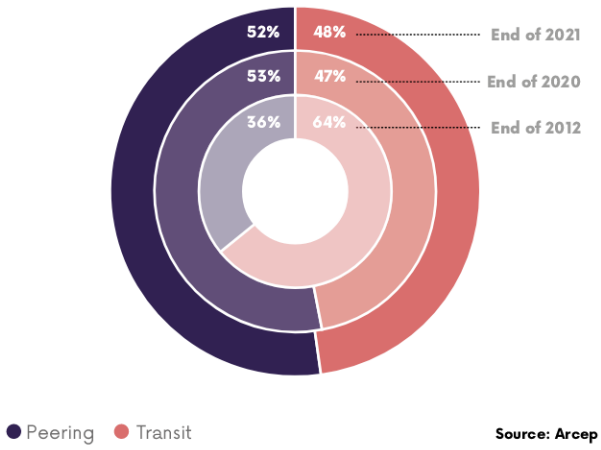
Peering vs. Transit

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.

However, between the end of 2020 and the end of 2021, peering's share decreased slightly: from 53% at the end of 2020 to 52% at the end of 2021. The situation is due, on the one hand, to the increase in transit traffic (including traffic from Open Transit International) and, on the other, to some of the peering traffic being replaced by traffic coming from on-net CDNs.

EVOLUTION OF PEERING AND TRANSIT FOR THE MAIN ISPs IN FRANCE

(in proportion of inbound traffic volume)



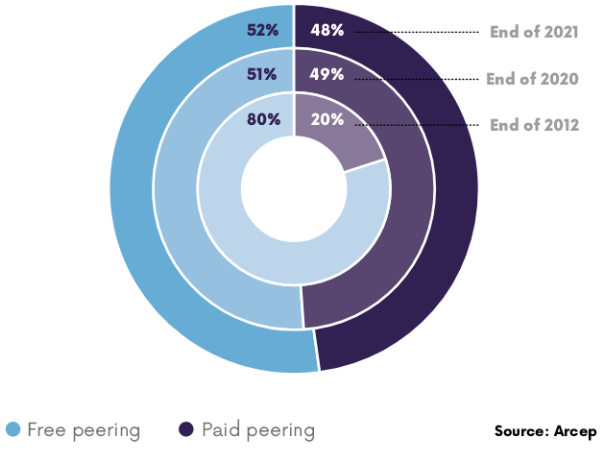
Source: Arcep

Free vs. paid peering

Peering's share of interconnection has changed very little since last year (49% at the end of 2020 and 48% at the end of 2021). This slight decrease can be explained, on the one hand, by the increase in free peering (private peering between players of comparable sizes and public peering) and, on the other, by the transfer of paid peering traffic between CAPs and ISPs to on-net CDNs.

EVOLUTION OF PAID PEERING PARTS FOR THE MAIN ISPs IN FRANCE

(in proportion of inbound traffic volume)



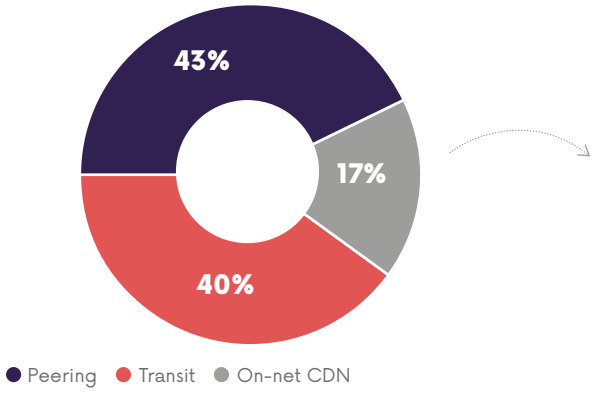
Source: Arcep

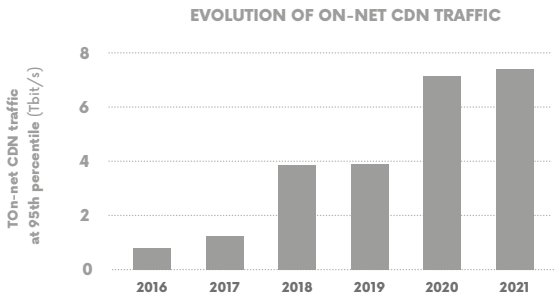
2.5. Traffic breakdown by interconnection type

Between the end of 2020 and the end of 2021, traffic coming from on-net CDNs to the four main ISPs' customers increased slightly to reach around 7.4 Tbit/s. The percentage of traffic from on-net CDNs (17%) decreased compared to last year (21%), which confirms that peering and transmit remain ISPs' two most widely used interconnection methods.

This percentage varies considerably from one ISP to the next: for some ISPs, 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 1:8 and 1:15 depending on the operator. In other words, data streams made available through on-net CDNs are viewed between five and fifteen times, on average.

BREAKDOWN BY INTERCONNECTION TYPE OF TRAFFIC TO CUSTOMERS OF THE MAIN ISPs IN FRANCE (END OF 2021)





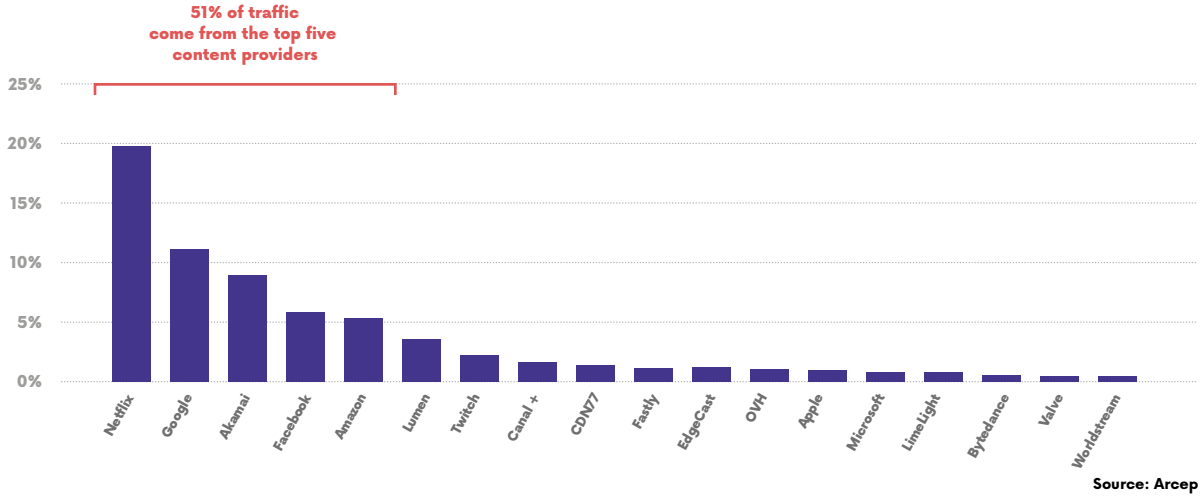
Source: Arcep

2.6. Traffic breakdown by origin

51% of all traffic to the customers of France's main ISPs come from five providers: Netflix, Google, Akamai, Facebook and Amazon. 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.

The presence of several CDNs in the traffic breakdown presented below confirms the major role these players have in the routing of Internet traffic. For example, Disney+ appears in this ranking through its various CDNs.

BREAKDOWN BY ORIGIN OF TRAFFIC TO CUSTOMERS OF THE MAIN ISPs IN FRANCE (END OF 2021)



Source: Arcep

2.7. Price changes

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 €0.05 (excl. VAT) to several euros (excl. VAT) per month and per Mbit/s. For paid peering, prices range from between €0.25 (excl. VAT) to several euros (excl. VAT) per month and per Mbit/s[19].

On-net CDNs 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.

A peek inside data centers: the Interxion example

Data centers provide their customers with:

- energy: guaranteeing uninterrupted power supply;
- cooling: guaranteeing a stable temperature range;
- security: guaranteeing physical safety and security via access control, protection against natural phenomena (lightning or floods), fire detection and suppression, etc.;
- interconnection: providing the ability to connect to networks and the data center's other customers in a secure fashion (with redundant paths).

These photos illustrate these main functions in the Interxion data centers in the Paris (PAR7) and Marseille (MRS1 and MRS2) areas.

Energy

A generator set is started if the power supply is lost.

Batteries continue to power the servers during the time it takes for the generators to start up and synchronise.

Inverters convert the direct current from the batteries into alternating current.

All of these elements are redundant, to ensure that an electrical power outage will not affect the server's power supply.

Cooling

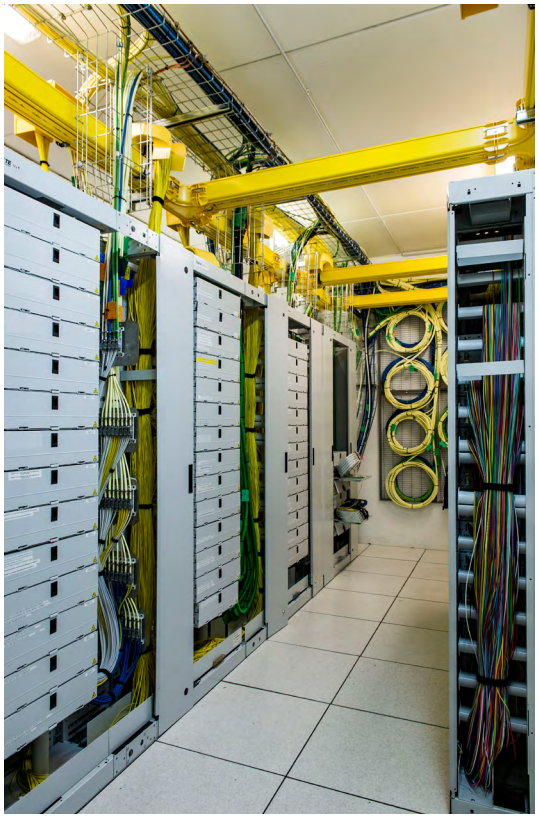
Several technical solutions are available, including multiple air conditioning systems.

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

Some data centers use an underground water-cooling system: via a plate heat exchanger at the Interxion data center in Marseille.

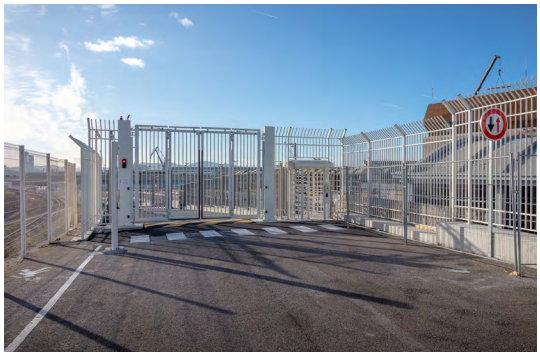
Interconnection

Data centers are outfitted with two meet-me-rooms (MMR) where all of the different bays' fibers and cables arrive. Why two rooms? To provide different cable paths to avoid there being a single point of failure (SPOF).



Security

Physical safety and security.



Airlocked entrance room.

Automatic fire detection and suppression (without having to switch off the servers' power supply).

CHAPTER 3

ACCELERATING THE TRANSITION TO IPv6

What you need to know

The rate of IPv6 use is increasing in France, reaching around **50%** in November 2021.

In November 2021, the IPv6 task force published a second handbook: "Enterprises: how to deploy IPv6?"

The IPv6 task force co-chaired by Arcep and Internet Society France has more than **120 members:** join the task force!

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[20].

1. Phasing out IPv4: the imperative transition to IPv6[21]

IPv4, which has been used since 1983, provides an addressing scheme of close to 4.3 billion addresses[22]. 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 2020, the top operators in France (Bouygues Telecom, Orange, SFR[23]) had already allocated between around 93% and 98% of their IPv4 addresses[24].

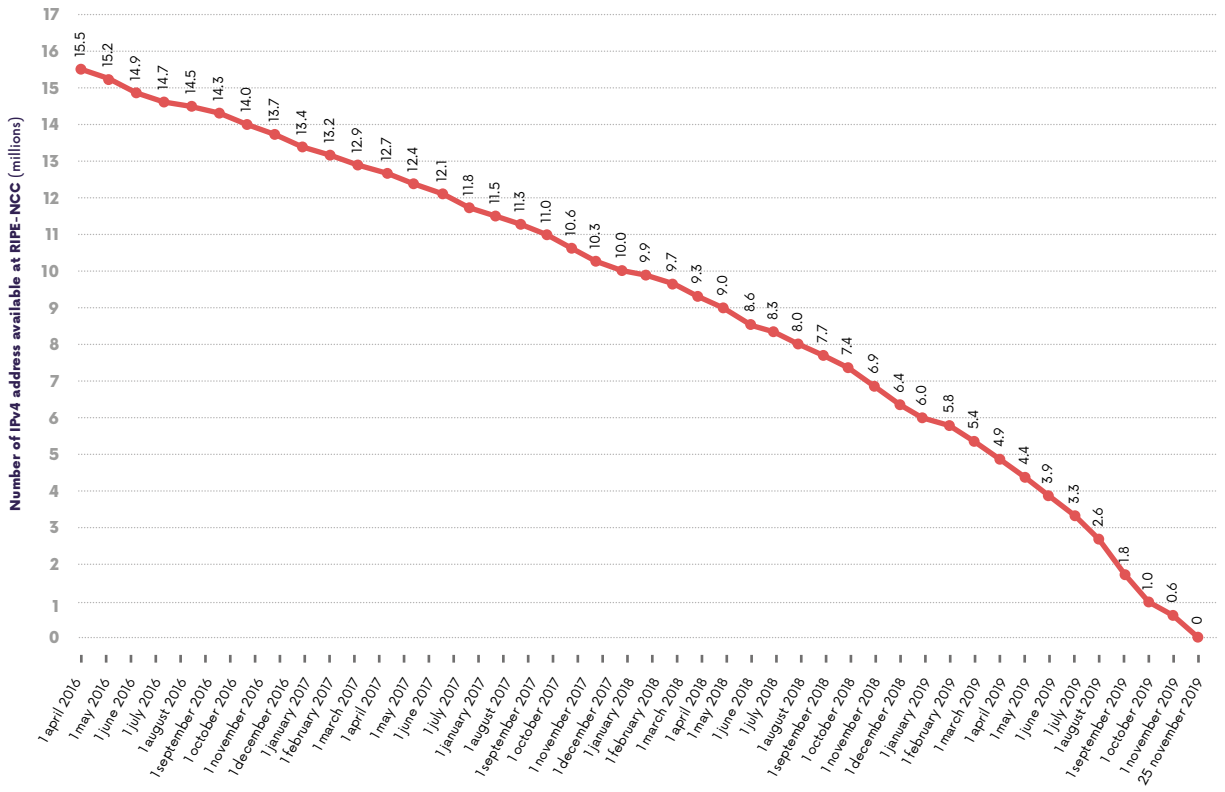
IPv6 specifications were finalised in 1998. They incorporate functions for increasing security by default and optimising routing. Above all, IPv6 delivers an almost infinite number of IP addresses: 667 million IPv6 addresses for each square millimetre of the earth's surface[25].

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 2021 the process was still only in the cohabitation stage.

Europe is currently experiencing a shortage of IPv4 addresses. 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 allocation n (i.e. 1024 addresses) from the last remaining IPv4 addresses in their pool.

20. 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).
21. 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.
22. IPv4 addresses use a 32-bit code. A maximum of 2^{32}, or 4,294,967,296 addresses can theoretically be assigned simultaneously.
23. Free did not provide the number of IPv4 addresses already assigned.
24. Data collected by Arcep from ISPs, in accordance with Arcep Decision No 2020-0305.
25. IPv6 addresses are encoded over 128 bits. In theory, a maximum of 2^{128} (or approximately 3.4×10^{38}) addresses can therefore be assigned simultaneously.

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. This is 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 service (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. The price of an IPv4 address on the secondary market, which was around 25 dollars per IP address in mid-2020, today can run as high as 60 dollars per IP address. Added to which, IPv4 addresses 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.

This shortage of IPv4 addresses, and the ensuing risks, make the transition to the new Internet communication protocol especially crucial to sustaining 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 galvanise the community and help speed up this transition.

Open floor to

VÉRONIQUE NEY
*Co-chairs of the Open Internet working group - **BEREC***

KLAUS NIEMINEN
*Co-chairs of the Open Internet working group - **BEREC***

BEREC FOLLOWS THE IPv6 DEPLOYMENT IN EUROPE AND FOSTERS INFORMATION SHARING BETWEEN NRAs

BEREC is following the IPv6 developments, even if it has no formal mandate in the field of IPv6. Considering BEREC's strategic priorities – promoting full connectivity, supporting sustainable and open digital markets, empowering end-users – it is clearly desirable for BEREC to place an emphasis on IPv6 adoption across Europe.

For the provision of applications and services, an Internet access service end-user's endpoint needs to be reachable by other endpoints. Therefore, a sufficient number of public IP addresses are needed so that end-users can use and provide services and that the Internet continues to function as an engine for innovation. This is also the goal of the Open Internet Regulation and explains why this topic is relevant for BEREC.

The IPv4 protocol offers an addressing space of around 4.3 billion addresses. However, the success of the Internet, the diversity of uses and the proliferation of connected objects (IoT) have as a direct consequence the growing exhaustion of IPv4 addresses, especially in the recent years. Europe is facing a shortage of IPv4 addresses nowadays and IPv4 alone cannot support growth of the Internet. Hence, the transition to IPv6 is required.

Various sources of data show that the IPv6 adoption rate differs significantly between countries. Even though some BEREC member countries are leading the IPv6 deployment, many BEREC member and participant countries are below the global average and in some of these countries the deployment has not even started.

The differences observed between BEREC member and participant countries are mainly due to national circumstances. There are differences with regard to competencies in the transition to IPv6 and actions taken at the national level. For instance, in some countries the responsibility in this matter lies with a public authority, while in others it is up to the industry or it is subject to self-regulation. However, it is possible that two countries with different institutional settings regarding the responsibility have a similar IPv6 adoption rate. NRAs active in the area have taken actions based on their general mandate and objectives to promote connectivity and availability and general quality of Internet access services.

BEREC has also done some work in this field. Key activities performed thus far include:

- Gathering information from invited stakeholders to a virtual workshop (October 2020);
- Providing an overview of the state of IPv6 across Europe and thus raising NRAs' awareness on the transition to IPv6 (January 2021);
- Presenting BEREC's perspective in the "National Workshop for Montenegro on IPv6 strategy, policy and implementation", jointly organised by EKIP and ITU (April 2021) ;
- Hosting a virtual public technical workshop with the participation of several key European stakeholders involved in the transition to IPv6 (May 2021).

BEREC will also continue having internal discussions and *"sharing of information on relevant market developments like the IPv6 deployment in BEREC members and participants without voting rights"*, according to Section 2.4.2 of the Annual Work Programme 2022.

China plans to accelerate the transition to the IPv6 protocol and to have IPv4 completely phased out by 2030

On 23 July 2021, China's Central Cyberspace Affairs Commission and Cyberspace Administration unveiled a three-stage plan to have IPv6 replace IPv4 on the different Internet access and hosting services located in China:

- By the end of 2023: all new routers will fully support IPv6 by default. Standalone 5G networks will be IPv6 only and will no longer use private IPv4 addresses.
- By the end of 2025: networks, platforms, applications, devices and various industries must be deployed with IPv6 running by default. New websites, applications, installations and security systems will fully support IPv6.
- By the end of 2030: the goal is to complete the transition to IPv6 by switching off the IPv4-compatible layers. At this point, China is due to have a single stack IPv6 network, and no longer be using the IPv4 protocol for either servers or customers.

China wants to become the world's IPv6 leader and is applying pressure to accelerate its deployment as, according to regulators, it is "an inevitable trend in Internet upgrading, a key direction of cyberspace technology innovation, and a key supporting infrastructure for a powerful cyberspace country".

In February 2022, China ranked 39th amongst the 100 countries with the most Internet users, with a 17% IPv6 adoption rate for Internet access. Arcep provides statistics that are updated every two months on its page: "IPv6 statistics on the 100 countries with the most Internet users".

Controlling how incoming IPv6 packets are forwarded by the router: PCP

Most ISPs have an IPv6 firewall by default that blocks unsolicited incoming IPv6 packets, to reduce security risks. Some applications, such as online gaming, and certain network equipment (e.g. accessing a NAS or an IP camera via the Web) requires opening streams on the ISP router's IPv6 firewall.

It is to address this issue that the Port Control Protocol (PCP) was standardised in 2013 (RFC 6887[1]) as the successor to the NAT-PMP port mapping protocol.

A PCP server runs on routers and authorises incoming software with a PCP client to ask it to forward an IPv6 stream on an IPv6 address and a specific port for a specific period of time.

PCP is a new protocol that creates the ability to forward unsolicited inbound streams (e.g. for online games) regardless of the protocol. It is therefore compatible with IPv4 and IPv6 as well as the multiple technical solutions used with IPv4 and IPv6 such as traditional NAT, NAPT (Network Address and Port Translation), Carrier Grade NAT, DS-Lite and NAT66. It should nonetheless be noted that, if RFC 6887 enables PCP to manage these different cases, some equipment has not yet implemented the protocol.

1. FC 6887: Port Control Protocol (PCP).

Open floor to

BRUNO BOUTTEAU
*Information Systems Project Manager - **Grand Est Regional Health Agency (ARS)***

THE TRANSITION TO IPv6 IN THE GRAND EST REGIONAL HEALTH AGENCY

Project background:

Since the start of the 2000s, every healthcare establishment's internal and external networks have been based on the Internet Protocol (IP). IP enables devices with an IPv4 address to communicate over the Internet andon an Intranet.

Why do we need to accelerate the transition from IPv4 to IPv6?

Getting a jump on a change in technical standard helps create a lever effect by fostering healthcare establishments and their suppliers' awareness of the issue through support for vanguard projects. Over time, this form of investment support will help lighten the spending needed for the transition. Healthcare establishments have highly complex and costly technical facilities, including operating rooms, radiology departments, biology labs, sequencers…

Findings for 2017-2018: still uneven progress amongst operators

On fixed networks, a very large percentage of the top four operators' customers have an IPv6-ready boxes. Among these compatible customers, however, the percentage that is IPv6-enabled, in other words who are sending and receiving traffic over IPv6, still varies a great deal depending on the ISP.

As RIPE projections for Europe show, telecom operators will begin encouraging use of IPv6 – in the same way that operators with infrastructures that are more than 50% IPv6-ready were already doing in 2021 in several countries, including France.

From a concrete perspective, this will translate into higher prices, with IPv4 becoming a paid option in an IPv6-based service, before being steadily phased out for economic reasons, and as compatible hardware becomes obsolete.

These changes all underscore the need to make the transition to IPv6, especially given the interconnected nature of establishments and geographic sites that make up regional hospital complexes.

This is why the Grand Est Regional Health Agency (ARS) created a two-phase financing programme: a study phase and a technical work phase.

A call for proposals was drafted and disseminated to the most strategic establishments, inviting them to apply for this backbone programme.

PHASE 1

Obtaining a diagnosis and a technical financial impact study from a specialised service provider within a regional hospital complex.

The Grand Est ARS was granted a non-recurring subsidy in the amount of €50,000, in accordance with the criteria set forth in the IPv6 call for proposals.

PHASE 2

Carrying out the work needed to make the transition from IPv4 to IPv6 based on the recommendations contained in the technical financial impact study produced by a specialised service provider within a regional hospital complex.

The Grand Est ARS was granted a non-recurring subsidy in the amount of €100,000, in accordance with the criteria set forth in the IPv6 call for proposals.

BENEFICIARY ESTABLISHMENTS:

The financing programme for establishments was set up in 2018:

- Financed in 2018: Strasbourg teaching hospital (CHU), Regional hospital complex (GHT) Coeur Grand Est, Nancy teaching hospital, Reims teaching hospital;
- Financed in 2019: Fondation Vincent de Paul, Civilian Hospitals of Colmar;
- Financed in 2020: Regional medical centre of Metz Thionville;
- Financed in 2021: GHRMSA in Mulhouse.

The impact studies have been completed and, if the technical work has begun, the transition is not expected to be complete until 2025 at the earliest.

Open floor to

APAR GUPTA
*Executive Director - **Internet Freedom Foundation, India***

PRATEEK WAGHRE
*Policy Director - **Internet Freedom Foundation, India***

THE NEED FOR A IPv6 POLICY PUSH IN INDIA

Digitisation is a core pillar in India's public policy for meeting welfare and economic goals. This makes the IPv6 transition immensely necessary. Here, India has among the largest shares of IPv6 adoption in the world. APNIC and NIXI estimate that IPv6 adoption in India exceeds 75%. Google's per-country IPv6 adoption tracker lists India as having over 60% IPv6 penetration against a global average below 40%, while Akamai's IPv6 visualization indicates that adoption in India exceeds 50%.

The need for a roadmap to transition from IPv4 to IPv6 was highlighted in the Ministry of Electronics and Information Technology's (MEITY) annual report for 2004-05. In 2010 the Department of Telecommunications (DoT) published the first *National IPv6 Deployment Roadmap* which recommended that major service providers should target having IPv6 capability in 18 months. It required the union and state government ministries, and public sector units to start using IPv6 services in 22 months and the creation of an India IPv6 Task Force which would eventually be replaced by a *Center for Innovation* that would serve as a dedicated national organization. The task force consisted of an Oversight Committee – which would take policy decisions and set strategic direction, a Steering Committee – that could coordinate amongst stakeholders and oversee the various working groups constituted, and ten Working Groups tasked with specific activities such as training/awareness, network implementation, standards, support, network security etc. As the transition progressed, various Working Groups were combined and reduced to six and four in 2013 and 2016 respectively. The operational working groups today are: IPv6 Awareness, Knowledge and Resource Development; IPv6 Security; Pilot Projects; and Readiness of Content, Cloud Services and End User Devices.

Since the 2010 roadmap, IPv6 transition plans have been updated periodically with a revised roadmap in 2013, and subsequent timeline extensions in 2016, 2020 and 2021. Notably, in 2020, the DoT recognised the role of market forces for content/application providers and cloud computing/data centers. However, the transition timelines for government organizations and TSPs/ISPs, have been periodically extended and have not been met. As per the most recent revision, government organizations are to complete the transition to IPv6 by July 2022, and new wireline customer connections after December 2022 should be able to support native/dual tack IPv6 traffic.

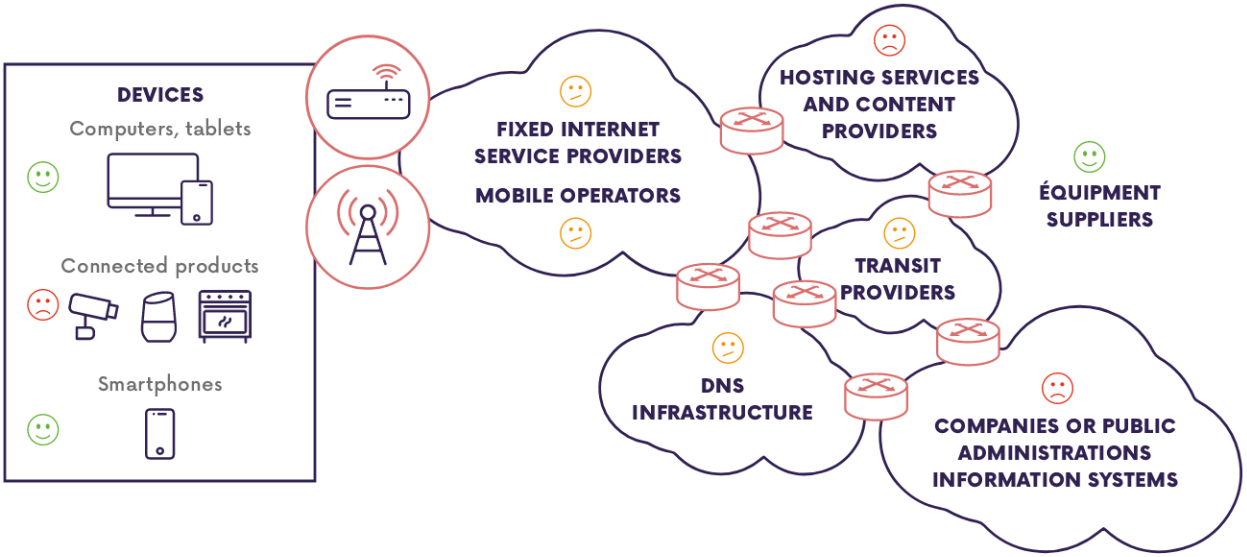
A daily IPv6 deployment tracker that monitors specific Government, Industry and University domains shows that no progress has been made for 62%, 41% and 32% of them respectively. For service providers, industry voices/analysts also cite the role of greenfield network deployments[1].

Meanwhile, ASN level data from NIXI and APNIC reveals that a long-tail of ASNs still receive low percentages of IPv6 capable connections. In order to capitalize on high adoption rates and the combination of proactive and responsive interventions to complete the transition from IPv4 to IPv6 will require the IPv6 ecosystem in India to: sustain its efforts thus far; continue to study and adopt global best practices.

1. Geoff Huston, 'What Drives IPv6 Deployment?', RIPE Labs, 23 May 2018,; Jagmeet Singh, 'How India Is Leading the World's March Towards IPv6 (And What It Means)', NDTV Gadgets 360, 4 February 2019 ; Muntazir Abbas and Danish Khan, 'India Becomes Largest IPv6 Subscriber, Seeks Self-Reliance in Internet Domain', The Economic Times, 3 February 2021.

2. Barometer of the transition to IPv6 in France

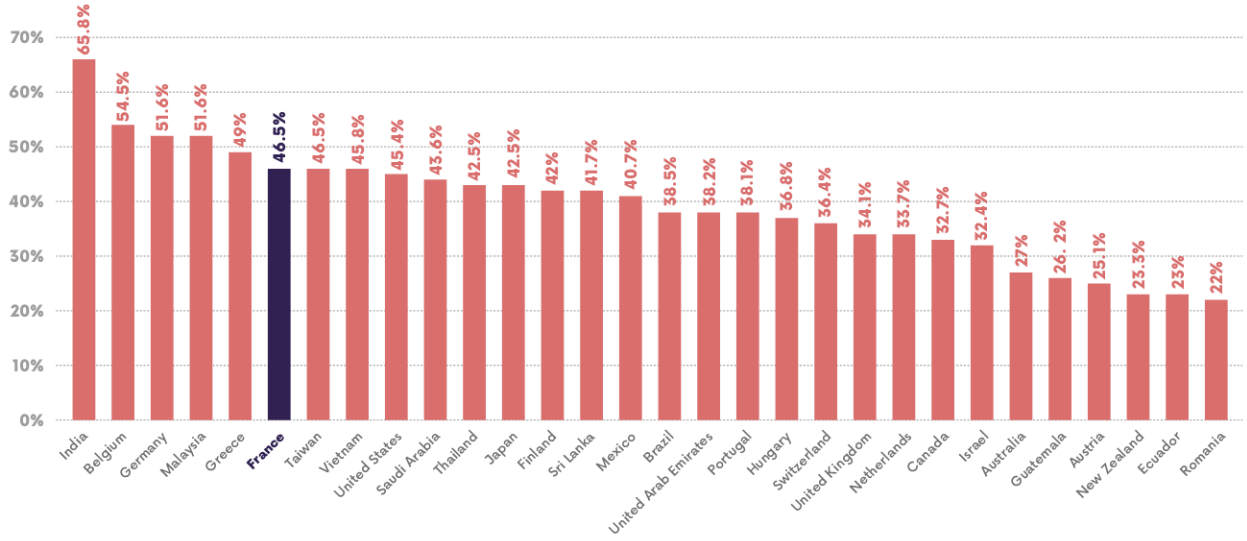
STATUS OF THE TRANSITION TO IPv6 OF THE DIFFERENT LINKS IN THE TECHNICAL CHAIN



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

Source: Arcep

TOP 30 COUNTRIES IN TERMS OF IPv6 ADOPTION



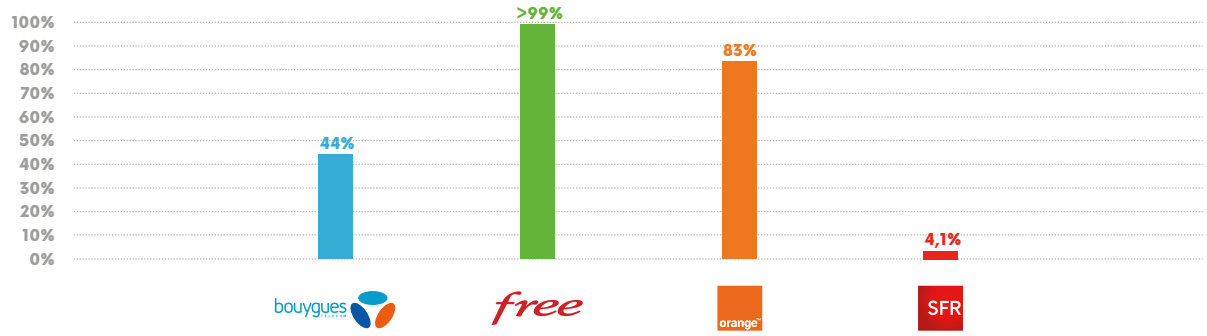
Source: median of "Google IPv6 adoption", "Akamai IPv6 adoption", "Facebook IPv6 adoption", "Apnic IPv6 adoption" data from October 2020. Pertains only to the 100 countries with the most internet users.

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[26]. Arcep published the 2021 edition of the barometer on 29 November 2021. As detailed here below, not all stakeholders are at the same stage of the transition.

This 2021 edition of the barometer revealed substantial progress on IPv6 with a rate of adoption that reached close to 50%[27]. France has significantly improved its place in the global IPv6 adoption rankings, going from tenth place at the end of 2020 to sixth place today, according to the median score of the four main sources of publicly available data assessing IPv6 adoption: Google, Akamai, Facebook and Apnic[28]. France ranks fourth in Europe, behind Belgium, Germany and Greece.

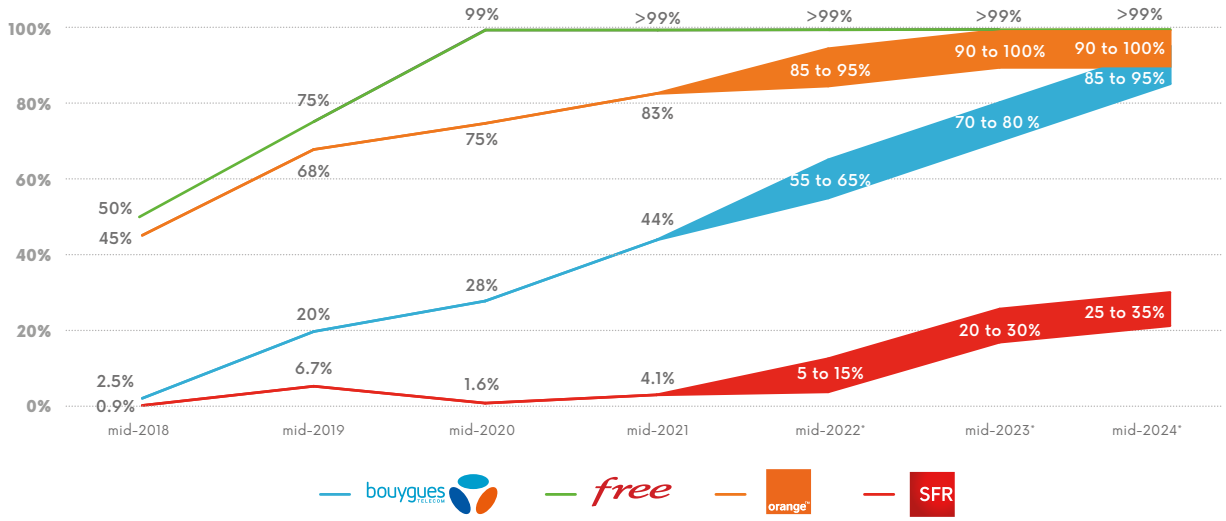
The barometer shows in detail the status of the transition for the Internet ecosystem's different stakeholders. Find IPv6 statistics on the top 100 countries in number of web surfers, updated every two months on Arcep website.

FIXED NETWORK: PERCENTAGE OF IPv6-ENABLED CUSTOMERS



Source: data as of the end of June 2021, collected by Arcep from operators.

FIXED NETWORK: PERCENTAGE OF IPv6-ENABLED CUSTOMERS EVOLUTION



* Figures subject to change

Source: data as of the end of June 2021, collected by Arcep from operators.

26. Arcep Decision No. 2021-0375 on implementing surveys in the electronic communications sector.
27. Based on "Google IPv6 adoption".
28. Based on the median of "Google IPv6 adoption", "Akamai IPv6 adoption", "Facebook IPv6 adoption", "Apnic IPv6 preferred" data from October 2021. Aggregation of national data is prorated based on the number of Internet users (source: Wikipedia, data as of 09/08/2021). The median of the four sources is calculated country by country, before being aggregated on a pro-rated basis, according to the number of Internet users in each region.

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.

On the fixed networks, Arcep notes significant disparities between the main telecom operators in their transition to IPv6:

- - The percentage of IPv6-enabled SFR customers, all technologies combined, rose from 1.6% by mid-2020 to 4.1% by mid-2021. As upcoming activations also remain insufficient (between 20% and 30% by mid-2023 and between 25% and 35% by mid-2024), SFR is being urged to accelerate the transition to IPv6 on its fixed network substantially, in particular on FttH, and to begin this transition on cable. Because the vast majority of users will not take the initiative to enable IPv6 manually, Arcep is encouraging SFR to systematically perform this configuration by default.
- - Although deployment efforts have been observed (around 44% of customers activated by mid-2021 compared to 28% by mid-2020), Bouygues Telecom is once again being urged to continue and to step up deployment efforts on its fixed network.
- - On fixed networks, the current percentage of Free and Orange customers who are IPv6-enabled is relatively high (approximately more than 99% and 83% respectively) and have increased. The projections for mid-2024 for Orange are encouraging (between 90% and 100%).
- - Bouygues Telecom, Free and Orange are being urged to begin the transition on 4G fixed wireless as soon as possible. SFR in particular, whose 4G fixed wireless customers are all IPv6-ready, is being encouraged to perform IPv6 activation by default on this technology.

Several initiatives amongst operators with between 5,000 and 3 million customers on fixed networks are encouraging, notably those taken by Orne THD which had already migrated all of its customers by 2019 and Vialis which started its transition last year (1% by mid-2020) and already 88% of its customers are IPv6-enabled. Zeop meanwhile went from 0.1% IPv6-enabled customers in mid-2020 to 21% by mid-2021. The percentage of IPv6-enabled customers for Coriolis (72%), KNet (17%) and OVH Télécom (19%) has decreased compared to last year, which is cause for concern.

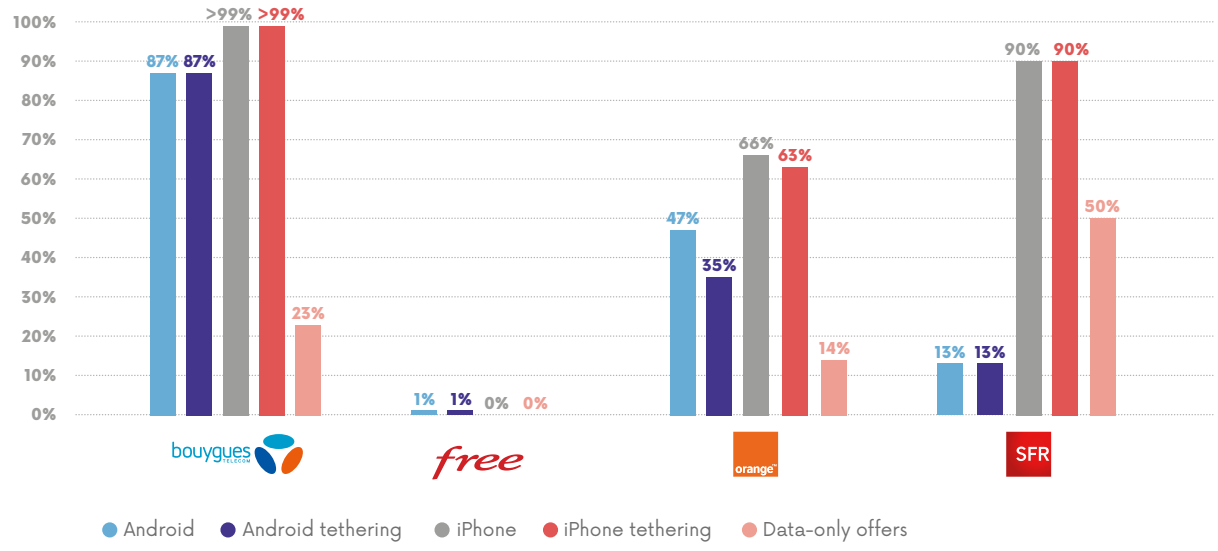
Alsatis, bigblu, Nordnet, Ozone, SFR Caribbean, SFR Réunion Mayotte, VidéoFutur and Wifirst, on the other hand, have not initiated their transition to IPv6 and do not yet plan to do so. K-Net and OVH Télécom were unable to provide their deployment forecasts. Even if several operators planned to accelerate their transition in 2021 (Coriolis Telecom, Vialis and Zeop) and that two additional operators (Canal+ and Tubéo) plan to start their transition this year, the rate of deployment still seems largely insufficient to deal with the shortage of IPv4 addresses[29].

To improve its monitoring of the transition to IPv6, Arcep expanded its information gathering to include operators who market solutions designed for business customers – aka "Pro" plans – on their fixed network. Arcep notes that the deployment of IPv6 continues to fall short, and urges operators to include IPv6 in their plans for businesses[30].

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.

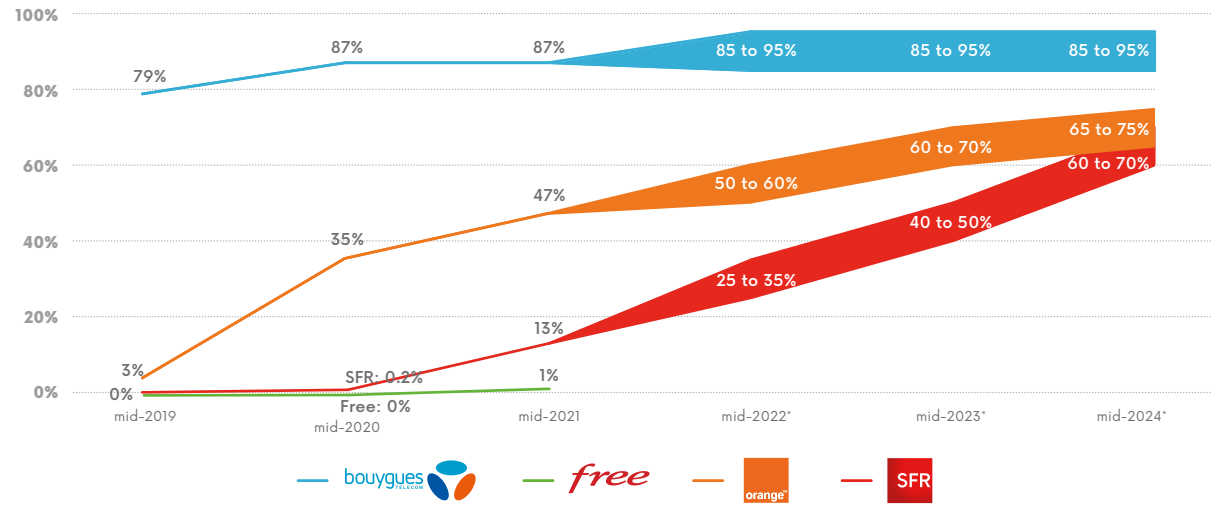
MOBILE NETWORK: PERCENTAGE OF IPv6-ENABLED CUSTOMERS



Source: data as of the end of June 2021, collected by Arcep from operators

29. 2021 Arcep IPv6 Barometer, "Operators with between 5,000 and 3 million customers on fixed networks". Click here.
30. 2021 Arcep IPv6 Barometer, "Operators providing 'Pro' plans on their fixed networks". Click here.

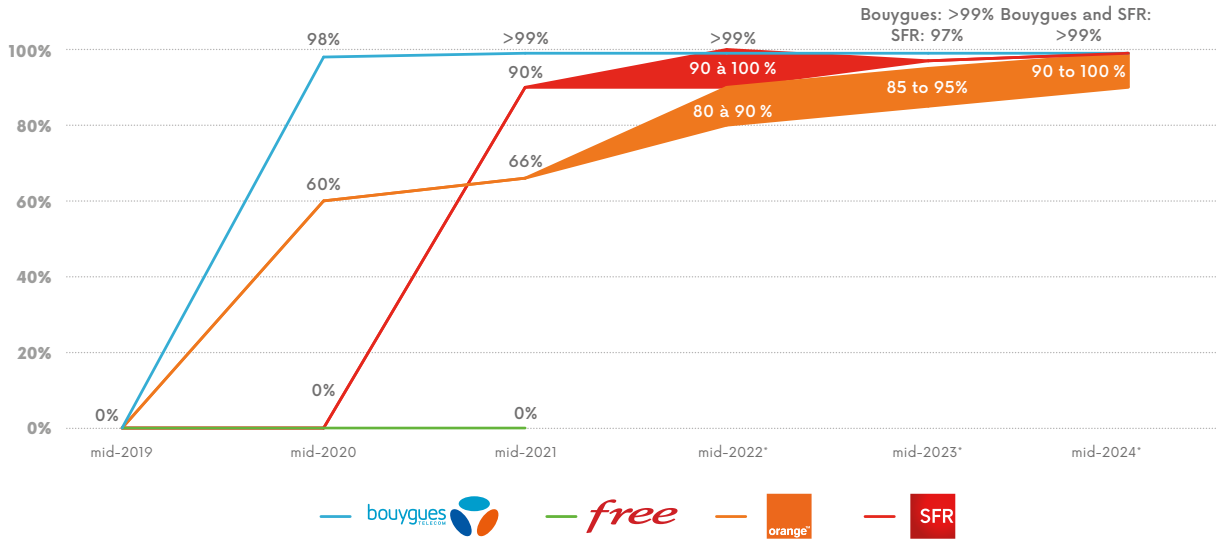
ANDROID: PROGRESSION OF IPv6-ENABLED CUSTOMERS



* Figures subject to change

Source: data collected from operators by Arcep, as of end of June 2021

iPHONE: PROGRESSION OF IPv6-ENABLED CUSTOMERS



* Figures subject to change

Source: data collected from operators by Arcep, as of end of June 2021

Arcep notes significant progress in the deployment of IPv6 on mobile networks but invites operators to continue their efforts to accelerate full support for IPv6 in their various plans:

- Bouygues Telecom has achieved a noteworthy deployment on mobile networks, with 87% of Android customers and more than 99% of iPhone customers IPv6 enabled in mid-2021.
- IPv6 on the Orange mobile network is also worth noting (47% of Android customers and 66% of iPhone customers IPv6 enabled). Orange is invited to continue its IPv6 activation of mobile devices.
- SFR has carried out a remarkable IPv6 push for its iPhone customers. The rate of iPhone IPv6-enabled customers has increased from 0% in mid-2020 to 90% by mid-2021. As the rate of Android IPv6-enabled customers as of mid-2021 (13%) and deployment forecasts for Android appear insufficient to cope with the IPv4 shortage, SFR is urged to step up the pace of providing IPv6 support for Android devices.
- It is particularly regrettable that Free Mobile does not support IPv6 by default for its mobile network plans, which has resulted in a very low percentage of IPv6-enabled customers (1% for Android and 0% for iPhone), and that the operator was unable to provide forecasts for upcoming support plans.
- Operators are all being called on to accelerate the pace of IPv6 deployment on their “data only” plans.

In order to better monitor the transition to IPv6 by the various mobile operators in France, and by the full-MVNOs[31] already included in the previous editions of this barometer, Arcep has broadened its collection of information to include light-MVNOs[32].

In Metropolitan France, thanks to the deployment of IPv6 within the main operators' networks, mobile operators with between 5,000 and 3 million customers that directly operate these operators' network access protocols (NAP) can provide their customers with IPv6 support. However, some of the operators with their own NAPs (China Telecom CTExcelbiz, Coriolis Telecom, Lebara Mobile, Lycamobile, Syma Mobile and Transatel) have not yet begun their transition and are not considering doing so.

In the French overseas departments and territories (DROM), Zeop is the only mobile operator with between 5,000 and 3 million customers that has begun to enable IPv6 on its network (30% in mid-2021) and has a target of between 35% and 45% of customers IPv6-enabled by mid-2022. The remaining operators do not plan to have deployed IPv6 by mid-2022. Further details are available in the IPv6 barometer[33].

There are sizeable disparities between perators when it comes to IPv6 deployment on their mobile network "Pro" plans. Operators are invited to begin and accelerate IPv6 deployment on all of their "Pro" plans. Further details are available in the IPv6 barometer.

IPv6-compatibility obligation for operators awarded 5G frequency licences

Arcep introduced an obligation to support IPv6 when awarding new frequencies:

- Metropolitan France: for operators that are awarded 5G frequencies in the 3.5 GHz band: "The licenceholder is required to make its mobile network compatible with the IPv6 protocol as of 31 December 2020" (excerpt from Decision No. 2019-1386).
- Réunion: for operators that are awarded frequencies in the 700 MHz and 3.5 GHz bands: "The licenceholder is required to make its mobile network compatible with the IPv6 protocol as of 31 December 2022" (excerpt from Decision No. 2021-0590).
- Mayotte: for operators that are awarded frequencies in the 700 MHz band: "The licenceholder is required to make its mobile network compatible with the IPv6 protocol as of 31 December 2022" (excerpt from Decision No. 2021-0591).

As stipulated in the reasons, the goal is to ensure services' interoperability and not hinder the use of services that are only available in IPv6, at a time when the number of user devices continues to grow and RIPE NCC has a shortage of IPv4 addresses.

This obligation is driven by the emergence of online services that are only available in IPv6 (no IPv4 connectivity). Some hosting solutions no longer offer IPv4 by default[1] and IPv6 is the only possible solution for accessing the NAS[2] of a customer connected to an ISP that uses CG-NAT. Which is why it is crucial that all customers be able to enable IPv6 on their mobile, to be able to access the entire Internet .

In its public consultation on the assignment of new frequencies (700 MHz, 900 MHz, 2.1 GHz and 3.5 GHz bands) in the French overseas territories, Arcep also proposed an IPv6-compatibility obligation:

- Guadeloupe and Martinique: for operators that are awarded frequencies in the 700 MHz and 3.5 GHz bands: "The licenceholder is required to make its mobile network compatible with the IPv6 protocol as of 31 December 2022" (excerpt from the public consultation).
- Saint-Martin: for operators that are awarded frequencies in the 700 MHz and 3.5 GHz bands: "The licenceholder is required to make its mobile network compatible with the IPv6 protocol as of 31 December 2022" (excerpt from the public consultation).
- Saint-Barthélemy: for operators that are awarded frequencies in the 700 MHz, 900 MHz, 2.1 GHz and 3.5 GHz bands: "The licenceholder is required to make its mobile network compatible with the IPv6 protocol as of 31 December 2022" (excerpt from the public consultation).
- Guiana: for operators that are awarded frequencies in the 700 MHz and 3.5 GHz bands: "The licenceholder is required to make its mobile network compatible with the IPv6 protocol as of 31 December 2023" (excerpt from the public consultation).

1. Example with the contribution from Ikoula in the 2020 report on the State of the Internet in France.
2. See lexicon.

31. See Lexicon
32. See Lexicon
33. 2021 Arcep IPv6 Barometer, "Operators with between 5,000 and 3 million customers on mobile networks". Click here.

Tutorial

How to activate IPv6 on your mobile phone ?

On its website, Arcep provides a step-by-step tutorial on how to activate IPv6 on your Android smartphone. iPhones do not currently allow users to modify the protocol themselves: your operator needs to ask Apple to perform the operation.

Reminder: the main operators' IPv6 activation policies are as follows[1]:

MOBILE NETWORK: IPv6 ACTIVATION POLICY

	bouygues	free	orange	SFR
IPv6-enabled by default on Android	YES Samsung S7 or newer Other manufacturers: new products from March 2018	NO Double activation of IPv6 by the customer required: on their Free customer area and on their Android device	YES Samsung S10 or newer Other manufacturers: new products from May 2020	YES SSamsung: S21 or newer Other manufacturers: new products from March 2021
IPv6-enabled by default on Android, with a shared connection			YES Samsung S20 or newer Other manufacturers: new products from January 2021	
IPv6-enabled by default on iPhone	YES iPhone 5S or newer, with iOS 12.2 or higher	NO Require iPhone 6S or newer, with iOS 15.4 or higher and an activation by the customer on their Free customer area	YES iPhone 7 or newer, with iOS 13.0 or higher iPhone 6S, 6S Plus and 6SE, with iOS 15.4 or higher	YES iPhone 6S or newer, with iOS 14.3 or higher
IPv6-enabled by default on iPhone, with a shared connection			YES iPhone 7 or newer, with iOS 14.0 or higher iPhone 6S, 6S Plus and 6SE, with iOS 15.4 or higher	
IPv6-enabled by default on data plans only	YES Progressive update of compatible devices	N/A	YES New products from January 2021	YES New products from March 2021

Source: data as of end of March 2022, collected by Arcep from operators.

When your mobile notifies you of an available update, do not hesitate to install it: in addition to correcting security flaws to increase your protection against being hacked, the update could enable IPv6 on your phone.

Go to the Arcep website for instructions on how to activate IPv6 on your Android smartphone, depending on your operator: https://www.arcep.fr/demarches-et-services/utilisateurs/activer-ipv6-mobile.html (in French).

1. More detailed information is available in the 2021 barometer of the transition to IPv6 in France.

2.3. Web hosting

Web hosting services continue to constitute one of the main bottlenecks in the migration to IPv6: only 29% of the most popular websites in France (compared to 26% in October 2020), according to Alexa rankings, are IPv6-enabled[34]. A site is considered IPv6-enabled if its domain name is mapped as being IPv6 (AAAA) in the DNS server record.

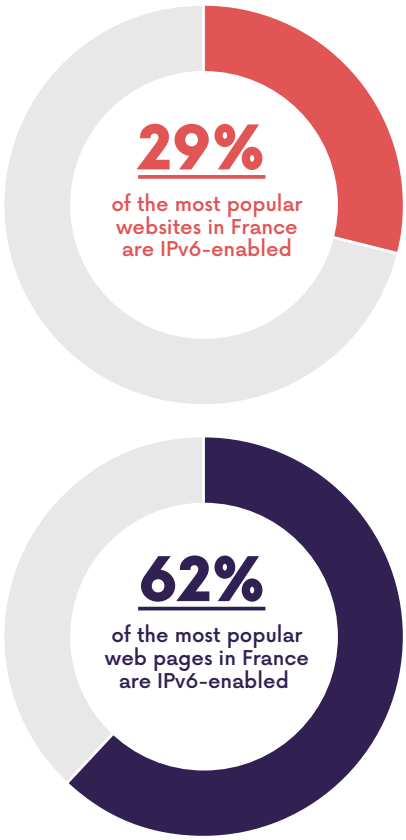
Note that the percentage of web pages that are IPv6-enabled (IPv6 content) is significantly higher than that (62%)[35]. The reason is that many of the smaller content providers operate websites (generally small number of pages viewed) that are not IPv6-compatible.

The percentage of IPv6-enabled sites stands at a mere 20% when looking at the 3.52 million .fr, .re, .pm, .yt, .tf, and .wf[36] websites. This percentage has been increasing since 2015, but the pace of this increase appears far from fast enough to enable a complete transition in the next few years.

Even if the vast majority of websites accessible in IPv6 are also accessible in IPv4 (the servers are configured in dual-stack with IPv4 + IPv6), a sharp increase in the number of websites accessible in IPv6-only can be noted. Some hosts do indeed offer IPv6-only solutions, charging extra for IPv4 compatibility. The sites hosted on these single stack IPv6-only servers are therefore not accessible to clients of IPv4-only operators. This situation testifies to the need to switch to IPv6 to avoid the development of an Internet split in two, with IPv4 on one side and IPv6 on the other.

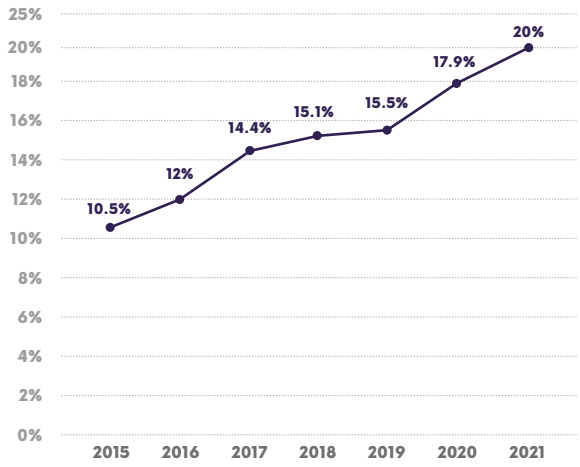
In September 2021, there were 1,028 domain names in .fr, .re, .pm, .yt, .tf and .wf accessible only in IPv6[37]. This number has doubled compared to 2020 (514 domain names), but remains very limited.

Even if several hosting services include IPv6 support in their solutions, the percentage of websites accessible in IPv6 is very low for all of the Top 10 web hosting services (in number of domain names) as it is not enabled by default. Among that Top 10, only IONOS 1&1 and Cloudflare[38] have more than three quarters of their sites IPv6 enabled, which make them standard bearers for the transition.



Source: 6lab Cisco as of 11/02/2021 (6lab.cisco.com). Data of the top 730 websites in France as ranked by Alexa (www.alexa.com/topsites/countries)

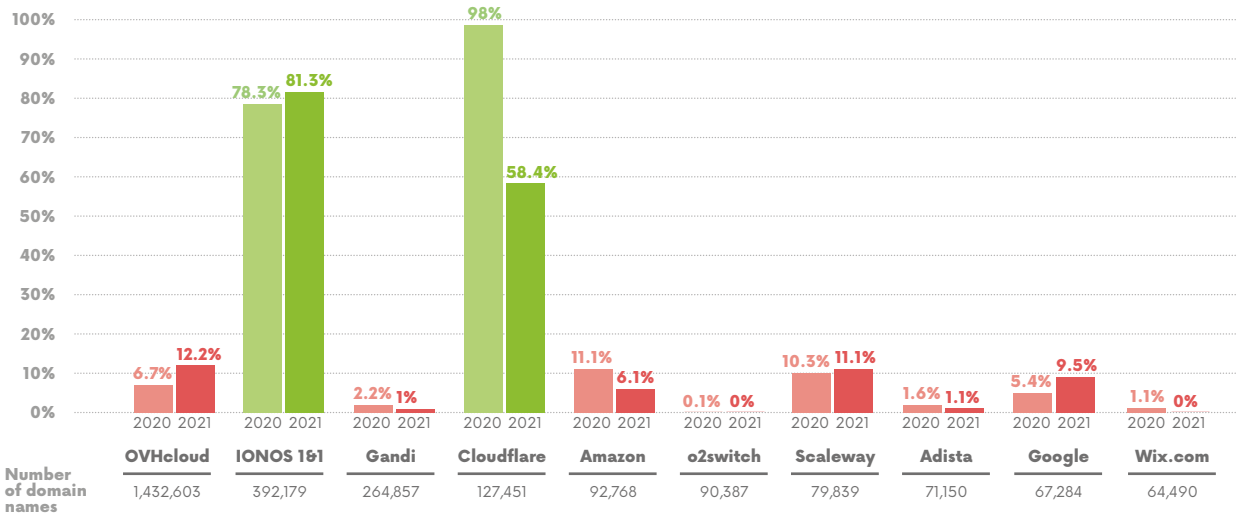
PROGRESSION OF IPv6-ENABLED WEBSITES on .fr, .re, .pm, .yt, .tf and .wf domain names



Source: Afnic data august 2021

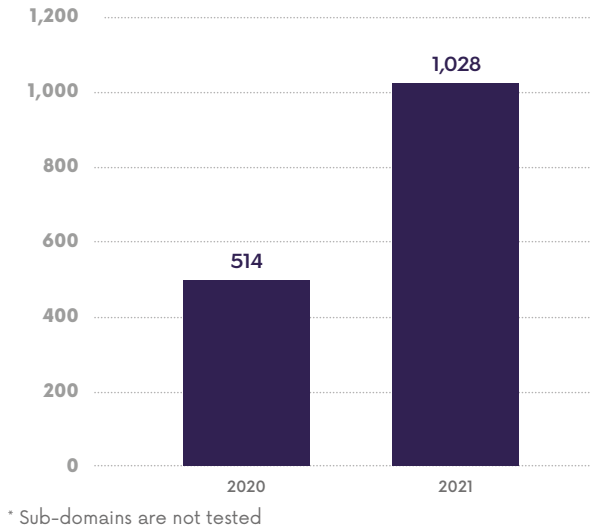
34. 6lab Cisco as of 31/10/2021. Data on the top 731 websites in France, Alexa rankings
35. Ibidem
36. Afnic data, August 2021. Data based on DNS zone information and analysis of A, AAAA, MX, and NS records configured on a domain name. The analyses of the DNS zones were carried out with the Zonemaster tool using an Afnic server. For each IP address retrieved, the MaxMind database was used to find the AS announcing this IP address.
37. This analysis is limited to the root domain: a subdomain accessible in IPv6-only will not be counted if the root domain is available in IPv4.
38. The percentage of IPv6-enabled websites at Cloudflare has fallen sharply (98% in mid-2020 compared to 58% in mid-2021). This can be explained by the partnership between Cloudflare and Shopify which resulted in Cloudflare supporting Shopify IP addresses which are IPv4 only.

PERCENTAGE OF IPv6-ENABLED WEBSITES on .fr, .re, .pm, .yt, .tf and .wf domain names



Source: Afnic data, August 2021

NUMBER OF IPv6-ONLY WEBSITES on .fr, .re, .pm, .yt, .tf and .wf domain names*



* Sub-domains are not tested

Source: Afnic data,September 2021

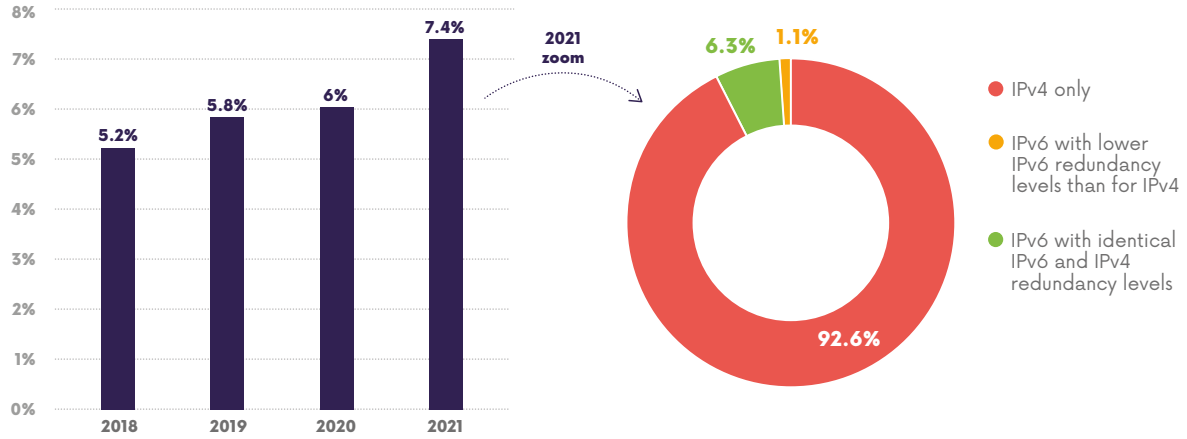
2.4. Mail hosting

The transition of the main mail hosting services is also proving very slow: only 7.4% of mail servers on .fr, .re, .pm, .yt, .tf and .wf domain names are currently IPv6-enabled (compared to 6% at mid-2020). 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[39].

Once again this year, the lack of IPv6-readiness amongst mail hosting services is alarming. If it is not remedied in the next few years, the protracted lag on this link in the Internet value chain could force IPv4 to be kept for longer than planned, with all the resulting costs. Only Google stands out here, with more than 95% of domain names for mail using IPv6.

39. Afnic data, August 2021.

PERCENTAGE OF IPv6-ENABLED MAIL HOSTING on .fr, .re, .pm, .yt, .tf and .wf domain names

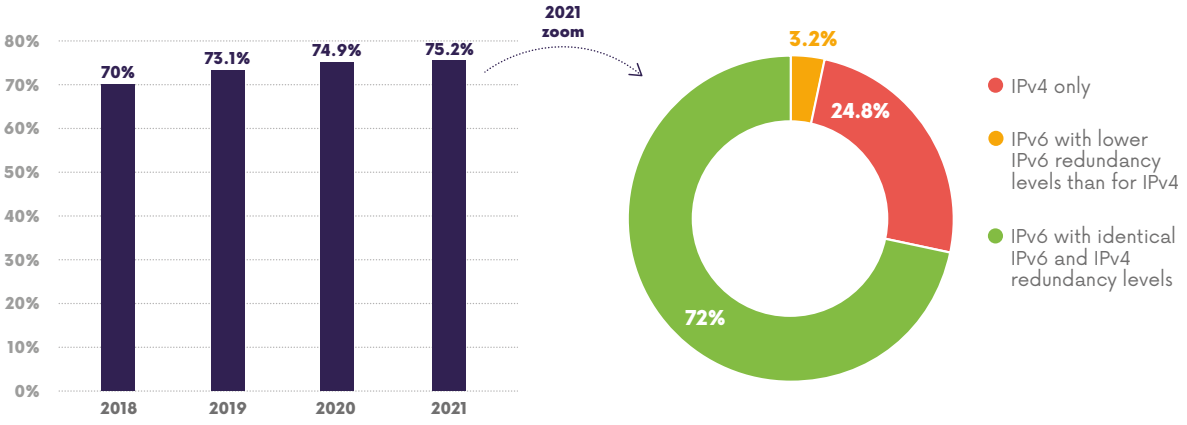


Source: Afnic data, August 2021

2.5. DNS Infrastructure

DNS infrastructure makes it possible to translate a domain name, e.g. www.arcep.fr, into an IP address. This is currently the sector that is the most advanced in the transition to IPv6, with around 73% of authoritative name servers supporting IPv6. Around 72%[40] of DNS servers guarantee an IPv6 resilience equivalent to IPv4 (identical redundancy levels).

PERCENTAGE OF IPv6-ENABLED DNS SERVERS on .fr, .re, .pm, .yt, .tf and .wf domain names



Source: Afnic data, August 2021

2.6. Government websites and online services (.gouv.fr)

Since having the government lead by example is one of the most important paths to an accelerated transition, the barometer has been enhanced with indicators on the progression of this transition to IPv6 by French government websites and online services. The current study pertains to the 243[41] sites with the .gouv.fr suffix and available in HTTPS[42].

DNS servers' transition to IPv6 is relatively well advanced and has progressed since last year, with 55% of them being IPv6-enabled, linked in particular to the IPv6 switchover of DNS hosting managed by Orange and Cegedim.cloud. Mail hosting, on the other hand, is still entirely in IPv4 and the percentage of government websites using IPv6 stands at only 2.9% for the main websites[43] and 0.9% for secondary ones[44].

40. Afnic data, August 2021.
41. There was an error in the 2020 edition of IPv6 barometer: only 145 sites (domain names starting with the letter «a» to the letter «l») had been taken into account.
42. Of the 1,009 existing domain names ending with .gouv.fr in August 2020, only the 243 whose HTTPS response has a valid TLS certificate were taken into account, and so excluding from the analysis domain names that are not being maintained or that are not attached to a website.
43. Main site: the site suggested/linked to by default by a search engine.
44. Secondary site: site that redirects to the main site (if the main site has the "www" prefix, the secondary site does not, and vice-versa).

Even if some sites are available in IPv6, it is regrettable that the vast majority are still using only IPv4 and that the progress has been very limited compared to last year, particularly given the goal of leading the transition to IPv6 by example. More attention could be paid to IPv6 compatibility when upgrading existing websites and when drafting specs for calls to tender to create new online services.

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

The next barometer will be published in the second half of 2022.

3. IPv6 task force galvanising the Internet ecosystem

3.1. The IPv6 task force is open to the entire ecosystem

Arcep and Internet Society France have set up a task force dedicated to IPv6 that is open to all Internet ecosystem stakeholders (operators, hosting services, businesses, government agencies, etc.). Its purpose is to accelerate the transition to IPv6 by enabling participants to discuss specific issues and share best practices.

The most pressing issue the task force identified was encouraging businesses to make the transition to IPv6. To this end, it published a handbook that explains to businesses why it is important for them to adopt IPv6.

3.2. Handbooks for businesses: "Enterprises: why switch to IPv6?" and "Enterprises: how to switch to IPv6"

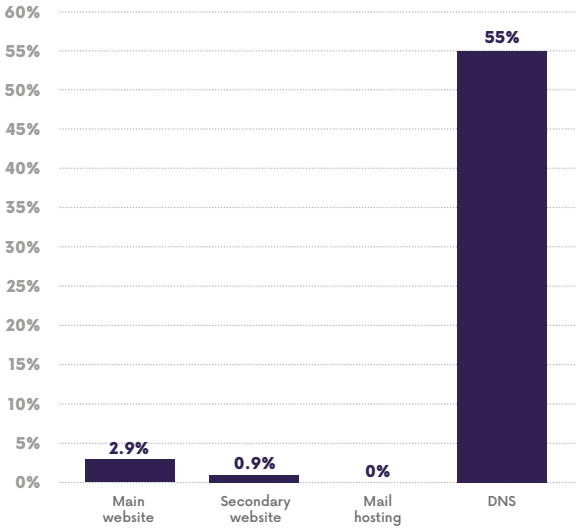
In December 2020, the IPv6 task force published a first handbook[45] which purpose is to increase businesses' awareness of how vital it is to switch to IPv6, and answers the most frequently asked questions:

- What are the drawbacks if I keep my local network in IPv4 or if the company website remains in IPv4?
- How long will it take to switch my company over to IPv6?
- What parts of the company infrastructure do I need to switch over to IPv6?
- Do the internal computers and servers need to be deployed in dual stack or in IPv6-only?

The handbook also includes four testimonials from companies that have already completed or are in the process of making the transition to IPv6:

- French power company, EDF, is an example of IPv6 migration undertaken for the information system of a corporation with 18 million IP addresses, and which has exhausted its pool of private IPv4 addresses. Rather than continue to "tinker" with ways to recover IPv4 addresses, EDF decide to switch some parts of its network to IPv6-only;
- Schneider Electric, a major manufacturer that is considering switching its internal network to IPv6 as some of its branch offices need to access IPv6-only Internet resources, and security issues have been reported on the LAN connections of Internet routers that are IPv6-enabled;
- Digdeo, a freeware services company that has committed to no longer relying on IPv4 NAT networks. The transition to IPv6 allowed it to resolve NAT issues for staff that needs to access backend resources;
- Olympique Lyonnais, an SME that was able to incorporate the migration to IPv6 into the larger project of building the new Olympic stadium in Lyon, which allows more than 60,000 people to communicate simultaneously during a match.

RATE OF IPv6 ADOPTION ON GOVERNMENT WEBSITES AND ONLINE SERVICES (.gouv.fr and available in HTTPS)



Source: tests performed by Arcep in November 2021, based on Afnic data.

In November 2021, the task force published a second handbook "Enterprises; how to deploy IPv6?" aimed chiefly at companies' IT experts and CTOs, to help them make the transition to IPv6. Its purpose is to assist them in defining their IPv6 needs, planning the protocol's implementation, and deploying it in-house.

3.3. Join the IPv6 task force

The task force will continue to work on helping businesses achieve this transition, and is producing a handbook on "How to deploy IPv6" which will be available soon.

People who want to contribute to this work, share feedback or set up IPv6 in their company are invited to communicate their interest in joining the task force to Arcep, by scanning the QR code.

45. N.B. This publication in no way constitutes a formal position from Arcep on the relevance, feasibility or priority of workstreams. It simply describes the information imparted by the different members of the IPv6 task force. The priority actions to be implemented will be decided in concert with the community of participants.

Open floor to

JEAN-CHARLES BISECCO
Network architect

THE 12 LABOURS OF IPV6

"It's 2022. And this offputtingly long-string address protocol finally reached more than 50% of access lines in the country this past winter. Little by little, it is invading every stratum of the country, both fixed and mobile. Every one? No! A group of Legacy IP diehards is holding out, and still resisting the switch to hexadecimal. And life isn't easy for the legions of IPv4 packets skirmishing through the hands of subscriber IP-sharing advocates that are 4rd, MAP-T/E and other IPv4aaS technologies."

This could be a fitting introduction to a future issue of a famous comic book explaining why IPv4 is no longer a native feature for most operators, but still being offered as an encapsulated service on a native IPv6 network. A comic book that could be titled: The 12 Labours of Aypeeveesix.

Instead of a comic book, Arcep's IPv6 task force opted for a handbook to help businesses migrate the different parts of their information systems to the new protocol, after having established their strategy.

And this because, unlike with top Internet companies, IPv6 is still very little deployed in the fringes of most businesses' information systems, i.e., their websites, messaging systems for more private services such as access to the corporate VPN or proxy, allowing staff to surf the web.

But behind this handful of examples of services, there are entire swaths of the system involved. For instance, filtering, configuration management tools, log collection, all building blocks where the deployment sequence needs to be established meticulously.

It would be hard to find a topic that is any more vast, as the verticality of a company IS and the uniqueness of the applications it contains mean that an effective transition will take time. One thing is certain: we cannot go backwards.

IPv4 is such a scarce resource that some are already billing extra for it, such as hosting service providers. A practice that will probably spread.

Changes in IPv4 traffic are becoming legion and will steadily make the protocol less effective than IPv6 on the Internet for every connection initiated by individuals, customers and remote workers alike. Changes driven by the scarcity of the resource and the need to share public IP addresses, which are bundled together under the monikers Address + Port (A+P) approach or IPv4aaS.

Let us pause on this last one, which shows that the IP transport industry no longer views IPv4 as a compulsory foundation, and that it has become a mere service marketed on top of the new Internet protocol. A service that is bound to become obsolete.

Others may also seize the opportunity beyond the Internet issue, namely large structures that have come to the end of private IPv4 RFC 1918 addressing internally, and now overlapping addresses.

Here too, the handbook provides answers and helps you map out your direction.

It also contains security recommendations, practices for streamlining address management, and many other things besides.

The handbook is designed to evolve over time, so do not hesitate to ask questions, suggest changes or additions, and especially to join Arcep's IPv6 Task Force so that we can work together on tackling the challenges of this Great Crossing over to a new paradigm.

Find here the handbook "Enterprises: how to switch to IPv63"

PART 2

Ensuring Internet openness

CHAPTER 4

GUARANTEEING NET NEUTRALITY

What you need to know

The European Open Internet Regulation guarantees access to an open Internet to more than **450 million European citizens** notably by granting them the right **to access and distribute information and content online.**

September 2021 The Court of Justice of the European Union handed down three decisions interpreting the Open Internet Regulation with regard **to zero-rating practices' compliance with that regulation.**

295 net neutrality-related **user reports** filed in 2021 through the "**J'alerte l'Arcep**" platform.

Net neutrality, aka network neutrality, is a term that was coined in 2003 par Tim Wu, Professor of Law at Columbia University in New York[46]. It creates the ability to guarantee equal treatment and handling of all information streams on the Internet, regardless of their sender or recipient.

1. Net neutrality: a founding principle of the Internet enshrined in law

The Internet's founding principles, starting with its openness by design, make it a place of freedom of expression, of communication, of access to knowledge, of freedom to share and freedom to innovate. The impetus behind the concept of net neutrality is to safeguard users' ability to exercise these fundamental Internet freedoms.

The principle of net neutrality precludes the creation of a two-lane (or multi-tiered) Internet through management methods that favour certain data streams over others (discriminatory practices), or the creation of Internet access that is limited to only certain content or platforms.

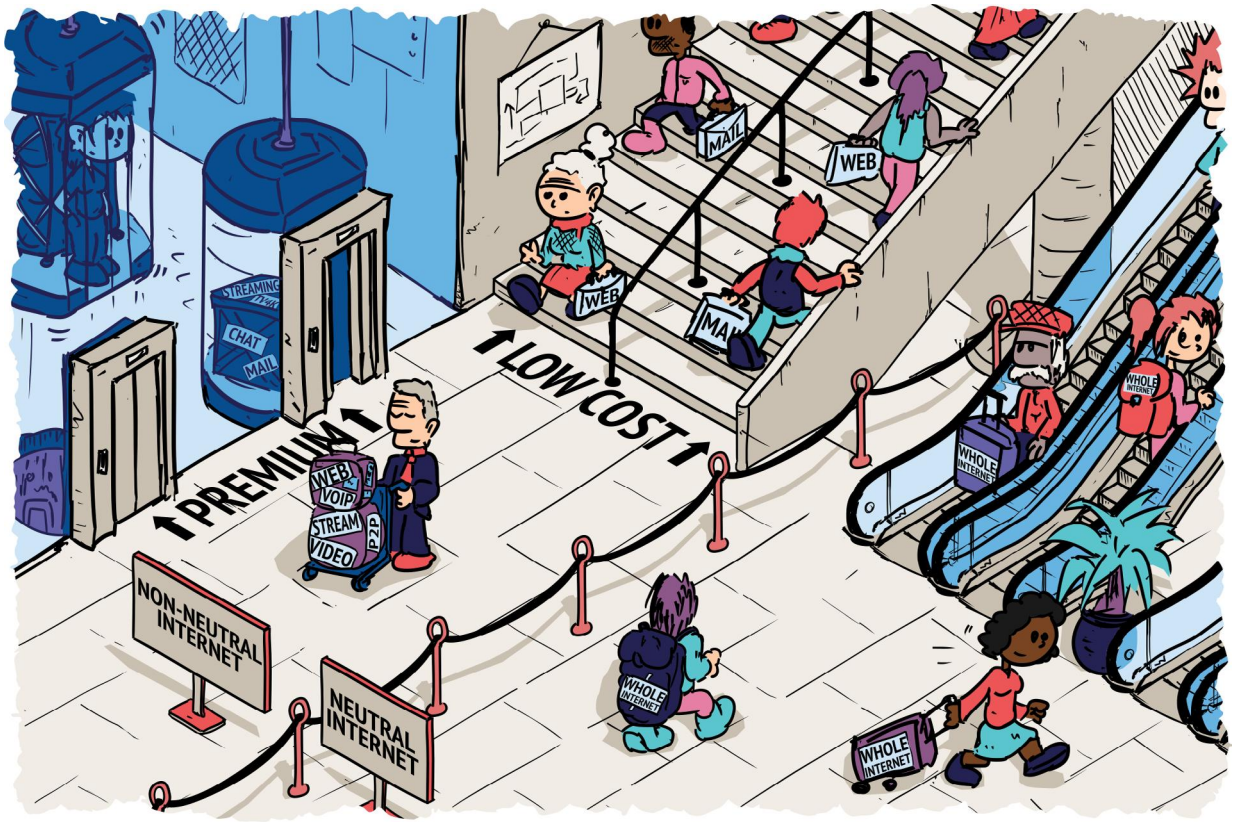
Ultimately, net neutrality protects the Internet's openness by design, while also creating tremendous positive externalities in terms of innovation and protecting the rights of end users.

European lawmakers have been protecting net neutrality since 2016, recognising the following points in particular in the Open Internet Regulation[47]:

- 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"[48];
- 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"[49].

The Internet access of a total 450 million European citizens is protected by this European regulation and its implementing guidelines, published in 2016 then updated in 2020 by the Body of European Regulators for Electronic Communications (BEREC).

46. Tim Wu, Network Neutrality, Broadband Discrimination, JOURNAL OF TELECOMMUNICATIONS AND HIGH TECHNOLOGY LAW, VOL. 2, P. 141, 2003. Click here.
47. Regulation (EU) 2015/2120 of the European Parliament and Council of 25 November 2015 laying down measures concerning open Internet access. Click here.
48. Article 3(1) of Open Internet Regulation No. 2015/2120.
49. Article 3(3) of Open Internet Regulation No. 2015/2120.


PREMIUM
LOW COST
WEB
VOIP
STREAM
VIDEO
P2P
CHAT
MAIL
STREAMING
NON-NEUTRAL INTERNET
NEUTRAL INTERNET
WHOLE INTERNET


This work of art is inaccessible with your ISP
I wonder if another ISP would let us see the arms as well...
Mona Lisa
L. da Vinci
The Raft of the Medusa
T. Géricault
Venus de Milo

Open floor to

STÉPHANE BORTZMEYER
*Internet expert - **Afnic***

SO WHAT IS THIS "NET NEUTRALITY" THAT EVERYONE'S ALWAYS TALKING ABOUT?

For years now, the topic of "Net neutrality" has been a regular topic of discussion. One of the problems raised in debates surrounding this issue is the fact that the term itself can refer to multiple things. So let's explore this wide-ranging debate.

Traditionally, discussions over network neutrality begin with an analogy with a service in the physical world. So let us not break tradition, and use the example of the Paris metro, managed by State-owned company, RATP (if this is all a bit too Parisian for you, you're welcome to substitute the metro system in another city, or a bus service or the TER regional rail service). The metro is neutral to the extent that it does not distinguish between its passengers. Regardless of whether they are travelling for work or leisure, or just for the sheer joy (!) of taking the metro, they are all treated in an identical fashion. Passengers would be very surprised, and probably a bit riled, if certain hours of the day were reserved for only business travellers, or if RATP had the power to prevent you from taking the metro because it had decided that your need to go from A to B was not really important.

Of course, the metro is not completely neutral. For instance, RATP rules explicitly exclude people who are drunk, who are forbidden from taking the metro because of the potential danger they represent to others. More subtle are certain restrictions that are not written down in black and white, for instance the lack of accessibility for people with disabilities – something that is not explicit but, in practice, does impede certain people's ability to take the metro. In short, total and absolute neutrality does not exist, so the question is rather "what are the restrictions and who defines them?"

Getting back to the Internet, neutrality comes from the fact that the network is just a pipeline, a service, and it has no views on the importance or legitimacy of how you use it. A mere intermediary, the network should not decide whether we watch videos on YouTube or on the decentralised PeerTube service or, for that matter, whether we watch videos at all. That's not its job. Despite which, everyone has concluded that there are more or less important and more or less legitimate uses. But everyone also has their own definitions of importance and legitimacy, and they are not compatible. Neutrality is therefore the recognition of this diversity of uses, which is why it is so crucial that this principle of neutrality be asserted and reasserted.

As with the metro, the difficulty lies in defining its restrictions. One easy example is denial of service (DDoS) attacks, when an assailant attempts to drown a service by flooding it with requests, which often affects the network as well. Like the drunk in the metro, nobody will argue that such an attack is a legitimate use of the Internet. But it is important that these restrictions be decided in a clear, objective and transparent manner.

As with the metro's accessibility, the most important rules are not always written down. If the network blocks or slows certain services, neutrality has been violated, even if it is not stated in a text. A great many Internet access plans make it difficult to host a server on one's own premises, because they do not support IPv6 (which enables an abundance of IP addresses and therefore avoids network address translation systems). While not fully quashing neutrality, this type of restriction will diminish it, and diminish its benefits. (In this case, for instance, it encourages traffic to be concentrated around a handful of major players.)

Neutrality therefore remains an essential goal. Its practical application in concrete cases is not always easy, but it is very important to always keep the ultimate goal in mind and to continue to underscore its positive influence on the Internet.

In October 2016, the Digital Republic Act (*loi pour une République Numérique*) designated Arcep as the Authority responsible for implementing the Open Internet Regulation in France. As a result, Arcep is tasked with monitoring Internet service providers' (ISP) practices that could violate net neutrality, with conducting investigations and imposing penalties that can reach as much as 3% of ISPs' revenue.

Net neutrality allows every end user to freely decide how they use the Internet. This ability to receive and communicate information freely contributes directly to promoting a number of end user' rights, including protecting the diversity and pluralism of media content, freedom of expression and freedom to access information. Protecting net neutrality also means protecting end users' ability to exercise their fundamental rights.

2. Renewed active participation at the European level

In 2021, Arcep and its European counterparts prepared changes to the guidelines for implementing the Open Internet Regulation, as a follow-up to recent rulings handed down by the Court of Justice of the European Union (CJEU).

On 2 September 2021 the CJEU delivered rulings on three cases[50] pertaining to zero-rating practices employed by two German operators: Vodafone and Telekom Deutschland. These rulings address the different preliminary questions that German courts referred to the CJEU regarding the legality of the contractual obligations surrounding use of the so-called zero-rating[51] option.

REGULATORY FRAMEWORK GOVERNING NET NEUTRALITY

NOVEMBER 2015
Regulation (EU 2015/2120) of the European Parliament and Council, laying down measures concerning open Internet access

JUNE 2016
Adoption of BEREC guidelines on the implementation by national regulators of European Net Neutrality Rules BoR (16) 127

JUNE 2020
Adoption of revised BEREC guidelines on the implementation by national regulators of the Open Internet Regulation BoR (20) 112

SEPTEMBER 2020
CJEU ruling regarding Telenor (Joined cases C-807/18 and C-39/19)
First CJEU interpretation of European net neutrality rules

SEPTEMBER 2021
Three rulings from the CJEU regarding Vodafone and Telekom Deutschland (case C-854/19, case C-5/20 and case C-34/20) – CJEU interpretation of zero-rating practices' compliance with the Open Internet Regulation

MARCH 2022
BEREC revised guidelines published for public consultation

JUNE 2022
Report on the public consultation on a new version of BEREC revised guidelines

JUNE 2022
Adoption of a new version of BEREC revised guidelines, for implementation of the Open Internet Regulation by national regulators, taking the Court of Justice of the European Union rulings into account

Source: Arcep

50. CJEU, 2 September 2021, Vodafone and Telekom Deutschland (cases C-854/19, C-5/20 and C-34/20).
51. Zero rating refers to practices whereby an ISP applies a zero-tariff or preferential pricing to all or part of the data traffic generated by a specific category of application provided by one of the ISP's partners. This means that the traffic generated by the use of that service or application is not deducted from the customer's data allowance. When offered as part of a plan with a set data allowance, this zero-rating option therefore allows ISPs' to bolster the appeal of their plans.

Open floor to

ORIANE PIQUER-LOUIS
Coordinator for the telecoms regulation working group of the French Data Network (FDN) Federation

NET NEUTRALITY IS A GOOD IDEA – SO IS BANNING ZERO-RATING

Since the adoption of the European Open Internet Regulation – six years ago now – net neutrality may seem to be a given, along with other hard-won rights that are now an integral part of our legislative corpus. If we can congratulate ourselves on the existence of this cornerstone of net neutrality protection, and its transposition into BEREC guidelines, the false sense of having "solved" the problem masks operators' never-ending requests for exceptions, even though the regulator had already made two concessions: "specialised services" and zero rating.

There is no denying that the September 2021 decision from the Court of Justice of the European Union (CJEU) against zero-rating (i.e., the practice of not deducting traffic to a certain service from end users' data allowance) stood out in a year where there was little movement on other topics. In a series of three rulings, the CJEU declared that this practice is contrary to Article 3, paragraph 3 of the Open Internet Regulation. This is good news: the associations to which I belonged repeatedly decried this exception.

Net neutrality is the digital manifestation of freedom of expression and information. Its purpose is to guarantee end users that when they read or write on their Internet, these fundamental freedoms are protected. This goes one step further than the letter of the European regulation which speaks only of an "Open Internet": opening the Internet to all market players and guaranteeing fundamental rights and freedoms are not exactly the same thing, even if one allows the other.

These freedoms emerged in Europe in the late 18th century. In *What is Enlightenment?* Kant shows us how the explosion of an independent and diverse press, and the structuring of scientific discussion at the European level enabled the peoples of Europe to begin thinking for themselves, and so to choose their government and leave behind the state of "tutelage" in which religion in particular had placed them. Children are in just such a state of tutelage, or guardianship, as decisions are made for them by their parents. This tutelage is lifted when we become adults, we become free to think and act for ourselves, and so become accountable. This is why freedom of expression and information are the bedrock of our democracies: pluralism of the press and public debate allow citizens to forge an independent opinion, which is necessary to elect a representative with awareness, to act as an adult.

Today, by being situated as the interface between the Internet and end users, an ISP has tremendous power over the way in which these fundamental rights are respected in the digital age, and so an equal degree of accountability. There is a fundamental aim of the technical neutrality required of them: treating all content and services in the same way means treating end users as adults. They are the ones that choose.

Zero-rating, however, has an undeniable effect of suggesting certain content or a particular source of information. End users have a choice, but it is illusory: exempting a given application or source of information from their data allowance naturally steers end users towards it. Here, the ISP leaves the realm of neutrality and no longer treats end users as adults, by offering up content or a service that enjoys preferential treatment on a platter. It tells them what to do and what to read.

Despite what some people say about it, net neutrality is a good idea: we need the Internet to remain a tool of emancipation for citizens. And there is still a lot of work to be done on improving and strengthening the set of rules laid down in 2015 – whether with measures or penalties. If putting an end to considering zero-rating an acceptable exception marks a step in the right direction, this is no time to lower our guard.

Open floor to

THOMAS LOHNINGER
Executive Director of Austrian digital rights NGO epicenter.works, Vize-President of European Digital Rights (EDRi) and non-residential Fellow at the Stanford Law School Center for Internet and Society.

EU IS BACKSLIDING ON NET NEUTRALITY TO THE ERA OF DONALD TRUMP

In 2021 the Court of Justice of the European Union (CJEU) decided in three cases from Germany[1] that zero-rating is illegal under the EU Net Neutrality Regulation[2]. These judgements are remarkable in several ways: First, they were unexpected and immediately prompted a reform of the BEREC Guidelines on Net Neutrality. Secondly, they are in line with the longstanding assessment of civil society that application-specific differentiated pricing practices (which include, but are not limited to, application-specific zero rating) are a harmful practice which is prohibited by the obligation to "treat all traffic equally" in Europe's Net Neutrality Regulation[3].

Since 2015 civil society has communicated this reading of the Regulation to BEREC in several consultation responses (2016 and 2019), oral hearings (2015 et 2019) and open letters (2016). Sadly, to no avail. The referenced exchanges are proof of the fact that the six-year-long inaction of telecom regulators cannot be attributed to negligence, but willful inaction to enforce their legal mandate. Given that zero-rating practices are a wide-spread phenomenon to be seen in all but two EEA countries, it would have been up to any of the 30 regulators in EEA countries to bring a case challenging it, but eventually it was up to the CJEU to answer a question no regulator dared to ask.

Two lessons should be learned from this: First, the weight within BEREC attached to consumer protection and civil society actors is out of balance compared to the weight attached to industry actors. Secondly, enforcement based on the updated Guidelines has to be swift, thorough and appropriate to the harm, the CJEU has affirmed in its judgements. Any delays in enforcement at this point would raise questions of regulatory capture and on the rule of law.

2022 could have been a moment to pause and realign the regulatory debate about the Internet in Europe. Sadly, that didn't happen and instead we went straight back to a debate we had 10 years ago. On 2nd May 2022 Commissioners Vestager and Breton announced to scrap core net neutrality protections by introducing a Sending Party Pays principle. This old idea of a two-sided market comes from the termination fees of the telephony era and has been rejected for the Internet numerous times; most prominently during the 2012 ITU meeting when the telecom industry tried to have it adopted as a global model for the Internet. Back then it faced criticism from NGOs, academics, Internet luminaries and even Commissioner Neelie Kroes. The only ones supporting this idea were authoritarian states that saw it as a way to take control of the Internet. A two-sided market ignores the paying Internet subscribers that demand the traffic sent to the network of their operator. This model also neglects the additional cost of market entry for startups, particularly in a segmented access market such as Europe. The irony is that the telecom industry until recently incentivized traffic from big content providers by excluding it from users' data cap and now it wants extra money for that exact data volume.

There is only one historical precedent for what Commissioners Vestager and Breton are currently proposing for the Internet in Europe: it's the complete abolishment of net neutrality protections under the administration of Donald Trump. Maybe that's where we'll end up.

1. CJEU, 2 September 2021, Vodafone and Telekom Deutschland (cases C-854/19, C-5/20 and C-34/20).
2. Regulation (EU) 2015/2120 of the European Parliament and of the council of 25 November 2015 laying down measures concerning open Internet access. Click here.
3. Article 3(3) paragraph 1 of Open Internet Regulation 2015/2120.

The Court had had an earlier opportunity to rule on zero-rating practices, in two cases brought by a Hungarian Court (ruling of 15 September 2020, Telenor Magyarország, C-807/18 and C-39/19). In these cases, the Court had only ruled on the practices in question without addressing the substance of the issue of commercial practices permitted by the Open Internet Regulation (validating the regulator's prohibition of two zero-rating practices that included differentiated technical treatment of traffic).

This time, however, to respond to the different questions, the CJEU concluded that a preliminary examination of the general legality of a zero-rating commercial practice, under the terms of Article 3.3 of the Open Internet Regulation, would be needed. This paragraph stipulates that ISPs must treat all Internet traffic equally and without discrimination, restriction or interference, regardless of the applications or services used. Any different treatment must not be based on commercial considerations and must be duly motivated, in accordance with the exceptions permitted by the regulation, which was not the case in the affairs in question. With these rulings, the Court of Justice issued a reminder that by not deducting the traffic going to partner applications from customers' data allowance, a zero-tariff option, such as those at cause, creates a distinction between Internet traffic based on commercial considerations. It concludes that such a commercial practice runs counter to the overall obligation to treat all traffic equally, without discrimination or interference, as required by the Open Internet Regulation[52].

To draw all of the necessary conclusions from these rulings, the Body of European Regulators (BEREC) reviewed its Open Internet guidelines, and submitted its revisions to public consultation in March 2022.

The new guidelines, published in June 2022, maintain the structure of the previous guidelines, published in June 2020, which themselves align with the Open Internet Regulation's structure around four main themes: commercial practices, traffic management measures, specialised services and transparency obligations. This update confines itself to the direct effects of the rulings. The goal is indeed to amend the initial wording on commercial practices, and on enforcement of the obligation to treat traffic equally and its exception, by incorporating the Court's reasoning in detail.

3. An ever-evolving toolkit

To safeguard net neutrality, Arcep has created a toolkit that helps the Authority obtain a complete overview of market practices with respect to the Open Internet Regulation's four cornerstones: commercial practices, traffic management, specialised services and transparency obligations.

ARCEP'S NET NEUTRALITY TOOLKIT

Source: Arcep

52. Press release No. 145/21 of the Court of Justice of the European Union. Click here.

As part of the Authority's monitoring duties, Arcep departments keep constant track of Internet service providers' (ISP) terms and conditions of use. In 2021, Arcep's monitoring work helped flag a plan marketed by a French overseas operator, which was subsequently required to switch to practices that more closely comply with the Open Internet Regulation (cf. following section).

As an adjunct to this work, Arcep has a set of regulatory tools that allow it to collect information from ISPs on their network/traffic management rules.

Since 2017, Arcep has also been providing end users with access to the "J'alerte l'Arcep" reporting platform. In 2021, 295 net neutrality-related reports were logged on the platform. The reports filed

DIFFERENT MEDIA SERVICES TESTED BY WEHE

Source: Arcep

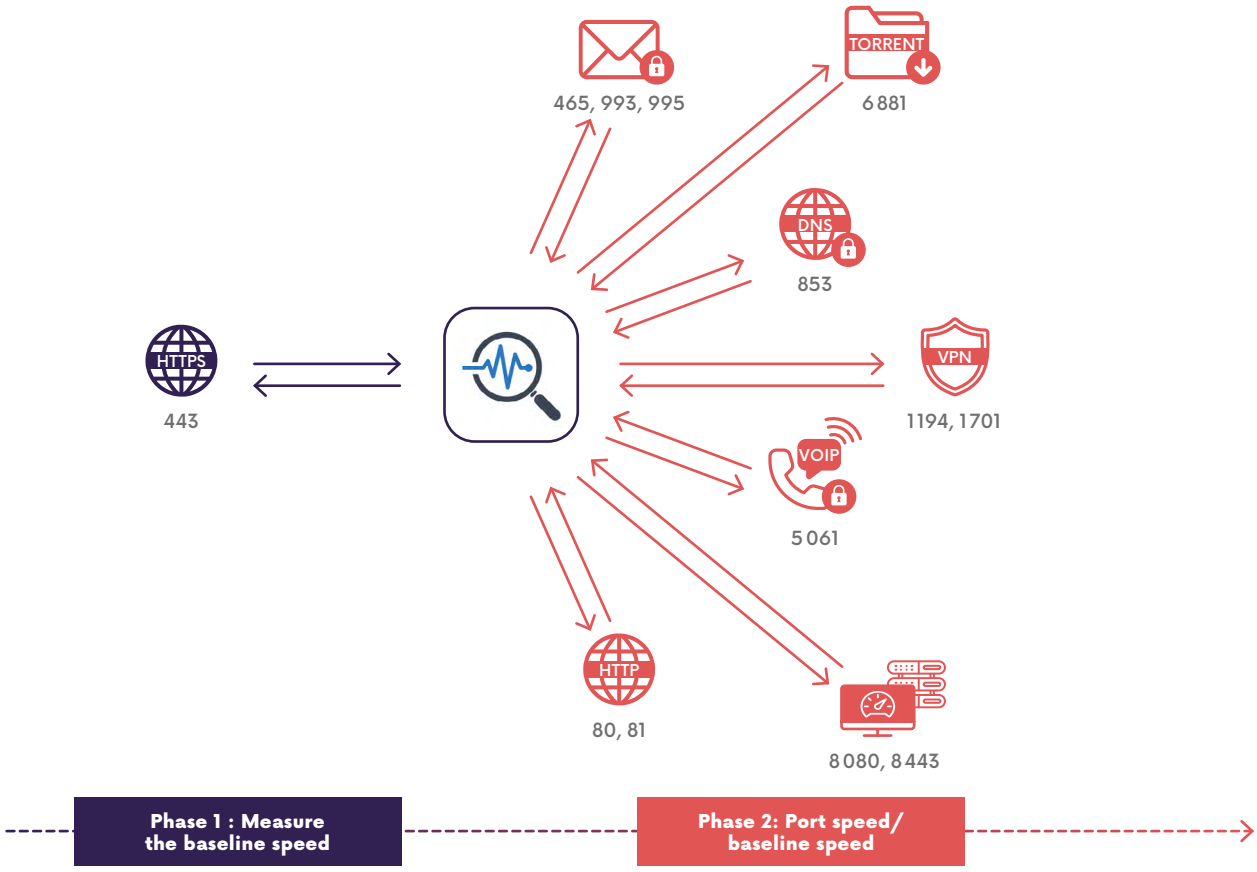
by end users allow the Authority to identify possible net neutrality infractions, and to achieve a swift resolution of the issues that were raised, which are detailed in the next section.

Over the course of last year, Arcep continued to collaborate with other national regulatory authorities in France, notably the Regulatory Authority for Audiovisual and Digital Communications (Arcom) with which a joint division was created in late 2020. National inter-authority cooperation creates the ability to tap into each one's respective knowledge and competencies to advance regulatory analysis of common and cross-cutting issues.

The work on net neutrality carried out by the different regulatory authorities within BEREC continued on through 2021. Arcep and its counterparts held multiple discussions within BEREC, including on the resilience of their networks in Europe as a result of the Covid-19 crisis. The CJEU rulings of September 2021 also required major cooperation between BEREC member regulatory authorities, in addition to the work on amending the guidelines for implementing the Open Internet Regulation, which has continued on in 2022. At the same time, Arcep increased cooperation with national regulators from other countries through bilateral discussions on case studies, which helped deepen its understanding of situations at home that are similar to those experienced by its counterparts abroad.

Lastly, Arcep has made a detection tool called Wehe available to the general public since 2018. Wehe is available for free in French, on Android, iOS and more recently on the F-Droid store. Developed in partnership with the Northeastern University in Boston, Wehe is an Open Source testing tool that analyses the traffic generated by an application to determine whether an operator might be throttling or prioritising some data traffic or ports. Arcep completed its work on updating Wehe, whose latest version was rolled out in late December 2020. Several improvements were made to the differentiation test: the list of services tested was updated to include the most popular services in France, new test categories were introduced to facilitate the selection of services tested by users and, finally, improvements were made to how the test results are displayed to users.

HOW WEHE'S PORT TESTING WORKS



Source: Arcep

Arcep also wanted to provide users with a tool for detecting any potential blocking, throttling or priority queuing applied to a port, which could affect end users' ability to access online services. Some online services and applications are accessed through a specific port, so any blocking, throttling or prioritisation of that port could affect how end users' are able to access that service. From a technical standpoint, the port test compares https traffic for each of the ports selected by the user, and compares it to traffic on port 443, which has been defined as the baseline port.

Should proven discrepancies be detected in the tests performed by Wehe, users are invited to report any issue directly via the "J'alerte l'Arcep" platform, so that Arcep can review potential incompatibilities with the Open Internet Regulation on a case by case basis.

Since launch, 600,000 tests have been conducted in France using the Wehe app. All of the statistics on the tests carried out in France are available online.

4. Status report on observed practices

Arcep continued to examine whether all of the Internet plans being marketed in the overseas territories complied with net neutrality principles. As a reminder, in 2020 Arcep worked with all of the overseas operators to produce a net neutrality scorecard. Several exchanges were held with operators, particularly regarding certain mobile Internet plans' general terms and conditions of use. Ultimately, most of the points that were raised had not been technically implemented, according to the operators in question. These clauses were thus rectified following discussions with the Authority's departments. The monitoring work conducted by Arcep nevertheless made it possible to flag a mobile plan being sold by an overseas operator that raised some questions over its compliance with the Open Internet Regulation. Arcep's proactive dialogue meant that Open Internet Regulation provisions could be more fully taken into account in the operator's plan. The operator in question thus amended its plan accordingly.

Arcep continued to examine Wi-Fi services onboard national railway company SNCF trains. This Internet access service which is offered to passengers is considered publicly accessible, and so subject to Open Internet Regulation provisions. Arcep departments' ongoing dialogue with SNCF helped these offers evolve towards practices that more closely comply with the Open Internet Regulation.

The Authority also continues to pay close attention to the reports it receives on possible net neutrality violations, notably those received via the "J'alerte l'Arcep" platform. In 2021, 295 net neutrality-related alerts were logged through the platform.

Finally in 2021, Arcep worked to update its understanding of how video on demand (VoD) services operate. One particular goal of this process was to deepen its knowledge of VoD service operations and the technical restrictions to which they are subject. To this end, Arcep departments spoke with several players who contribute to video on demand operations in France, namely telecom operators, VoD content providers, hosting companies that market dedicated video storage solutions, and linear and time-shifted video content providers. Some of the findings of this analysis can be found in Chapter 2 on data interconnection. Arcep departments continue to engage in a dialogue with telecom operators to analyse their practices in light of the technological developments of VoD.

« J'alerte l'Arcep »

Launched in 2017, the "J'alerte l'Arcep" platform allows any user – be they individuals, businesses, local authorities, developers or consumer associations – to report any malfunctions encountered in their relationship with their mobile operator, Internet service provider, postal service provider or press distributor. In 2021, Arcep produced a scorecard of its pro-consumer actions and its "J'alerte l'Arcep"* reporting platform. Users submitted more than 38,000 reports to Arcep last year. Of these, 40% concerned a fixed or mobile QoS or service availability issue.

These reports constitute an important addition to Arcep's diagnostic capabilities. They enable the Authority to track the problems being encountered by users in real time, to identify recurrent malfunctions, and detect spikes in user alerts – with the ultimate aim of taking more effective regulatory action. The reports are also a useful source of information for Arcep departments for identifying potential infractions of the Open Internet Regulation and its net neutrality rules.

The "J'alerte l'Arcep" platform is continually evolving, and being enhanced with other data-driven regulation tools developed by Arcep (Mon réseau mobile, Carte fibre, Ma connexion Internet and Wehe).

* The 2021 scorecard of Arcep's pro-consumer actions and the "J'alerte l'Arcep" platform.

Network slicing: delivering innovations enabled by 5G, while protecting net neutrality

Network slicing is a technology enabling the creation of subnetworks (or subnets) in the form of virtual networks, aka slices, overlayed on a physical network infrastructure. Flexible and dynamic slicing is expected to become possible once 5G core networks are deployed, and will give operators the ability to supply differentiated services by creating a virtual network to satisfy their customers' different needs.

Network slicing allows an operator to administrate its network to meet customers' expectations. Some of the sector's players are still wondering whether 5G technology is compatible with net neutrality. But is it or is it not? The Open Internet Regulation is technology neutral[1], which means ISPs can use any technology they want. The principle of technological neutrality, mentioned in the Open Internet Regulation, states that "The measures provided for in this Regulation respect the principle of technological neutrality, that is to say they neither impose nor discriminate in favour of the use of a particular type of technology". The use of network slicing is therefore not intrinsically incompatible with the Open Internet Regulation. This was in fact the conclusion reached by the European Commission[2] and BEREC[3] which, after investigations conducted in 2019 and in 2018, respectively, concluded that there was no a priori incompatibility between the Open Internet Regulation and network slicing.

The concrete organisation of the slices defined by ISPs (slice numbers and scaling, services involved, QoS associated with each slice, etc.) and the potential impact on Internet availability and overall quality must be examined case by case, with respect to the Open Internet Regulation provisions and implementing guidelines.

To this end, Arcep published a memo in May 2022 on network slicing and net neutrality, which can be accessed on its website (french only).

Arcep will continue to closely monitor the development of 5G use cases, and will remain available to answer stakeholders' questions on these use cases' compatibility with the principle of net neutrality.

5G NETWORK COMMON INFRASTRUCTURE

Source: Arcep

1. Article 2 of Open Internet Regulation 2015/2120.
2. Report from the Commission to the European Parliament and the Council on the implementation of the open Internet access provisions of Regulation (EU) 2015/2120, 30 April 2019.
3. BEREC Opinion for the evaluation of the application of Regulation (EU) 2015/2120 and the BEREC Net Neutrality Guidelines, 6 December 2018.

Open floor to

JOE KANE
*Director of Broadband and Spectrum Policy - **Information Technology and Innovation Foundation (ITIF)***

NET NEUTRALITY IN THE UNITED STATES: MUCH ADO ABOUT NOTHING

Despite frantic predictions of the Internet's doom following the 2018 rollback of certain "net neutrality" regulations in the United States, the last five years have shown the fever-pitched outcries to be much ado about nothing. Harmful violations of net neutrality—anticompetitive blocking and throttling—have not materialized, and ISPs have maintained that they are neither necessary nor desirable for their business. Indeed, the Internet in the United States has thrived, even in the face of a dramatic uptick in bandwidth-intensive, real-time services during the COVID-19 pandemic.

As a practical matter, therefore, net neutrality is a nonissue. Politically, however, net neutrality still looms large. The remaining political question, however, is not whether to have net neutrality but which legal authority should form the basis for enforcing it. Those on the political left tend to favor specific, bright-line regulations promulgated and enforced by the Federal Communications Commission (FCC) under Title II of the Communications Act, which governs common carrier services and empowers the Commission to take aggressive steps such as regulating rates. Those on the political right would prefer the FCC classify ISPs under less prescriptive Title I of the Communications Act and have harmful net-neutrality violations addressed by the Federal Trade Commission (FTC) Act, which bans "unfair methods of competition" and "unfair or deceptive acts or practices."

These competing frameworks combined with courts' deference to the FCC's choice of regulatory scheme has resulted in a back a back-and-forth every time control of the FCC changes partisan hands. Indeed, it is widely expected that the current FCC will reimpose Title II regulations once the Senate confirms a fifth commissioner. Thus, the regulatory ping-pong will likely continue in the absence of compromise legislation that directly enshrines the consensus net neutrality principles into law while removing the looming threat of the more onerous provisions of Title II.

Such legislation has been proposed by members of Congress and civil society groups, but the prospects for its enactment remain grim. This assessment is based partially on partisan gridlock in Congress but also by the apparent preference of some advocates to impose a Title II classification precisely because it sets the stage to recreate the broadband market under a rate-regulated, public utility regime, not just ensuring net neutrality. This aspiration is misguided as the full weight of Title II would likely produce the sclerosis and lack of competition that characterized its previous application to twentieth-century telephone service. Title II is, therefore, a mismatch for sustaining the vibrant and competitive U.S. broadband marketplace.

The ultimate way to improve connectivity for consumers remains to build up the quality of broadband networks so that the tradeoffs occasioned by scarce bandwidth become less pressing. Development along these lines is continuing apace despite, and likely because of, the lack of prescriptive utility regulation. The innovation and investment driven by private network operators in the United States help eliminate congestion and make problematic network management practices unnecessary.

In sum, net neutrality's cachet is based primarily on its value as a political slogan rather than any active threat to the Internet's functioning. While this political sideshow will likely continue, Internet users would be better served by enacting compromise legislation that codifies basic net neutrality principles and forecloses draconian regulations that would undermine the ongoing growth and improvement of the U.S. broadband networks.

Open floor to

WILLMARY ESCOTO
US Policy Analyst - ***Access-Now***

THE ROAD TO NET NEUTRALITY IN THE US

Net neutrality – the principle that Internet service providers treat all Internet traffic equally – has been a contentious issue in the US. In the wake of the Trump presidency, there is no federal rule preventing blocking, throttling, or paid prioritization of Internet traffic. Therefore, the US has become an outlier on an issue of critical importance to the future of the Internet, and the current "pay to play" policy is trampling on the human rights of millions of Americans. Here's why net neutrality matters, what happened to it, and what's in store for the future of the open Internet under the Biden administration.

Why net neutrality matters?

Net neutrality is the most crucial attribute for an open and free Internet, and it is vital to maintaining free speech online. Its principles are fundamental to ensuring open, secure, and affordable access to the Internet and enabling a level playing field for reaching audiences online. With net neutrality in place, small start-ups, citizen journalists, and creators can compete on an equal footing with larger platforms. This is especially important for marginalized voices. Net neutrality and democracy are just as inextricably linked as democracy is to freedom of expression. Full participation in democratic discourse entails engagement in digital spaces. Net neutrality is fundamental to empowering people across the US and worldwide to voice their opinions and reach an audience without paying for preferential treatment. From the #BlackLivesMatter movement to the #MeToo uprising, the free and open Internet, and the net neutrality principles that sustain it, has allowed people to take back their power, amplify their voices, and share their stories. Communities of colour need an open Internet to continue fighting for a world where nations recognize their humanity. Without robust net neutrality protections in place, the right to freedom of expression, opinion, association, and many other fundamental rights, are at risk.

What happened to net neutrality in the US?

When it comes to protecting the Internet and treating all information on the Internet the same, the federal government's position on the issue has shifted with the political winds. The regulatory stop-and-go over the past decade has left Americans in a dizzying sea of uncertainty. In 2015, under former President Barack Obama, the FCC adopted federal net neutrality rules. Two years later, after the Trump administration took control, the Federal Communications Commission (FCC) abandoned net neutrality, repealing landmark protections the Obama administration had put in place. Under the 2015 net neutrality rules, Internet service providers (ISPs) could not block or slow Internet content or offer paid «fast lanes". After these rules were reversed at the federal level, California's legislature adopted its own state net neutrality law in 2018. The law bars ISPs from blocking, throttling traffic or offering paid fast lanes, and prohibits paid data cap exemptions ("zero-rating"). Industry associations representing major Internet providers that profit from a lack of net neutrality, like AT&T, Verizon, and Comcast, challenged the California law. After losing three times in federal court, these associations finally abandoned the lawsuit. Several other states have also stepped up to stop network discrimination, including Hawaii, Montana, New York, New Jersey, Washington, Rhode Island, Vermont, and Colorado. Many net neutrality supporters in the US expect (and strongly hope) that more states will step up to the bat.

Global implications and the road ahead

The FCC's back-and-forth on net neutrality continues to risk isolating the US from global norms for free expression and non-discriminatory access to the Internet In more than 40 countries, net neutrality is the law of the land, as the European Union protects these principles. However, no one can take net neutrality for granted. Even in the EU, lawmakers and Internet service providers continue to advance proposals to undermine or limit net neutrality. It is the time for the US to reignite the fight for the free and open Internet, which is vital for free expression and democratic participation in the US and across the globe. An FCC commissioner vacancy is complicating the effort to restore net neutrality at the federal level. The confirmation process for Biden nominee Gigi Sohn has stalled for months. Without a full slate of commissioners, the FCC remains deadlocked. Once Sohn is confirmed, net neutrality advocates hope to see the full reinstatement of the Obama-era rules. At that point, Americans will be assured their ideas and voices will be heard and amplified without a surcharge to large corporate conglomerates setting up Internet pay tolls for their speech.

CHAPTER 5

CONTRIBUTING TO THE REGULATION OF GATEKEEPER PLATFORMS

What you need to know

After the European Commission published the proposed **Digital Markets Act** in December 2020, Arcep continued its commitment to the issue, to strengthen this proposed regulation and ensure its efficient implementation.

Arcep has contributed actively to **national, European and international** work through a variety of bodies (e.g. French Task Force, BEREC, international conferences).

Within BEREC, Arcep is currently contributing to the analysis of **the Internet ecosystem** and **the enforcement of interoperability measures** between instant messaging services.

The European Open Internet Regulation[53] grants users rights such as the right to access and distribute information and content online. But it applies only to Internet service providers (ISPs). Located at the end of this chain, devices (smartphones, voice assistants, connected cars, etc.) and especially gatekeeper[54] platforms' closed ecosystems have proven to be the weak links in achieving an open Internet.

The work that Arcep has done on digital platforms since 2018[55,56], concluded that a small number of powerful players had become the "gatekeepers" to people's and businesses' digital lives, by concentrating control over many of the services that had become an integral part of all of our daily lives. Around 70% of people in France send and receive text messages and 60% make calls using an app[57], 84% of Europeans use at least one of the instant messaging services belonging to the Meta Group (WhatsApp and Facebook Messenger)[58], and 90% use Facebook, YouTube or Instagram as their main media platform[59]. These companies now have the power to determine what content and services can be put online and under what conditions users can access them. Added to which, as they concentrate control over a plethora of services, they operate closed ecosystems within which users are kept captive, which automatically limits their freedom of choice.

To tackle these crucial issues, on 15 December 2020 the European Commission published two draft regulations: the Digital Services Act and the Digital Markets Act. Through the Digital Services Act, the Commission is proposing to review the e-commerce Directive of 2000, and to make online platforms liable for the significant risks to which they can expose their users by distributing illegal, dangerous or counterfeit content and products (cf. Arcom contribution on page 81). Thanks to the Digital Markets Act (DMA), the Commission intends to introduce economic regulation of gatekeeper platforms, to make digital markets open and fair, and to harmonise the legal framework at the European level. Under this new regulatory framework gatekeeper platforms will, among other things, no longer have the right to prevent users from uninstall the software and apps that are preinstalled on their devices, to engage in self-preferencing[60] or to prevent consumers from accessing other firms' services outside their ecosystems. They will also be subject to an obligation to make their operating system interoperable with third-party app stores.

This is a major step forward that largely echoes the recommendations that Arcep has been making since 2018[61], in particular by targeting the most influential platforms, including operating systems, i.e. services that have been revealed to impose multiple restrictions on users' freedom of choice[62].

53. Regulation (EU) 2015/2120 of the European Parliament and Council of 25 November 2015 laying down measures concerning open Internet access. Click here.
54. "Gatekeepers" as defined by Articles 2 and 3 of the Digital Markets Act.
55. https://www.arcep.fr/uploads/tx_gspublication/rapport-devices-fev2018.pdf.
56. https://www.arcep.fr/uploads/tx_gspublication/platforms-numeriques-structurantes-caracterisation_reflexion_dec2019.pdf.
57. Digital Market Barometer, 2021 edition, pages 107-108.
58. BEREC, "Analysing EU consumer perceptions and behaviour on digital platforms for communication", page 42.
59. BEREC, "Analysing EU consumer perceptions and behaviour on digital platforms for communication", page 27.
60. For a platform, self-preferencing consists of giving preferential treatment to its own services and products over similar products and services that third parties market on its platform.
61. In particular its work on devices, which are seen as the "weak link in achieving an open Internet", February 2018.
62. Arcep report, "Smartphones, tablets, voice assistants: devices, the weak link in achieving an open Internet" (February 2018).

Outside the European Union, several legislative proposals have been introduced, notably in the UK and in the United States. In the UK, a Digital Markets Unit was established in April 2021 within the Competition and Markets Authority (CMA)[63], with the goal of (i) protecting the interests of consumers and citizens, (ii) being a centre of expertise for digital markets, (iii) overseeing digital firms that have "Strategic Market Status"[64]. The British government held a public consultation on this proposal for a new "Pro-competition regime for digital markets" and is currently in the process of examining the responses[65]. In the United States, the House of Representatives introduced a series of bills in late 2021 that seek to regulate leading digital platforms' market power. These bills, which are currently being debated, are a follow-up to the House of Representatives' publication of report, investigating competition in digital markets.

1. Arcep's contributions

Arcep remained committed to the issue throughout 2021, working to strengthen the measures contained in the DMA and to ensure an effective and efficient implementation of the regulation. Among other things, the Arcep and BEREC proposals pertained to the regulation's scope of application and the role that competent national regulatory authorities (NRA)[66] can play within an advisory board.

Regarding the scope of application, Arcep and BEREC underscored the decisive role that devices play, and suggested that other services provided by gatekeeper platforms, such as voice assistants and web browsers, also be covered by the regulation. In addition, without challenging action taken at the European level and the Commission's role as sole regulator, Arcep and BEREC proposed creating a DMA Advisory Board: a group of high-level experts whose task would be to assist the European Commission in its regulatory work, by providing it with expertise and recommendations, including market studies, or concerning changing obligations and monitoring compliance with those obligations. These two proposals – which were also introduced in the European Parliament – were included in the final version of the DMA, following the latest trialogue on 24 March 2022.

All of Arcep's proposals were submitted through various channels, notably multiple BEREC publications, keynotes and roundtables at national and international conferences, and participation in the French Task force (see inset).

Contributions to discussions on introducing regulation of gatekeeper platforms

BEREC's contributions

Several weeks after the publication of the Commission's DMA proposal, BEREC published an opinion[1] that set forth its initial recommendations for strengthening the Commission's proposed regulation. Two papers published in June 2021 underscore the need to set up structured remedies-tailoring and participation processes[2] and to create an Advisory Board at the European level[3].

Drawing on these publications, and on the many workshops and interactions held with European institutions and stakeholders, BEREC's report on *ex-ante* regulation of gatekeeper platforms[4] (published in September 2021 following a public consultation) sets forth proposals designed to foster competition between digital platforms, protect the interests of end users, treat identified problems in a proportionate and tailored fashion, and ensure the implementation of an effective regulation through a system of reinforced oversight. All of these proposals were submitted to public consultation, and received widespread support amongst stakeholders[5].

Moreover, the provisions of the European Electronic Communications Code (EECC) already apply to some of services – such as instant messaging[6] – targeted by the DMA. This means that regulators can, under certain conditions, impose interoperability measures on the

1. *BEREC Opinion on the European Commission's proposal for a Digital Markets Act*.
2. *BEREC proposal on remedies-tailoring and structured participation processes for stakeholders in the context of the Digital Markets Act9*.
3. *BEREC proposal on the set-up of an Advisory Board in the context of the Digital Markets Act*.
4. *BEREC Report on the ex ante regulation of digital gatekeepers*.
5. Business users, rival platforms, representatives of civil society, consumer associations, sector experts, etc.
6. Number-independent interpersonal communication services (NI-ICS).

63. https://www.gov.uk/government/collections/digital-markets-unit#full-publication-update-history.
64. This is roughly equivalent to the European Commission's notion of "gatekeepers".
65. https://www.gov.uk/government/consultations/a-new-pro-competition-regime-for-digital-markets.
66. Electronic communications regulatory authorities, national competition authorities and authorities that regulate personal data privacy and protection.

providers of these services when end-to-end connectivity is endangered[1]. BEREC published a report[2] that aims to ensure appropriate interplay between the EECC and DMA, and to remove potential legal uncertainties.

Arcep's contribution to conferences

Drawing on their expertise in electronic communications sector regulation, Laure de La Raudière, in her capacity as Arcep Chair, along with Emmanuel Gabla, in his capacity as member of the Arcep Executive Board and BEREC Vice-chair for 2022, participated at conferences during which they argued for the need to introduce an asymmetric *ex-ante* regulatory framework to safeguard users' freedom of choice, and foster competition and innovation in digital markets. Targeted action would reduce information asymmetries by structuring upstream supervision and associating stakeholders, and by incorporating data-driven regulation.

These positive outcomes were laid out by Laure de la Raudière during a talk at the Internet Governance Forum France (IGF) on 25 November 2021 and by Emmanuel Gabla during a conference hosted by the High Commission for Digital and Postal Affairs (CSNP, *Commission Supérieure du Numérique et des Postes*) on 20 January 2022. At IGF, Laure de La Raudière spoke alongside fellow regulators Roch-Olivier Maistre, Chair of Arcom, and Marie-Laure Denis, Chair of CNIL. Emmanuel Gabla spoke at the CSNP conference alongside members of the French and European Parliaments, including Stéphanie Yon-Courtin, draftsperson for the Digital Market Act (DMA) to the European Parliament's Committee on Economic and Monetary Affairs (ECON).

Arcep also opened up to a range of stakeholders: decision-makers, market players, consumer associations, experts, academics and representatives of civil society. It co-hosted and ran two BEREC workshops that attracted close to 250 participants. The first workshop was dedicated to the methods for ensuring effective competition between digital platforms in the context of the DMA, with talks from Prabhat Agarwal (Head of Unit, Digital services and platforms, DG Connect, European Commission), Carlos Zorrinho (MEP and rapporteur for the ITRE[3] committee on the DMA), as well as a panel of experts and representatives of competing platforms and gatekeepers' business users. During the second workshop, Inge Bernaerts (Director for Strategy and Policy, DG Competition, European Commission), Andreas Schwab (MEP and European Parliament rapporteur on the DMA), as well as a panel of experts and representatives of consumer associations and civil society discussed how to enshrine the protection of end users' rights in the DMA.

Arcep also spoke at several conferences hosted by academic institutions – including the Brazilian Institute of Competition and Innovation (IBCI), the Florence School of Regulation and the Governance and Regulation Chair – European trade associations and think tanks. To discuss Arcep's proposals and measures being planned in the UK, Arcep also hosted a seminar with Amelia Fletcher, Professor of competition policy, Deputy Director at the Centre for Competition Policy in the UK, and co-author of the Digital Competition Expert Panel report, headed by Jason Furman.

1. Article 61(2)(c) of the European Code.
2. BEREC Report on the interplay between the EECC and the EC's proposal for a Digital Markets Act concerning number-independent interpersonal communication services.
3. European Parliament Committee on Industry, Research and Energy (ITRE).

Arcep's contributions at the national level

Since March 2020, Arcep has been an active participant in the Task Force led by the Directorate-General for Enterprise (DGE), and contributes to drafting France's positions within the Council of the European Union. This inter-ministerial Task Force provides supporting works and conducts investigations into the most efficient way to regulate digital platforms.

In September 2020, French authorities also set up the Digital regulation expertise hub/*Pôle d'expertise* de la *régulation numérique* (PEReN) that lends its expert assessment and technical assistance to national government departments and authorities involved in regulating digital platforms. To this end, the members of this unit with a national purview, include data scientists and IT and algorithm experts. Arcep and PEReN meet on a regular basis, to identify avenues of investigation.

Arcep's contributions to European think tanks

These discussions over the regulation of gatekeeper platforms are also being carried out at the Centre on Regulation in Europe (CERRE). Arcep contributed in particular to the work done on proposals for improving the implementation of the DMA, and on mobile devices' openness, non-discrimination and transparency issues.

2. Outlook for 2022

The Digital Markets Act is an ambitious piece of legislation, and represents a crucial step towards limiting the excess power enjoyed by certain digital platforms, and BEREC will continue to provide the expertise needed for its adoption and enforcement. The regulation will, however, probably not tackle all of the outstanding issues on every link of the Internet chain, as these issues are many and varied. Added to which, tech companies can change their behaviour rapidly, and adapt strategically to new laws. Which is why it is important that Arcep and BEREC continue their work in this area.

In 2022, Arcep's contributions will centre around several core matters:

- The BEREC report on the Internet ecosystem. Begun in 2021 and currently in the final stages, this report seeks to analyse every element of the ecosystem (from network infrastructures to operating systems to cloud services), to identify competition dynamics, obstacles to an open ecosystem, player strategies and potential bottlenecks.
- The BEREC report on the interoperability of number-independent interpersonal communication services will deliver an economic and technical analysis of the application of interoperability measures set forth in the DMA and in the European Electronic Communications Code, and of the interplay between these two regulatory frameworks.

From a broader perspective, and in addition to the work being done within BEREC, Arcep will continue its dialogues within and contributions to the different national (digital Task Force, PEReN), European and international (OECD, CERRE) bodies.

Open floor to

ANDREAS SCHWAB

Member of the European Parliament since 2004. European People's Party coordinator in the influential committee on the internal market and consumer protection. Parliament's rapporteur on the Digital Markets Act.

THE DIGITAL MARKETS ACT – EUROPE STARTS A NEW ERA OF BIG TECH REGULATION

The Digital Markets Act (DMA) is Europe's key to ensure fairness and contestability in digital markets. The DMA imposes new obligations on a few large digital platforms that intermediate between business users and end users. Such powerful intermediating positions have given large platforms the power to dictate access conditions to their platforms - they act as "digital gatekeepers". Thereby, during the past two decades, Gatekeepers leveraged dominant positions from one market into another, engaged in self-preferencing and became both platforms hosting businesses and competitor to those businesses at once.

The DMA's obligations in Articles 5 and 6 tackle these problems. The European Parliaments' additions ensure that these articles will not be outdated soon after the DMA's entry into force. The Parliament strengthened rules on data-siloing, on transparency in advertising markets, on access conditions to platforms and side-loading, and on data portability. Moreover, the Parliaments' amendments open up Gatekeeper ecosystems, for example by extending interoperability mandates for connected devices and by creating possibilities for horizontal interoperability between messaging services.

By design, the Digital Markets Act addresses several aspects of the online platform economy.

That increases the technical complexity of regulatory tasks the European commission has to fulfil, while its enforcement capacities remain unchanged.

Therefore, the European Parliament proposed the creation of a "High Level Expert Group of Digital Regulators" (HLEG), where BEREC will be a member. The HLEG would advise the Commission in supervising compliance with the DMA and report on the DMAs synergies with national, sector-specific legislation. Thereby, the HLEG's technical expertise would significantly improve the enforceability of the Digital Markets Act. Moreover, by analysing the synergies with national legislation, regulatory red tape could potentially be reduced in the long term by identifying possibilities for more harmonization.

The DMA will shape Europe's digital economy for years to come. Given the rapid pace of change in digital markets, the parliaments' amendments will guarantee the DMA's enforceability and future-proofness. The European Parliament finished its job in March 2022. Now, it will be up to the European Commission to enforce the DMA.

Open floor to

ROCH-OLIVIER MAISTRE
*President - **Arcom***

EUROPE'S DIGITAL SERVICES ACT MARKS A MAJOR STEP FORWARD IN THE REGULATION OF LARGE ONLINE PLATFORMS

Presented by the European Commission in December 2020, and currently in the final stages of negotiation in the European Parliament, the Digital Services Act (DSA) sets the ambitious goal of strengthening regulation of the digital sphere to "guarantee a safe and accountable online environment". The text thus seeks to increase online platforms' accountability to promote transparency, democratic oversight, and citizens' fundamental rights.

The DSA thereby pursues online platform supervision efforts introduced by the French legislature on a Europe-wide scale – notably the Act of 22 December 2018 on combatting disinformation, the Act of 24 June 2020 against hateful material on the Internet, and the Act of 24 August 2021 upholding compliance with the principles of the French Republic. These different laws expand the powers granted to French regulator, Arcom, to deal with the consequences of Big Tech companies' limited self-regulation, and to set up a framework for dialogue and supervision adapted to the issues they represent. The goal is not to "regulate the Internet" or verify every bit of online content: this approach is based on an obligation of means and transparency to combat the systemic disfunctions embodied by the phenomena of disinformation and the proliferation of hate speech.

At the European level, advances introduced by the DSA are at the heart of the discussions taking place within the ERGA (*European Regulators Group for Audiovisual Media Services*), the body that unites Arcom and its European counterparts. In particular, this new legislation will increase regulators' ability to access gatekeeper platforms' data, and plans to impose diligence and transparency obligations on both those platforms and on the leading search engines. European bodies will be able to rely on national regulatory authorities and the ERGA to implement and enforce the Digital Services Act, as they are experienced in balancing fundamental freedoms and have developed proven, effective cooperation mechanisms.

The DSA thus arms Europe with the tools to tackle an ambitious, necessary and much awaited task, to protect our rights and our values, and contribute to creating trust and transparency in the information and digital space.

PART 3

Tackling digital sector's environmental challenges

CHAPTER 6

WORKING TO ACHIEVE DIGITAL SUSTAINABILITY

What you need to know

In January 2022, ADEME and Arcep submitted the findings of the joint study they conducted in 2021 on the digital sector's environmental footprint in France. This study reveals that

devices have the largest carbon footprint, followed by data centers then networks.

In 2022, having

its environmental data collection powers expanded

to include players other than electronic communications operators will give Arcep the ability to address the entire Internet access chain.

1. The Authority's commitment to achieving digital sustainability

The first embodiment of Arcep's commitment to tackling the environmental issues surrounding digital technology was the "Achieving digital sustainability" collaborative platform which launched on 11 June 2020 – calling on associations, institutions, operators, tech companies and interested experts to contribute to the investigative process. After six months punctuated by five thematic workshops and two "big discussions," on 15 December 2020 Arcep published a status report which was the culmination of the work done thus far, and included 42 contributions authored by participating stakeholders. In this report, Arcep sets forth 11 proposals for successfully combining the ongoing increase in the use of digital tech and reducing its environmental footprint.

Arcep's work on these issues continued on throughout 2021, deepening the Authority's expertise and making strides in establishing rules for achieving a more sustainable Internet and user behaviours. Since 2020, Arcep has also been a driving force on environmental issues within BEREC, co-chairing the "Sustainability" working group, and sharing its experience and the work it has done at the national level.

At the same time, Parliamentary discussions over bills and legislative proposals on digital and the environment gradually took shape. These legislative milestones helped to expand some of Arcep's powers and responsibilities with respect to the environment, including:

- the Act of 22 August 2021 on combatting climate change and promoting more sustainable energy use, aka the "Climate and Resilience Act"[67];
- the Act of 15 November 2021 on reducing the digital environmental footprint in France, aka the "Chaize Act" or "REEN Act»[68];
- the Act of 23 December 2021 on reinforcing environmental regulation of the digital sector by Arcep, aka the "Collection Act[69].

These laws introduce new provisions on measuring the digital environmental footprint and creating a Environmental Barometer, on the environmental impact of broadcasting and the consumption of audiovisual media, the sustainable design of digital services in France, and the incorporation of environmental considerations when installing new infrastructures and when assigning frequencies. All projects that will keep Arcep busy in the coming months.

67. Act No. 2021-1104 of 22 August 2021 on combatting climate change and promoting more sustainable energy use.
68. Act No. 2021-1485 of 15 November 2021 on reducing the digital environmental footprint in France.
69. Act No. 2021-1755 of 23 December 2021 on reinforcing environmental regulation of the digital sector by Arcep.

2. Overview of 2021 – Work done by ADEME and Arcep on assessing the environmental impact of the different links in the Internet access chain

The question of digital sustainability was a major area of focus for Arcep throughout 2021, and the Authority worked on several publications and events:

- a report on mobile device replacement patterns and the impact of distribution practices, published on 12 July 2021;
- a status report on "Achieving digital sustainability" aimed at the platform's participants, to lay out the latest advances made by Arcep and reaffirming the Authority's ambition;
- two workshops to help inform Arcep's investigations into the ways and means for taking environmental imperatives into account when assigning 26 GHz band frequencies for 5G;
- a study by the Mobile network technical experts committee providing a comparative assessment of a 4G vs. 5G deployment.

In particular, to complete an assignment entrusted to it by the Government, Arcep, together with the National Agency for the Ecological Transition (ADEME), produced a report on assessing the digital environmental footprint in France. The first two parts of this report were published in January 2022 and provide a review of the available literature (bibliographical and methodological), along with a current assessment of the digital environmental footprint in France.

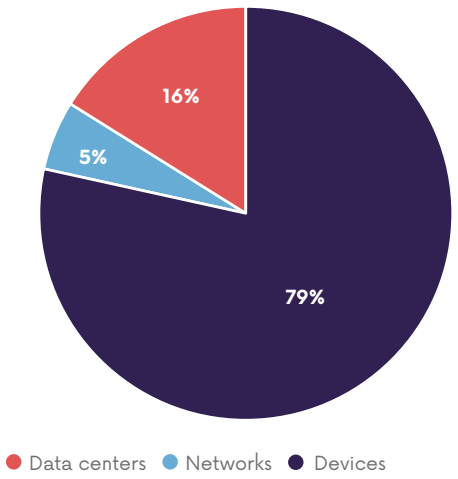
Based on the life-cycle assessment (LCA) methodology, the study breaks down digital sector into three hardware building blocks: devices, networks and data centers (this is the multi-component aspect of LCA). The digital environmental footprint is assessed using 11 additional environmental indicators on top of its carbon footprint (this is the multi-criteria aspect of LCA). The analysis includes the environmental impacts at every stage of the lifecycle of each of these three building blocks, namely production, distribution, utilisation and end of life (this is the multi-stage aspect of LCA).

Based on this approach, and on the most current data collected by the study's authors, it emerges that devices have by far the biggest footprint: they are responsible for 65% to 90% of the digital sector's total footprint, according to the indicators considered.

Devices' carbon footprint represents 79% of digital's total footprint, and the production stage accounts for the majority of this footprint: 78% of total compared to 21% for the utilisation stage.

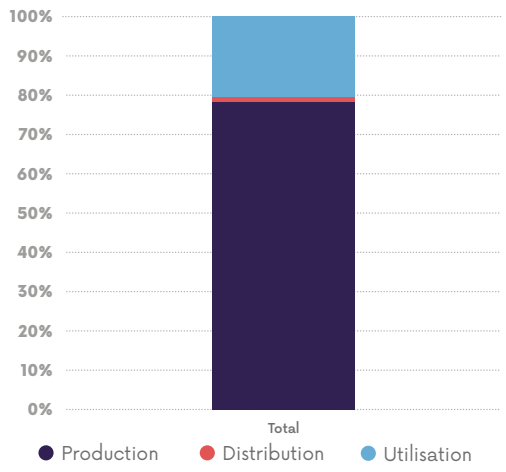
The digital sector's environmental footprint is not limited to its carbon footprint, however. In addition to the environmental impacts, notably those tied to energy consumption (including the carbon footprint, ionising radiation, as well as the depletion of abiotic fossil fuel resources which account for around 64% of the impact) – which are impacts that are common to a great many sectors – the depletion of abiotic resources (minerals and metals), emerges as a crucial criterion (around 27%) amongst digital technology's predominant effects on the environment. The carbon footprint is thus far from being the only impact on the environment, hence the relevance of a multicriteria approach.

EACH DIGITAL BUILDING BLOCK'S SHARE OF THE CARBON FOOTPRINT



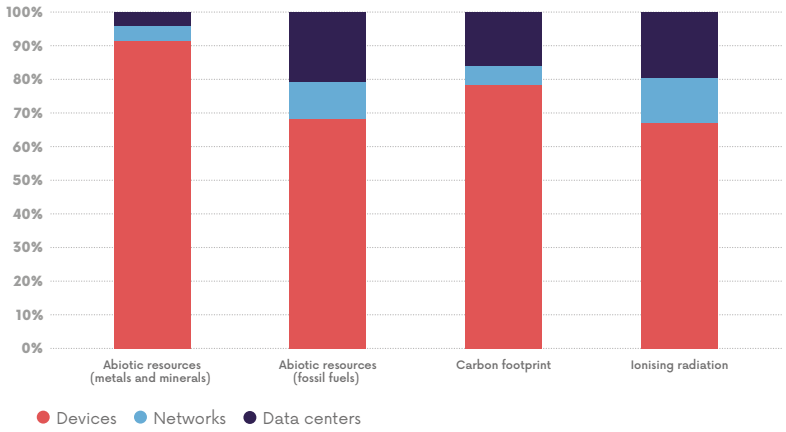
Source: ADEME-Arcep study on assessing the digital environmental footprint in France

THE DIGITAL BUILDING BLOCK'S SHARE OF THE CARBON FOOTPRINT



Source: ADEME-Arcep study on assessing the digital environmental footprint in France

BREAKDOWN OF ENVIRONMENTAL IMPACTS BY DIGITAL BUILDING BLOCK



Source: ADEME-Arcep study on the digital environmental footprint in France

The study also shows that the main contributors to the digital sector's environmental footprint are user devices. These include a range of devices[70] of varying footprints. The "screens and audio-visual hardware" category has the biggest environmental impact for all of the indicators considered (followed by the "computers" category). If the impact of telephones[71] is substantial, it is far from being the largest. Measures for prolonging the life of devices must therefore go well those aimed at mobile phones.

Data centers rank number two in terms of environmental impact. By performing a more detailed analysis of the equipment that makes up a data center the study concluded that, in every case, it is servers that have the greatest impact, during their production and their utilisation. The study also highlights the role of enterprise servers and collocated servers (data centers where multiple clients house and operate their own IT equipment) which account for the bulk of data centers' environmental footprint: more than 80% for each environmental indicator. The study did not, however, make it possible to determine the extent to which these results are the fruit of a volume effect tied to the number of enterprise and collocation servers, or whether a particular issue needs to be addressed. It should also be noted that only data centers located in France were modelled[72].

Lastly, networks represent the smallest percentage of the digital environmental footprint. Their contribution to the sector's carbon footprint stands at around 5%, and the orders of magnitude for the other types of environmental impact are roughly the same (between 5% and 10% for abiotic resource depletion – minerals and metals, fossil fuels and ionising radiation).

The study helped to fine tune the assessment of the digital sector's environmental impact. In addition to the assessment itself, the study confirms the complexity of the exercise and identifies the key obstacles that need to be lifted to improve the measurement process. This evaluation work is just one stage in a lengthier endeavour to fine-tune and disseminate a proven and operational methodology, and enable access to more data.

It confirms that devices are the source of most of the impacts (65% to 90%), for every indicator, followed by data centers (4% to 20%) then networks (4% to 13%). It thus seems imperative to tackle the environmental impact of all devices, and especially those with the most decisive influence (televisions, computers, etc.). That being said, this is an issue that must be addressed as a whole. This breakdown of the different categories' impact must not obscure digital technology's ecosystemic dimension: the interdependence of devices, networks and data centers created by Internet-based applications must be considered when drafting public policies designed to tackle the digital carbon footprint as a whole. All of the ecosystem's stakeholders must do their part towards achieving digital sustainability.

The multi-step analysis also reveals that the production phase often has the biggest footprint (over 80%), which confirms the importance of public policies aimed at extending the life of digital equipment by promoting product durability, reuse, refurbishment, and the functionality and repair economies. Depending on the indicators being considered, the utilisation phase can also represent the main source of the digital carbon footprint (up to around 80% in terms of natural abiotic resource depletion (fossil fuels) and ionising radiation).

The work that the two institutions have already begun should help lift some of the identified obstacles, and both will continue to work together to complete the final stage of the ADEME-Arcep study, which will provide forward-looking scenarios.

70. A non-exhaustive list of the devices considered in the study: desktop and laptop computers, tablets, smartphones, landline phones, computer displays, televisions, projectors, TV boxes, home and handheld video game consoles, etc.
71. The "telephones" category can be broken down into smartphones, feature phones and landline phones. For virtually every environmental indicator, smartphones account for around 80% to 90% of the impact (except for ionising radiation where landline phones' energy consumption decreases that share to 32%).
72. Modelling does therefore not include the environmental impact of foreign data centers supporting consumption in France, and does not exclude the environmental impact of data centres on French soil supporting consumption abroad.

3. Outlook for 2022 – The next stages of Arcep's work: taking a global approach to tackling the digital environmental footprint, across the entire Internet access chain

Arcep wants to build on the work already accomplished on measuring the digital sector's environmental impact. In addition to the study on the digital environmental footprint conducted with ADEME, the Authority is steadily forging its expertise and so its ability to take a global approach to the digital environmental footprint. This is crucial work that will help identify the hardware and behaviours that have the greatest impact on the environment, to be able to then target the most fruitful levers for action.

Data collection for creating and publishing Arcep's Environmental Barometer is a significant part of this workstream, which is also an integral part of the objectives set by the "Digital Sector and Environment" roadmap that the Government published in February 2021.

In April 2022, Arcep had already published the initial version of this barometer, referred to as the "Achieving digital sustainability" annual survey, with the first indicators covering only electronic communications operators.

With the Act of 23 December 2021 on reinforcing environmental regulation of the digital sector by Arcep[73], the Authority's data collection powers have been expanded to include network equipment suppliers, device manufacturers, public online communication service providers, operating system providers and data center operators. This means that Arcep will have the ability to cover the entire Internet access chain.

Expanding the scope of environmental data collection to include these players will create the ability to steadily enhance the annual publication of environmental impact indicators, to keep all of the sector's players and public authorities informed and thereby enable the introduction of adapted policies, while encouraging economic actors to adopt more virtuous behaviours and heightening consumers' awareness of the impact of their digital habits.

A great deal of discussion with stakeholders will be needed to reach an agreement on the different methodological aspects involved in implementing new indicators. To this end, Arcep is committed to pursuing its collaborative approach throughout 2022. Since the start of the year, it has been holding bilateral meetings with digital sector and environmental stakeholders, which will culminate in a workshop for all of these parties, devoted to reaching a collective decision on the indicators to be included in this new version of the "Achieving digital sustainability" annual survey.

Arcep plans on holding a public consultation on its expanded data collection decision in summer 2022, and on publishing the final version before the end of the year. This will be followed by a massive pre-publication data collection, processing and editing effort in 2023.

Arcep will also undertake several projects in collaboration with Arcom and ADEME in 2022:

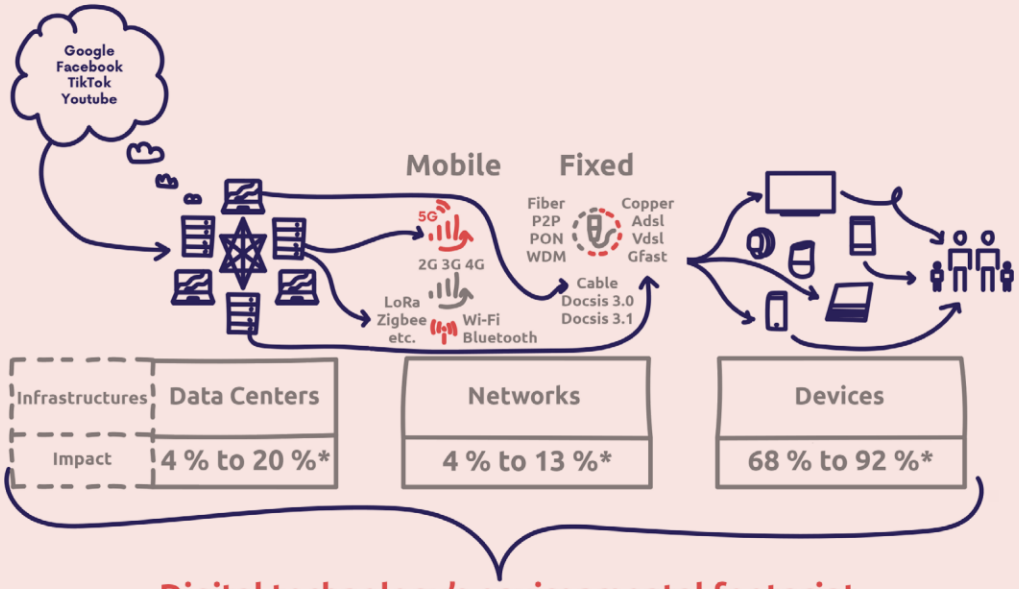
- an outside study on measuring the environmental impact of audiovisual content broadcasting and consumption in France;
- a publication by Arcom, in concert with Arcep and ADEME, of a recommendation on informing consumers via television services, audiovisual media services and video sharing platforms on the energy consumption and carbon footprint of their media habits;
- definition by Arcom and Arcep, in concert with ADEME, of the content of a general policy framework for the eco-design of digital services, by January 2024.

73. Act No. 2021-1755 of 23 December 2021 v on reinforcing environmental regulation of the digital sector by Arcep.

Tutorial

Extending the life of computers

Devices' contribution to the digital environmental footprint



* according to the most relevant environmental impact indicators considered

Source : aggregation of data from the study conducted by ADEME and Arcep in January 2022 on assessing the digital environmental footprint in France

Does one automatically need to change computers once security updates are no longer available? No, because devices represent 76.4% of the digital environmental footprint.

Added to which, of all the devices, computers have one of the most substantial environmental footprints, accounting for close to a quarter of electronic devices' total footprint. So replacing one's computer less frequently will help reduce the digital carbon footprint.

Importance of security updates

It is important for computers that are connected to the Internet to stay updated, even if they do not have any important data on their hard drive. Hackers and cybercriminals pay very close attention to security updates, to see which security flaws they correct, and attack computers that have not installed those updates. A computer that is not updated can become a botnet or zombie, in other words a computer that has been hijacked by a cybercriminal without its owner's knowledge. Zombie armies or botnets, i.e. large groups of comprised computers, are then used for DDOS (distributed denial of service) attacks, to mine cryptocurrency or simply to send out floods of spam. A botnet will also have an impact on the environment, due to the computer's excess power consumption.

Availability of security updates

Security updates are not available for the whole of a computer's life. After a certain period of time, the operating system provider stops offering updates.

For example:

- The lifespan of Windows 10 is due to end on 14 October 2025. Updates to Windows 11 are only for newer computers[1]. Most of the PCs sold in 2018 are not Windows 11-compatible.
- For Apple users, a 2015 MacBook cannot install macOS 12/Monterey, and must continue to run macOS 11/Big Sur. Apple typically allows macOS updates for three years.

1. List of Intel processors that support Windows 11 and list of AMD processors that support Windows 11.

Tutorial

Solutions for extending the life of a computer

Two solutions for extending the life of a computer, when it becomes too slow for its original purpose or when it is no longer receiving operating system updates:

- Give an old computer a second life by donating it to an association, cooperative or a humanitarian entity that will collect and restore the computer with a new operating system, after having wiped all the data from its hard drive[2].
- Install a new operating system oneself. The process does not require great technical skill, but does require a memory stick (typically 4 GB minimum) and erases all of the computer's data. Which means that it is crucial to back up all of one's documents, etc. beforehand.

  There are several types of operating system (OS):

  - Operating systems based on the use of online services. They therefore require an Internet connection to function, even if certain basic features may be available offline. With Google's Chrome OS Flex, for instance, the life of a PC built after 2010, with at least 4 GB or RAM and a minimum 16 GB hard drive can be extended.
  - OS that install applications and data on the hard drive and can be used offline. Standard versions of Linux require a PC built after 2008, with at least 4 GB or RAM and a minimum 32 GB hard drive to function properly. For those willing to sacrifice certain features, there are also Linux lightweight distributions that can run on any PC with just 1 GB of RAM.

  A memory stick is required to install a new OS. Arcep provides step by step instructions on its website: How to create a bootable USB flash drive and perform a reliable speed test.

A Linux distribution is simply a coherent collection of software around a Linux kernel. The first step in choosing a Linux distribution is the choice of graphical environment, or GUI. The three most popular are Gnome, KDE and Xfce. There are several Linux distributions for each. The choice of environment will be based on the desired functionalities, but also on the computer's RAM, which is often a limiting factor on old computers.

- RAM enables the processor to temporarily store the data it needs to boot up the programme. The operating system and open source software are loaded into RAM. To give an idea: an open-source web browser uses approximately 1 GB or RAM and an OS uses 1 to 2 GB. When the RAM is saturated, the RAM's least used data are swapped over to the hard drive, which will significantly deplete performances.
- The second limiting factor is the microprocessor, the computer's brain. Many operating systems require a 64-bit microprocessor, and virtually all PCs built since 2008 have a 64-bit microprocessor.

RAM (Random Access Memory)	Operating system to use to extend the life of a computer
Under 1 GB	It will be difficult to perform security updates on and run a computer with less than 1 GB of RAM. But old computers can still serve multiple purposes, provided they are not connected to the Internet. One of the best solutions is to install an old Linux distribution and use the computer as a teaching tool, or to play certain old installable video games. It can also pay DVDs if it had a built-in DVD player.
1 GB	With only 1 GB of RAM, it is hard to use a web browser on a daily basis, but the computer can be used to run desktop applications, educational software or to rediscover old video games. Emmabuntüs is a Linux distribution designed to facilitate the restoration of old computers, particularly for Emmaüs humanitarian communities (hence the name).
2 GB and 3 GB	From 2 GB of RAM upwards, a PC can be used to browse the web and stream video. To free up as much RAM as possible for the web browser, it is recommended to use a Linux distribution with a lightweight GUI. Desktop environments best suited to computers with a modest set-up include Xfce and LXQt. Xfce has a few more functionalities and is better integrated than LXQt, but uses a bit more memory. Both of these lightweight environments are supported by Linux distributions such as Emmabuntüs and Debian.

2. A list of support organisations that refurbish old devices can be found, for instance, on LaCollecte.tech.

Tutorial

RAM (Random Access Memory)	Operating system to use to extend the life of a computer
4 GB and up	Any Linux distribution can run on a 64-bit PC with 4 GB of RAM. It is recommended to use a Linux distribution with a popular desktop environment with a good set of functionalities such as Gnome (possible distribution: Ubuntu), Cinnamon (e.g. with Linux Mint) or KDE (e.g. with Mageia). It is also possible to install Google's Chrome OS Flex. A computer with more than 4 GB of RAM can run more applications simultaneously without lagging.

What can old computers be used for?

Below are some examples of how old computers can be repurposed (a non-exhaustive and indicative list):

- **GCompris** is open-source educational software, included in most Linux distributions, which offers a variety of activities for children between the ages of two and 10, or over: reading, geography, science, maths, riddles, puzzles, initiation to Mastermind and chess, learning braille, etc. GCompris includes more than 100 activities in all. The software can run on a Pentium III with 512 MB of RAM.
- **Tux Paint:** Open-source drawing software for stimulating children's creativity. It is included in most Linux distributions, and includes a range of magic effects and stamps for sticking images on a drawing. It can run on a Pentium II with 256 MB of RAM.
- **PlayOnLinux** is software that makes it easy to install and use multiple games and software designed to run only on Microsoft Windows. PlayOnLinux is based on Wine software while saving users from having to understand its complexity. It allows them to run old Windows games on an old Linux PC. For instance, the CD of SimCity 4, a game released in 2003, is no longer compatible with Windows 10, but runs perfectly on Linux with PlayOnLinux.
- **LibreOffice Writer,** word processing software included in Linux distributions, providing autonomy to prepare documents. It can run on a Pentium III with 512 MB of RAM and can import and export Word .docx format documents.
- **VLC multimedia player** allows users to play DVDs (provided the computer has a DVD player). It can be used on a Pentium 4 with 512 MB of RAM. Videos in 720p resolution, however, require a minimum Core 2 Duo hard drive and 1 GB of RAM.
- **Firefox** allows users to access the main video on demand (VoD) platforms with a Core 2 Duo hard drive running at more than 2.5 GHz, and 2 GB of RAM. N.B. a 64-bit Linux environment is needed to play videos with DRM (Digital Rights Management) protection, used by most commercial VoD platforms.

What about older smartphones?

An old smartphone can be given a second life, by donating it to an association, cooperative or humanitarian entity, or to someone in one's circle who does not own a smartphone.

Even if it does not work perfectly, an old smartphone can still be used for variety of purposes. Below are a few suggestions.

Functions that require a SIM card:

- Making phone calls
- Accessing a Wi-Fi hotspot (requires a 4G smartphone)

Functions that do not require a SIM card:

- MP3 player
- Baby monitors (over Wi-Fi)
- Running educational apps (e.g. Gcompris)
- Simple applications (e.g. apps to encourage children to brush their teeth)
- GPS (there are apps that can be used offline)
- Remote control
- Video games
- Watching videos (over Wi-Fi)

Open floor to

CAROLINE SOHN

*Member of the experts collective - **GreenIT.fr***

DIGITAL TECHNOLOGIES ARE NON-RENEWABLE RESOURCES: LET'S USE IT WISELY!

Digital sector is a critical sector, non-renewable resource that is being exhausted inexorably and far too quickly.

We have become totally dependent on digital technology, whether for the operation of our infrastructures, running the global economy, or simply for communicating and sharing knowledge… And we continue to be engaged in this mad dash to digitalise everything (cryptocurrency, metaverses, etc.). It is the only sector that is growing exponentially!

Digital sobriety is the cornerstone of more responsible digital tech, from both an environmental and social perspective. Simply put, it means saving digital resources while respecting life and nature when we design, build and use it.

For more than fifteen years, our studies on every scale – global[1], France[2], businesses[3,4] – have demonstrated that the greatest environmental impacts occur during the hardware production stage (34 Bn units worldwide).
If we take a closer look at networks and data centers, we see that the footprint stems chiefly from utilisation (energy consumption).

To achieve this objective, eco-design needs to be extended to digital services and equipment, along with the creation of a mass market for reuse, putting an end to the incremental technologies race and moving towards disruptive innovation (low and high tech).

We also believe that digital sobriety can create a competitive advantage for France which can be a standard bearer in this area.

Having good ideas is not enough, we need to put them into widespread action.

1. [EENM 2019] "The global environmental footprint of digital sector", study, GreenIT.fr, octobre 2019.
2. [iNUM 2020] "iNUM: Digital's environmental impact in France/Impacts environnementaux du numérique en France", joint study, June 2020.
3. [WEGREENIT 2018] "How can France's major corporations embrace Green IT?/Quelle démarche Green IT pour les grandes entreprises françaises ?", GreenIT.fr, WWF France, Club Green IT, February 2020.
4. [GREENCONCEPT 2020] "Greenconcept Position Paper", Summary of collective work, February 2020.

ARNAUD LEROY

*President of the Board from 2018 to June 2022 - **ADEME***

TO ACT MORE EFFECTIVELY, PUBLIC AUTHORITIES ARE REFINING THEIR EXPERTISE ON THE ENVIRONMENTAL IMPACT OF DIGITAL SECTOR

The work being done to understand the environmental impact of digital sector remains vital, as understanding is a prerequisite for reducing it. An environmental assessment supposes an analysis of a product's entire life cycle using a multicriteria approach. ADEME and Arcep have pooled their respective expertise to develop a shared knowledge of the environmental impacts of the different digital building blocks, using these methods. The first output of this work – which fulfils the role of observatory described in the Act on reducing the digital carbon footprint in France – illustrates digital services' share of France's carbon footprint (2.5%), their impact in terms of resources and materials, and in terms of waste production throughout their life cycle. These findings also serve to highlight equipment and devices' very significant weight in digital's environmental impact.

Extending the useful life of digital equipment and services is equally important, given that 75% of digital's environmental footprint is tied to hardware production. This extended lifespan also contributes to the circular economy and so to reducing waste production and the consumption of resources, by avoiding or delaying the purchase of new products. Moreover, the repair sector helps generate jobs, most of which can only be local, and can help increase French consumers' purchasing power. ADEME is currently conducting a study on the impacts avoided thanks to refurbished products. The first findings on smartphones reveal that, on average, buying a refurbished mobile phone can reduce one's annual environmental footprint by 55% to 91% (depending on the type of impact), compared to use of a new smartphone. This avoids the extraction of 82 kg of raw material, and the emission of 25 kg of greenhouse gases per year of use, or 87% less than with a new device.

ADEME and Arcep will continue to fuel the work being done on digital's environmental impact, to continue to build widespread awareness, and work with stakeholders on achieving more eco-friendly performance.

LEXICON

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

ADEME:
Agence de l'environnement et de la maîtrise de l'énergie.

Android:
mobile operating system developed by Google.

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.

APN (Access Point Name):
identifier that enables a mobile phone user to connect to the Internet.

Arcom:
French regulatory authority for audiovisual and digital communication.

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.

Cable networks:
electronic communications networks made up of an optical fiber 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.

Cache server:
dedicated network server that saves Internet content locally, and so making that content available to users more quickly.

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

CDN (Content Delivery Network):
Internet Content Delivery Network.

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

Codec:
a device or computer program that encodes or decodes a digital data stream.

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 instruments that centralise the QoS and/or QoE tests performed by volunteer users (aka "the crowd").

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.

---

ePrivacy:
European Parliament and Council Directive 2002/58/EC of 12 July, concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). A draft revised ePrivacy Directive intended to replace the current one is currently being debated, and pertains in particular to the use of cookies and associated practices, as well as obtaining Internet users' consent.

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

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 fiber is pulled right into the customer's premises.

Full-MVNO:
MVNO which manages its addressing plan and which takes control of the core network and service platforms, while leasing radio capacity from host operators.
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.

GDPR (General Data Protection Regulation):
Regulation (EU) 2016/679 of the European Parliament and of the 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 throughout the European Union.

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.

Interleave:
a method that consists in cutting data packets into smaller bits and then, rearranging them so that data that were previously contiguous are now more widely spaced to form a non-continuous stream. In this mode, when a disturbance occurs, it usually affects a single bit per byte, even if it occurs in a large number of bytes.

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 used since 1983. IPv6 (IP version 6) is its successor.

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

IPv6-ready:
device or connection that 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.

LAN (Local Area Network):
For residential users, this is the network made up of the ISP's box (router) 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.

Light-MVNO:
MVNO which entrusts their host operator with the operational management of the network.

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).

---

macOS:
operating system developed by Apple for its computers.

Multi-connection 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.

MVNO (Mobile Virtual Network Operators):
operators that do not have their own wireless network, and who therefore rely on the services of one or more mobile network operators (of which there are currently four in France: Bouygues Telecom, Free Mobile, Orange and SFR) by purchasing wholesale communications from them, to be able to then market mobile communication services to their own subscribers.

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.

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

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

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.

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.

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.

Preliminary questions:
a legal term that refers to a procedural rule that arises when it appears to a court that a particular question of law must first be resolved by the usual court of competent jurisdiction before the seised court can rule. This procedure is provided for in European Union Law, whereby Courts in Member States refer questions of interpretation of a treaty, or an act of secondary legislation to the Court of Justice of the European Union (CJEU), before ruling on a case in which said act is invoked.

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).

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.

SDN (Software-Defined Network):
a network architecture model that is based on centralised control of network resources, centralised orchestration and virtualisation of physical resources.

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

Single connection 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:
Also referred to as throughput. 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.

TCP (Transmission Control Protocol):
reliable, connected mode, transport protocol developed in 1973. 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 speeds and allows 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.

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.

VoD (Video on Demand):
an interactive technique for distributing digital video content over wireline (Internet) or nonwireline networks. SVoD = subscription VoD services.

VoIP (Voice over IP): technology to transport voice on IP compatible networks through the Internet.

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

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 which 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.

This document was produced by Arcep

Cécile Dubarry, director-general
Virginie Mathot, advisor to the Chair

"INTERNET, PRESS, POSTAL AFFAIRS AND USERS" DEPARTMENT

Loïc Duflot, *director*

"Open Internet" unit

Aurore Tual, *head of unit*
Samih Souissi, *deputy head of unit*
Pierre Faurie and Vivien Guéant, advisors

"Data-driven regulation" unit

Gaspard Ferey, *head of unit*
Léna Morvan, *deputy head of unit*

"ECONOMY, MARKETS AND DIGITAL AFFAIRS" DEPARTMENT

Anne Yvrande-Billon, *director*

"Economic analysis and digital intelligence" unit

Adrien Haïdar, *head of unit*
Chiara Caccinelli, *deputy head of unit*
Estelle Patat and Charles Joudon-Watteau, *advisors*

" MOBILE AND INNOVATION" DEPARTMENT

Franc Tarrier, *director*

"Mobile coverage and investments" unit

Guillaume Decorzent, *head of unit*
Gabriel Aubert, Noé Faure and Axel Piau, *advisors*

"COMMUNICATIONS AND PARTNERSHIPS" DEPARTMENT

Clémentine Beaumont, *director*
Marie-Alix Dadillon and Charlotte Victoria, *advisors*

"LEGAL AFFAIRS" DEPARTMENT

Elisabeth Suel, *director*
Agate Rossetti, deputy to the Director

"Infrastructures and open networks" unit

Rémy Maecker, *head of unit*
Paul Pastor, *advisor*

"EUROPE AND INTERNATIONAL AFFAIRS" DEPARTMENT

Anne Lenfant, *director*

"Europe" unit

Rodolphe Le Ruyet, *head of unit*

Heartfelt thanks to...

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

ANNEX: THE MAIN VIDEO CODECS

1.1. H.262 / MPEG-2 Part 2 (1995)

H.262/MPEG-2 is used little on the Internet but is the codec used on all video DVDs. It is also used for first-generation digital terrestrial television (DTT), i.e. from 2005 to 2016, for cable television and on the first triple play boxes in France. H.262/MPEG-2 is far less efficient than H.264/AVC, and every operator replaced customer premises equipment that was incompatible with H.264/AVC, to be able to stop using this inefficient codec. In 2021, playing DVDs was still the main use of MPEG-2. Resellers of products and services using the H.262/MPEG-2 standard must pay for the right to use a patented technology. As the last American patent expired on 14 February 2018, only patents in the Philippines and Malaysia remained active after that date.

1.2. H.264 / AVC (2003)

H.264/AVC is currently supported by virtually everything that is connected to the Internet. Only a few rare Open-Source purists do not install this proprietary codec on their Linux/BSD system. It is used massively for everything that records and plays video. HD DTT has used H.264/AVC since launching in 2008 (alongside SD DTT in H.262/MPEG-2 from 2008 to 2016). Designed 20 years ago, H.264/AVC has two major drawbacks: there are now more efficient video compression codecs, and it is subject to a licensing fee: resellers of products and services using the H.264/AVC standard must pay for the right to use a patented technology. Firefox does not have an H.264 licence but uses the codec built into the operating system.

1.3. VP8 (2008)

VP8 is a proprietary codec developed by On2 that is technically close to H.264/AVC. In February 2010, Google acquired the company. The Free Software Foundation wrote Google an open letter asking that it release VP8 under a royalty-free licence, and use it on its YouTube video sharing site, which Google did on 19 May 2010 by incorporating it into the WebM project under a Creative Commons attribution licence (CC-by), with a three-clause BSD licence implementation. Its advantage over H.264 is that it was open source at a time when H.264/AVC was not systematically supported by web browsers. It was used by YouTube in addition to H.264 before being replaced by VP9. The compression algorithm used for VP8 key frames is used in WebP image format, which is more efficient than jpeg.

1.4. VP9 (2012)

VP9 is the successor to VP8. VP9 is significantly more powerful than VP8 and H.264/AVC. VP9 enables speeds and video quality comparable to H.265/HEVC but, unlike the latter, it is open source and royalty-free. VP9 can be used on any recent equipment, except in Safari and iOS which carry restrictions on the use of VP9. Apple has in fact implemented VP9, but only makes it available in cases where it is indispensable, e.g. with WebRTC to allow iPhone/Mac users to make video calls, or with YouTube to provide access to 4K resolution videos when only the choices of codec are VP9 and AV1.

1.5. H.265/HEVC (2013)

On the Internet, H.265 is being pushed mainly by Apple which has been using it since 2017, with iOS 11 and macOS High Sierra. Apple is among the firms that earns royalties on this codec. H.265/HEVC is lucrative: initially, it planned to demand royalties equal to 0.5% of the revenue generated by video stream distribution (so 0.5% of the price of VoD videos would go to the Access Advance (formerly HEVC Advanced) licensing administrator company. H.265 should have been a success, including on the Internet, but that did not factor in the arrival of the VP9 and AV1 open-source codes and the lack of support for H.265 outside the Apple ecosystem, and the traditional TV broadcasting ecosystem: Firefox, Edge, Chrome and multiple other web browsers do not support videos encoded with H.265. The codec is used by Ultra HD Blu-rays and ISPs to distribute 4K channels, and could be used by HD DTT a few years from now, which would mean having to use external DTT set-top boxes for the many incompatible TVs.

Here is an excerpt of the French language Wikipedia page on H.265: "*On 26 June 2012, MPEG LA announced plans to licence HEVC patents. Unlike earlier MPEG codecs, however, MPEG LA did not have unanimous support, and two rival patent licensing administrators emerged: HEVC Advance and Velos Media. Some of the industry's biggest companies prefer to licence their patents directly, without going through rights management organisations. Royalties have increased compared to earlier standards, and information on them is not always made public. This uncertainty over costs, which can run into the millions of dollars, was the impetus for the creation of the Alliance for Open Media, which aims to create a royalty-free codec*."

For a number of analysts, the large number of patent pools that must be negotiated with hampered the use of HEVC, and drove a great many players to support a powerful royalty-free codec: AV1.

1.6. AV1 (2018)

AV1 is more powerful than VP9 and H.264, with an efficiency close to H.265/HEVC (some studies show that AV1 is more powerful than H.265/HEVC, others less). AV1 was developed by the Alliance for Open Media – whose members include Cisco, Google, Intel, Microsoft, Mozilla, Netflix... – and who pooled their technical expertise to develop the AV1 codec. AV1 can be used on any recent browser, except Safari. AV1 benefits from a hardware acceleration (lightening the load on the CPU) on the generations of smartphones and microprocessors designed in 2021. Playback is still possible on older smartphones using the microprocessor to decode the stream.

AV1 will probably enjoy another advantage over H.264 by still being readable in in 15 years. Those who still have MPEG-2 encoded video, the format used by DVDs, have noticed as much since support for MPEG-2 is being removed more and more from software and hardware. Windows 10, for instance, no longer supports it, to avoid having to pay royalties, and even though it was integrated into earlier versions of Windows. MPEG-2 videos cannot be read in Linux, by default. The same future could be awaiting H.264.

The compression algorithm used for AV1 key frames is used in AVIF image format, which is more efficient than jpeg and WebP.

1.7. H.266/VVC (2020)

H.266/VVC for Versatile Video Coding was published by the Joint Video Experts Team (JVET) on 6 July 2020. As with HEVC, two patent pools were created for the use of its patents: MPEG LA and Access Advance. VVC is said to be more efficient than AV1, but it is still too early to know whether it will be used.

1.8. AV2 (en développement)

AV2 is the successor the AV1 codec, and currently being developed by the Alliance for Open Media.

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

Design
Agence Luciole

Translation
Gail Armstrong

Photos' credits
p. 6, 7, 8 and 9: Adobe Stock
p. 8 : Directique, Arcep's 2021
measurement campaign (Guyana,
the Caribbean)
p. 43 and 44 : « Interxion: A Digital
Realty Company »

Illustrations
p. 61: Carte done by Vivien Guéant
based on the map from Simon
Giraudot,under the terms of licence
CC BY-SA 2.0
p. 64: Simon Giraudot

June 2022

ISSN n°2258-3106

MANIFESTO

NETWORKS AS A COMMON GOOD ARCEP

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.