

2021 REPORT

The state of the internet in France

**2021
EDITION**

TOME 3

2021 REPORT

The state of the internet in France

Table of contents

INTRODUCTION	06	PART 2	70
2020 Arcep Highlights	06	ENSURING INTERNET OPENNESS	
Networks during the Covid-19 crisis	10	CHAPTER 4	
		Guaranteeing net neutrality	71
PART 1	19	CHAPTER 5	
ENSURING THE INTERNET FUNCTIONS PROPERLY		Platforms: internet access gatekeepers	87
CHAPTER 1		PART 3	96
Improving internet quality measurement	20	TACKLING DIGITAL TECHNOLOGY'S ENVIRONMENTAL CHALLENGES	
CHAPTER 2		CHAPTER 6	
Supervising data interconnection	38	Working to achieve digital sustainability	97
CHAPTER 3		LEXICON	104
Accelerating the transition to IPv6	48		

Editorial

THE YEAR 2020: BETWEEN CHALLENGES RELATED TO THE PUBLIC HEALTH CRISIS AND PERSPECTIVES REGARDING PLATFORM REGULATION



**By Laure
de La Raudière,**
*President
of Arcep*

The public health crisis and resulting lockdown in France provided us with a stark reminder of how vital networks are to the life of the country, notably for competitiveness, growth and employment. Many people in France also discover new uses during the lockdowns: remote working, online learning, remote medical visits with close relatives to maintain social links. This crisis illustrated the need for each household, in all parts of the French territory, to have a high quality internet connection.

This exceptional situation confirmed the extent to which networks are and must remain a “common good” and an “infrastructure of freedom”. Internet is indeed an area of freedom: freedom of expression, freedom to communicate, freedom to access knowledge and to share it, but also freedom of enterprise and innovation.

**“Networks are and must
remain a ‘common good’”**

Because it is essential in all open, innovative and democratic societies to be able to enjoy these freedoms fully, it is more than ever necessary to ensure that internet meet high standards in terms of accessibility, universality, performance, neutrality, trustworthiness and fairness.

The Internet’s founding principles, notably equal treatment and routing on both the access and distribution sides must remain. The net neutrality principle, enshrined in Europe through the Open Internet Regulation in 2016, constitutes a legal framework to safeguard these principles.

The European legislator now imposes to Internet service providers (ISPs) obligations that national regulators would control and apply sanctions if necessary. In France, Arcep is the body responsible for implementing net neutrality and ensuring that ISPs comply with it.

However, if the European Open Internet Regulation enshrines users’ right to access and distribute information and content online, it applies solely to ISPs. Located at the end of the internet access chain, devices (smartphones, voice assistants, connected cars...) and structural platforms’ closed ecosystems

(aka gatekeepers) have proven to be the weak links in achieving an open internet. Arcep shared this conclusion on devices in its 2018 report and extended this examination to the operators of the gatekeeper platforms in 2019. As for the debate on internet openness, Arcep also mobilized the European level, notably through the European network of telecommunications regulators.

This work contributes to the opening of a new sequence of digital regulation for the European Commission which published two proposed regulations. Through the Digital Services Act, the European Commission is proposing to review the e-commerce Directive of 2000, and particularly the liability provisions governing hosted content, which apply to technical intermediaries. Through the Digital Market Act, the Commission aims at introducing an *ex ante* economic regulation of the largest technology companies qualified as gatekeepers¹.

“The proposal of Digital Markets Act marks a major step forward”

The proposal of Digital Markets Act marks a major step forward, but warrants being strengthened in several respects.

It seems particularly necessary to better consider the ecosystemic dimension of certain undertakings with a view to improving competition conditions, including between platforms themselves. This would create the ability to take fuller account and foster the freedom of choice of end users who, today, can be captive to a centralised ecosystem.

The regulator needs to be equipped with proactive tools and to strengthen the resources it is allocated to ensure its *ex ante* intervention can be implemented effectively. This will include strengthening the process of monitoring these gatekeepers to reduce information asymmetry and, alongside the obligations set in advance and which apply to every player, to plan for tailored remedies that are more suitable than a one size fits all solution. Increased cooperation between the Commission and Member States could make the system more efficient, and provide critical resources and support mechanisms.

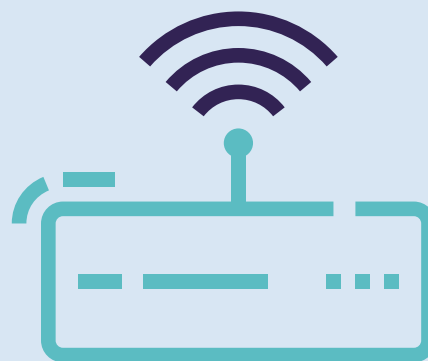
Arcep, as architect and guardian of communication networks in France, will continue to ensure internet openness and also rely on the mobilization of the entire ecosystem to carry out this mission.

1. This notion is very similar to the concept used by the Authority of structural digital platform operators.

16 JANUARY 2020

Internet quality of service

The Government approves in an Order published in the Journal Officiel the Arcep decision No. 2019-1410, which aims at implementing an “access ID card” API by operators, marking the start of the deployment calendar.



2020 ARCEP HIGHLIGHTS

SPRING 2020

Monitoring networks during the public health crisis

The outstanding mobilisation of all of the ecosystem’s players (public institutions, operators, content and application providers and end users) made it possible to deal with the unprecedented intensity of digital needs, to reduce congestion risks and to ensure compliance with net neutrality.



6 APRIL 2020

Environment

Arcep includes environmental indicators to its annual gathering campaign (greenhouse gas emissions related to electricity consumption and activities of the telecommunications operators). Arcep co-chairing a new BEREC expert working group devoted to sustainability which aims at studying the environmental impact of telecom networks in the broadest sense, and exploring avenues for reducing it.



11 JUNE 2020

Environment

“Achieving digital sustainability”: Arcep is launching a collaboration platform and calling all the digital and environment ecosystem players to debate together and contribute to the first progress report. The inaugural meeting on 9 July 2020, attended by 65 participants, allows to identify points that warrant closer attention and potential courses of actions.

16 JUNE 2020

Open Internet

The Body of European telecommunications regulators, BEREC, publishes the revised guidelines which aims at guiding national regulators on the Open Internet Regulation, adopted in November 2015. In France, Arcep is in charge of implementing net neutrality and ensuring that Internet service providers (ISPs) comply with it.

7 SEPTEMBER 2020

Regulating platforms

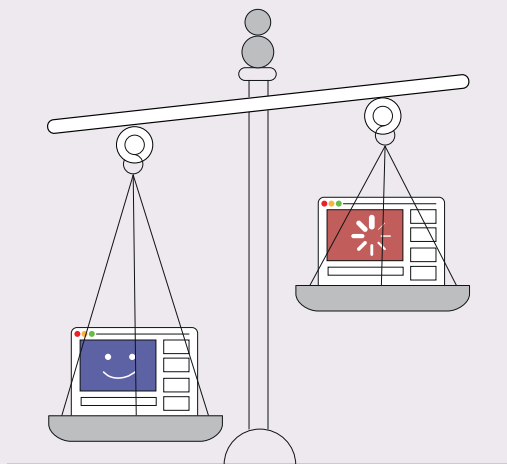
Arcep responds to the European Commission’s public consultation on the Digital Services Act, urging the European Union to adopt *ex ante* regulation on gatekeeper platforms, and once again ensure that the internet is a place of freedom of choice and innovation.

14 SEPTEMBER 2020

Internet quality of service

Arcep published the 2020 version of the Code of conduct on internet quality of service. It is to encourage QoS measurement tools to increase the transparency and robustness requirements for measurement protocols and for results publications.





15 SEPTEMBER 2020

Open Internet

First interpretation from the Court of Justice of the European Union on the net neutrality regulation, on a question related to a Hungarian operator's zero-rating offers.



4 DECEMBER 2020

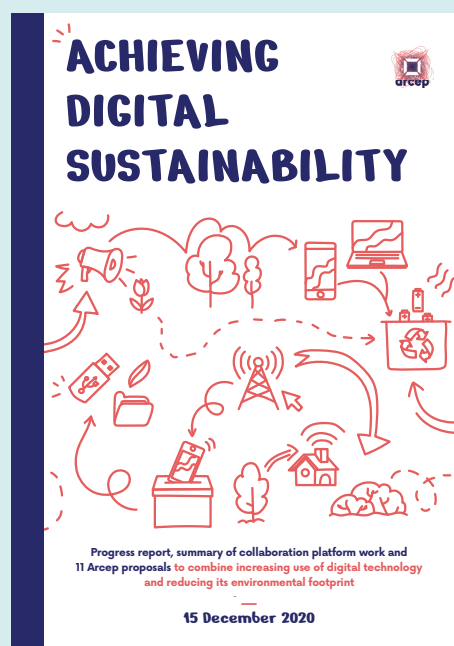
Transition to IPv6

Arcep publishes its 2020 barometer of the transition to IPv6, which reveals significant but still insufficient progress in the migration to IPv6, and the first handbook of the IPv6 task-force "Businesses: why switch to IPv6?".

AUTUMN 2020

Environment

"Achieving digital sustainability": Between September and November 2020, Arcep organises five thematic workshops and two "big discussions", occasions for everyone to trade views, practices, tools and skills on electronic communications networks, devices, datacentres and ICT use.



8 DECEMBER 2020

Mobile quality of service

Arcep publishes the findings of its measurement campaign for 2020: QoS continues to improve despite the public health crisis, the average download speed measured in Metropolitan France stands at 49 Mbit/s, compared to 45 Mbit/s in 2019, and Arcep publishes the first coverage maps with increased reliability threshold from 95% to 98%.



15 DECEMBER 2020

Environment

“Achieving digital sustainability”: Arcep publishes a progress report and 11 proposals to combine increasing use of digital tech and reducing its environmental footprint. This report results from the dialogue within the “Achieving digital sustainability” collaboration platform and includes 42 contributions authored by the participating players.

15 DECEMBER 2020

Regulating platforms

The European Commission published two regulation proposals: the Digital Services Act, reviewing the e-commerce Directive of 2000, and the Digital Market Act, whose aim is to introduce an *ex ante* economic regulation of the largest technology companies.



31 DECEMBER 2020

Transition to IPv6

Arcep introduces an obligation for operators who are awarded a licence to use 5G frequencies in the 3.4 – 3.8GHz band in Metropolitan France to make their mobile network compatible with IPv6 as of 31 December 2020.

21 DECEMBER 2020

Open Internet

Arcep launches a new version of the Wehe application, available for users to detect internet traffic throttling and port blocking. The application is available for free in French, on Android, iOS and F-Droid store.



END OF 2020

Data interconnection

Thanks to the information gathering on data interconnection and routing, Arcep updates its barometer on data interconnection in France with 2020 data.



NETWORKS DURING THE COVID-19 CRISIS

The Covid-19 public health crisis affected network use in several ways, especially during the first lockdown in spring 2020. The observations and main lessons drawn from this time thus derive chiefly from that period. Arcep will confine itself here to the topics addressed in this report and, despite their significance, will not address the issues surrounding digital inclusion that arose during this crisis.

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

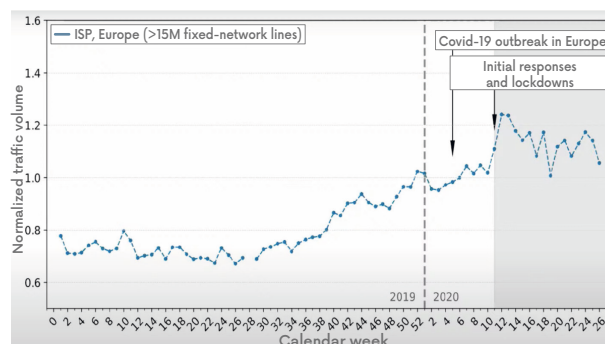
This situation raised a number of questions about the Internet's operation that tie into the topics addressed in this report: How did the lockdown affect network use? Were the networks properly scaled to handle the surge in traffic related to the crisis? What were the main sources of potential congestion?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

HOW DID THE COVID-19 CRISIS AND THE LOCKDOWN AFFECT NETWORK USE?

The change in usage patterns resulted in a tremendous surge in internet traffic for ISPs: increasing by around 30% during the first lockdown, according to some estimates^{1,2}. An equivalent increase in traffic also occurred at internet exchange points (IXP). This was observed in particular at the two points of presence (PoP) in Paris and Marseille³ belonging to France-IX, the country's largest internet exchange point.

On mobile networks, meanwhile, no significant increase in traffic was observed during the first lockdown, even if some temporary congestion was experienced in France.

EVOLUTION OF THE MAIN EUROPEAN ISPS' TRAFFIC DURING THE FIRST HALF OF 2020



Source: "The Lockdown Effect: Implications of the Covid-19 Pandemic on Internet Traffic"

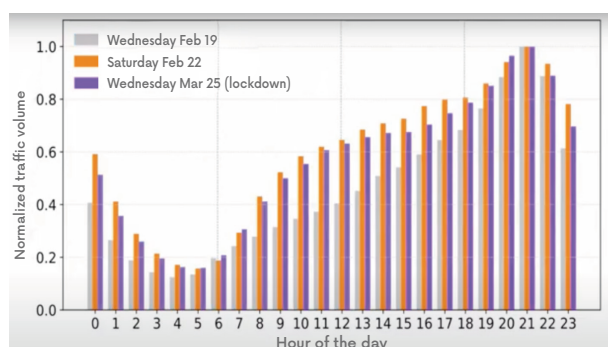
One major change to the traffic profile was observed: the traffic peak that typically happens in the evening was "spread out" across the entire day. So the daytime traffic profile more closely resembled the traffic profile typically observed at weekends. This change in profile can be attributed to changes in users' behaviours, notably an increase in the use of videoconferencing tied to remote working, but also to an increase in video streaming and online gaming, both of which consume a great deal of bandwidth.

1. Netscout report based on data from French ISPs.

2. Anja Feldmann, Oliver Gasser, Franziska Lichtblau, Enric Pujol, Ingmar Poesse, Christoph Dietzel, Daniel Wagner, Matthias Wichtlhuber, Juan Tapiador, Narseo Vallina-Rodriguez, Oliver Hohfeld, and Georgios Smaragdakis. 2020. The Lockdown Effect: Implications of the Covid-19 Pandemic on Internet Traffic. In Internet Measurement Conference (IMC '20), October 27–29, 2020, Virtual Event, USA. ACM, New York, NY, USA, 18 pages. <https://doi.org/10.1145/3419394.3423658>

3. <https://www.franceix.net/en/technical/traffic-statistics/>

CHANGE IN THE DAILY TRAFFIC PROFILE



Source: "The Lockdown Effect: Implications of the Covid-19 Pandemic on Internet Traffic"

According to some crowdsourcing tools, internet quality of service (QoS) decreased slightly during the first lockdown, which could be tied to the increase in traffic and the few congestion incidents that occurred. According to the Ookla observatory on the impact of the Covid-19 pandemic on internet performance⁴, average speeds measured on the fixed network in France decreased from 146.26 Mbit/s on 9 March 2020 to 126.45 Mbit/s on 13 April 2020, which is equal to around -15%. This variation was also observed by nPerf⁵ but is less visible in the QoS⁶ 2020 annual barometer. The variation in QoS was less overt on the mobile network (around -5% between March and April 2020⁷). Speeds on fixed and mobile networks were back to normal around two months later, so the impact on QoS was minimised over the long term.

An increase in the number of QoS tests performed by end users was also observed during this period, which testifies to consumers' use of crowdsourced testing tools, especially when there is a drop in quality of service. Ookla, for instance, experienced a peak of +77% fixed network testing at the start of the first lockdown in France.

Lastly, an increase in the rate of IPv6 use was also observed during the first lockdown, which could be explained in particular by the increase in residential traffic, which is more widely IPv6-enabled than business internet access (cf. chapter 3 on IPv6).

Despite a massive increase in internet usage and traffic, fixed and mobile internet networks demonstrated their resilience during the first lockdown.

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

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

Overloads can sometimes occur at the Local Access Network (LAN) level inside users' homes, e.g. because of an over-solicited Wi-Fi connection⁸. Looking beyond these limitations that may exist at the end user level, this section focuses on the potential congestion points for the different players along the Internet chain. To put it simply, and as illustrated above, congestion issues can occur at three levels: with content and application providers (CAPs) or on content delivery networks (CDNs) (1), on intermediary networks and exchange points (2) and on Internet service providers' (ISPs) networks (3).

4. <https://www.speedtest.net/insights/blog/tracking-covid-19-impact-global-internet-performance/#/France>

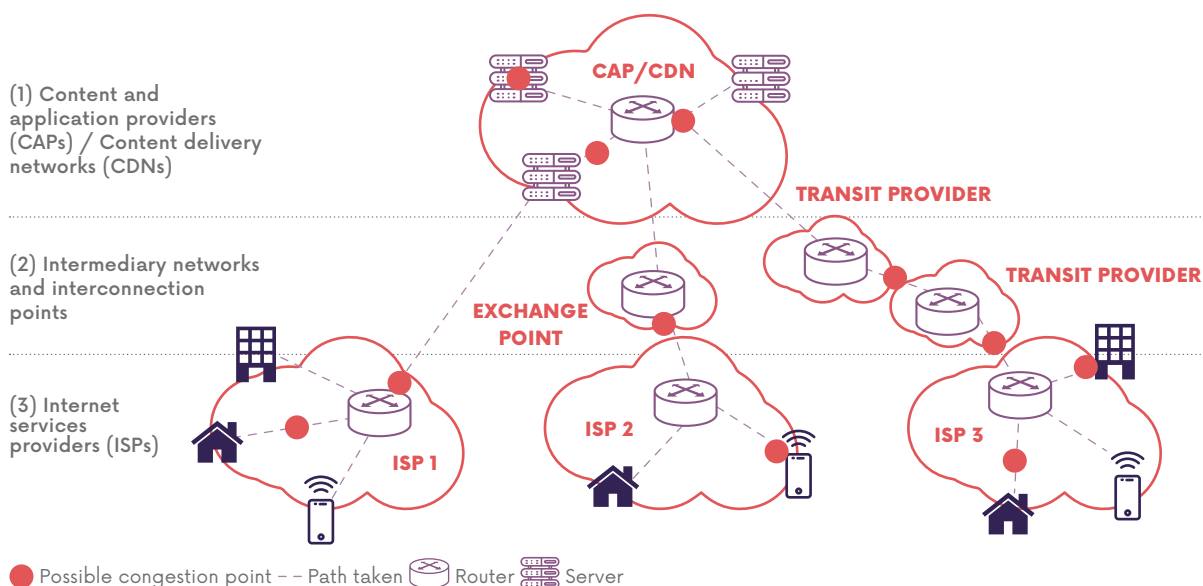
5. Barometer of fixed Internet connections in Metropolitan France in the first half of 2020: https://media.nperf.com/files/publications/FR/2020-07-27_Barometre-connexions-fixes-metropole-nPerf-S1-2020.pdf

6. Study of the quality of experience (QoE) provided by mobile operators in Metropolitan France in 2020: https://www.5gmark.com/news/2020/Etude_Connectivite_Mobile_France_QoS_2020_v1.pdf

7. <https://www.speedtest.net/insights/blog/tracking-covid-19-impact-global-internet-performance/#/France>

8. See the next section on optimising usage.

SIMPLIFIED ILLUSTRATION OF POSSIBLE NETWORK CONGESTION POINTS



Source: Arcep

Congestion can occur on CAP/CDN (1) servers when a service is more solicited than usual. This overload can be due to hardware (processor, memory, network card, etc.) or software-related (exceeding the maximum number of simultaneous users, open files, open TCP ports, etc.) limitations. There are a number of other possible points of congestion at the CAP/CDN level: links, aggregation, backhaul, firewall⁹ and routing equipment can all create bottlenecks if their (physical or assigned) capacity in bits per second or packets per second is exceeded.

Congestion can occur on intermediate networks and interconnection points (2) links if they are not sufficiently scaled to handle the amount of traffic being relayed. This congestion will typically manifest itself on a private peering link, a public peering link (at an IXP), between a CAP and a transit provider, between two transit providers or between a transit provider and an ISP. Depending on where the overload occurs, it can affect one or several services, or one or several players. Internet stakeholders usually overprovision and ensure redundancy for interconnections, to be able to handle exceptional situations, such as major sporting events. To a certain extent, the situation tied to the Covid-19 crisis was unprecedented, and caused an important surge in traffic on the network.

Congestion can occur at several levels on ISPs' networks (3): at the access level, both fixed or mobile, on the ISP's transport/backhaul network or in the ISP's core network. When a customer subscribes to a fixed Internet plan, they are not allocated their plan's advertised bandwidth end to end (unless they have a special

contract): at each point in the network, a greater capacity is shared between the different users, based on the presumption that not all users employ their connection at maximum speed simultaneously¹⁰. Here too, the network is scaled to ensure it does not get overloaded, but an atypical situation has the potential to cause congestion. In addition, on the mobile Internet, congestion can occur in a given cell, notably when several of the users connected to that cell solicit bandwidth-hungry applications (video streaming, videoconferencing, downloading, etc.).

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

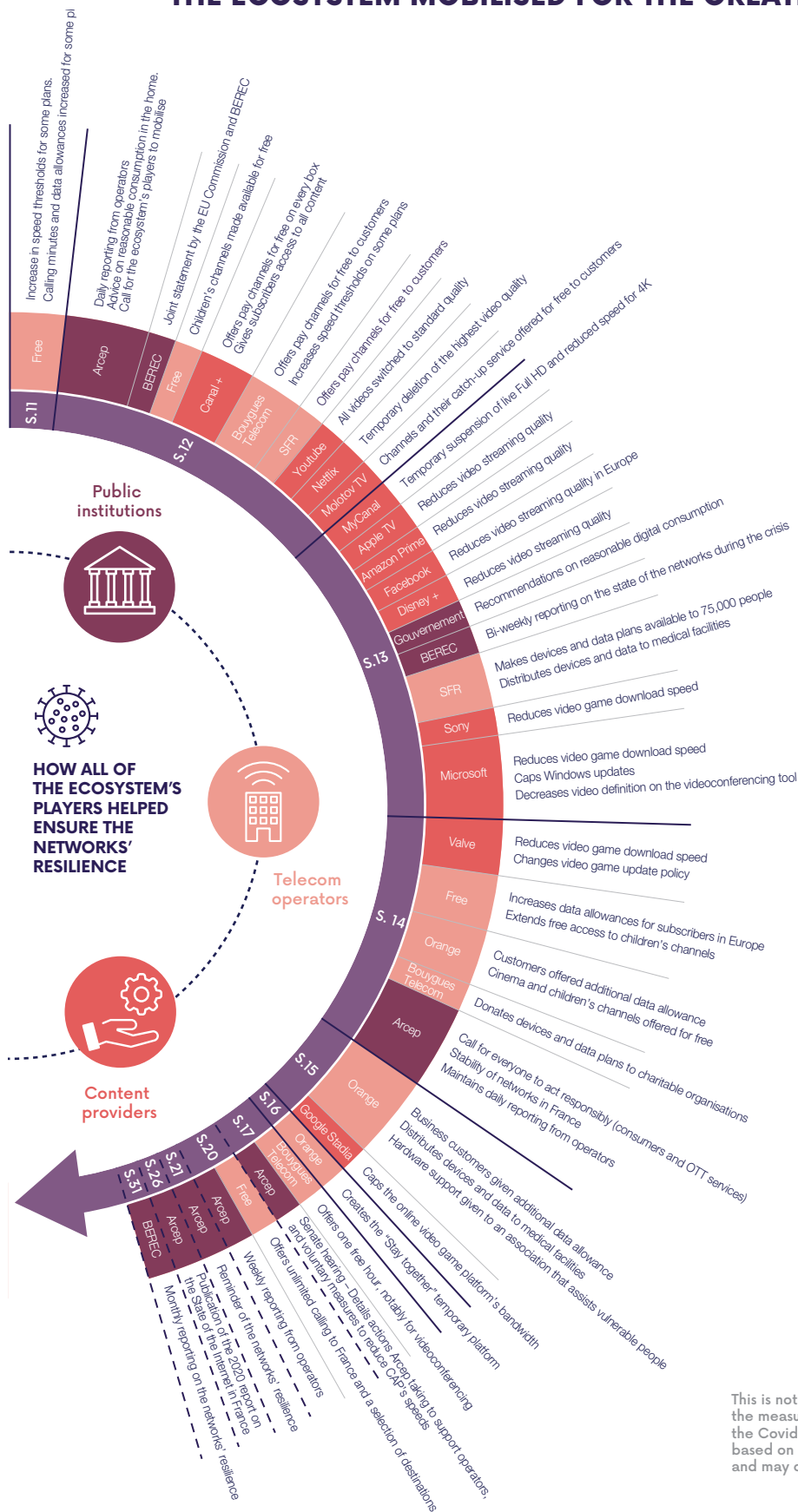
In addition to the Internet network, congestion can also occur on voice calling networks. This happened during the first days of the lockdown: a sharp increase in phone calls caused occasional and temporary overloads on voice networks. Operators' rescaling of the affected interconnections rapidly solved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

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

9. See lexicon.

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

THE ECOSYSTEM MOBILISED FOR THE GREATER GOOD



This is not an exhaustive list of all of the measures that were taken during the Covid crisis. It was produced based on publicly available information, and may contain errors or inaccuracies.

Source: Arcep

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

It was the outstanding mobilisation of all of the ecosystem's players (operators, content and application providers, end users and public institutions) that made it possible to cope with the unprecedented intensity of digital needs during the crisis. Telecoms companies and the entire fabric of small and medium businesses, local stakeholders and associations that surround them, worked in concert to maintain the networks and ensure that they continued to run smoothly. In addition to the mobilisation of their teams in the field, operators also handed out a number of bonuses to customers: additional mobile data, free calling, free access to pay-TV channels, increased speeds for certain plans, etc. Lastly, operators also donated devices and data to hospitals and associations that assist the most vulnerable and underprivileged members of society, to help everyone stay connected.

Following a proactive dialogue initiated by the Government, or on their own initiative, content and application providers also contributed to the collective effort. "Heavy" network users, such as video streaming platforms and online gaming platforms reduced the strain their content put on the network by capping the bandwidth their services required, by downgrading the quality of their videos and by scheduling downloads and service updates during off-peak hours. The dialogue established between Disney and operators also helped anticipate the launch of Disney's new video streaming platform. Unlike other CAPs, the architecture Disney chose was not based on its own content delivery network (CDN)¹¹ but rather on third-party CDNs, hence the potential to overload an interconnection link shared with a CDN hosting other content, should the platform's launch cause a spike in traffic. The rescaling of certain interconnections was therefore required to prevent potential risks of network overload.

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

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



Source: Arcep

11. See Lexicon.

By the same token, end users too were able to contribute to the joint effort to relieve the networks, by adapting their usage – notably by following the recommendations that the Government and Arcep issued on best practices, for instance when teleworking¹², as well as Arcep recommendations on how to improve a home Wi-Fi¹³ connection. The end users who followed these tips thus switched from using 4G to Wi-Fi when at home, boosted their Wi-Fi connection (e.g. by using Wi-Fi repeaters), spread their digital service use out across the day, and postponed the use of any bandwidth-hungry tasks and applications to off-peak hours

Throughout the crisis, the Government and Arcep monitored telecom networks' evolution on a daily basis. Alongside the mechanisms devoted specifically to the operational management of the crisis, operators reported to the Government and Arcep on the status of their networks – initially every day, and later less frequently. Telecoms networks' resilience is also a transnational matter, and European regulators, of which Arcep is one, worked together within BEREC to actively monitor the state of European networks. BEREC also published a bi-weekly, then monthly, report detailing the state of networks in Europe during the crisis, which consistently concluded that no major network congestion had occurred in the EU.

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

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

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

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

In the very early days of the crisis, Arcep and the Government also established a dialogue with operators to ensure ongoing compliance with net neutrality rules, despite the exceptional circumstances. Operators' constant dedication to maintaining their networks, combined with the mobilisation of all of the ecosystem's stakeholders, enabled the networks to continue to function in an uninterrupted and neutral fashion throughout the entire crisis.

The issue of telecommunications networks' resilience also arose at the European level. In a joint statement¹⁴, the European Commission and BEREC reminded operators of their ability to adopt such exceptional traffic management measures when congestion was imminent. The different reports, produced by BEREC, do not mention any formal decision taken by any EU Member State on the basis of Article 3 of the Open Internet regulation, tied to the Covid crisis.

And so, despite the gravity and hardship of the public health crisis in France and in Europe, the Open Internet regulation proved its ability to withstand any circumstances.

12. Best practices for using the Internet for telework, published by Arcep: <https://www.arcep.fr/demarches-et-services/utilisateurs/teletravail-et-connexion-internet.html>

13. Tips on how to improve your Wi-Fi signal: <https://www.arcep.fr/demarches-et-services/utilisateurs/comment-ameliorer-la-qualite-de-son-wifi.html>

14. Joint statement from the European Commission and BEREC on coping with the increased demand for network connectivity due to the Covid-19 pandemic: https://berec.europa.eu/eng/document_register/subject_matter/berec/others/9236-joint-statement-from-the-commission-and-the-body-of-european-regulators-for-electroniccommunications-berec-on-coping-with-the-increased-demand-for-network-connectivity-due-to-the-covid-19-pandemic

Open floor to



LUCA BELLÌ

PhD, Professor at Fundação Getúlio Vargas Law School (FGV - Rio de Janeiro), Coordinator of the Center for Technology and Society at FGV, and Chair of the Coalitions on Net Neutrality and on Community Connectivity of the UN Internet Governance Forum (IGF)

THE VALUE OF INTERNET OPENNESS IN TIMES OF CRISIS: NET NEUTRALITY, COMMUNITY NETWORKS AND DIGITAL SELF-DETERMINATION

The Covid-19 pandemic has harshly highlighted the fundamental importance of Internet access, and the total exclusion that the unconnected face in times of crisis. Our new routine relies on online meetings, e-learning, telemedicine, and e-commerce apps. However, for the almost 4 billion people who do not enjoy Internet connectivity or cannot afford it, the arrival of Covid-19 equals to house-arrest. Moreover, an undefined portion of the population formally considered as “connected” is de-facto only partially connected.

Official statistics consider as a connected individual someone who has accessed the Internet at least once over the past three months.¹ Such definition is questionable and fails to consider the incredibly large number of undue restrictions, either politically or economically motivated, that affect how an individual is connected.

If your access is blocked or throttled, but you have accessed one of few government-approved websites, once, over the past three months, you are formally considered as a “connected individual,” despite the fact your connectivity is remarkably limited. By the same token, the “Internet” experience of needy persons who cannot afford “full” Internet access subscriptions (i.e. most of the world population) is limited to few sponsored apps

(typically dominant social networks featured in so-called zero-rating plans)². These users are far from being “connected” Individuals, but are officially considered as such.

Internet users are active “prosumers” as they can access but also create and share any content or applications of their choice. They can actively contribute to the evolution of the Net through their creativity and innovation. This idea to keep the end-user at the centre of the Internet is the essence of the original Internet architecture, considering that the “intelligence” of the Net “is end-to-end.”³ This same philosophy is at the core of Net Neutrality regulations that demand that Internet Access Providers treat Internet traffic with no discrimination based on their commercial interests.

The importance to preserve and foster Internet openness is key in the context of the current pandemic. Indeed, Covid-19 forces us to face some tough questions. How can almost half of the world be still excluded from connectivity? How can we think that those only accessing a small number of predefined apps once every three months can be considered as connected individuals? How can we think that “zero-rated” apps, that are falsely presented as “free”⁴ and paid with personal data – and anything that may be done out of them – represent

a sustainable business model, instead of exacerbating the evident problems of concentration, lack of competition, while undermining (digital) sovereignty? What can we do differently?

To address such questions and provide concrete answers, the UN Internet Governance Forum (IGF) Coalitions on Net Neutrality and on Community Connectivity organised a joint report dedicated to **The Value of Internet Openness in Times of Crisis**.⁵ Below, some key considerations addressed by this IGF outcome.

First, Internet access has become vital for our economies, societies, and democracies to function. Digital divides have, therefore, an enormous economic, social, and democratic impact. Divides exist not only between those who lack access and those who have it, but also amongst those formally considered as “connected.” The Internet experience of the “meaningfully connected”⁶, who enjoy high-quality Internet and all its benefits, is radically different from the poorly connected, who are obliged to trade their privacy for sponsored apps and are left with low-quality and limited connectivity.

When the pandemic exploded, the European Commission and BEREC started to regularly monitor Internet traffic to identify congestion phenomena. Indeed, the Open Internet Regulation (EU) 2015/2120

1. ITU (2014). *Manual for Measuring ICT Access and Use by Households and Individuals*, p.81.

2. <http://www.zerorating.info/>

3. Carpenter (1996). *Architectural Principles of the Internet*. Request for Comments: 1958.

4. Belli & Zingales (16.02.21). *WhatsApp's New Rules: Time to Recognize the Real Cost of 'Free' Apps*. Medianama.

5. Belli, Pahwa & Manzar (Eds.) (2020). *The Value of Internet Openness in Times of Crisis*. Official Outcome of the UN IGF Coalitions on Net Neutrality and on Community Connectivity.

6. See <https://a4ai.org/meaningful-connectivity/>

prescribes that traffic management measures going beyond the reasonable traffic management may be applied to prevent or mitigate the effects of temporary or exceptional congestion. While traffic increase was observed in both fixed and mobile networks no exceptional congestion was reported. Even under stress, European networks, regulations, and institutions have proven resilient. Unfortunately, this rosy picture applies only when an individual already enjoys Internet access.

Connectivity challenges are still widespread, even in the most developed countries. Hence, it is time to consider alternative solutions to expand connectivity, as those we traditionally use have clear limits.

Many groups of individuals around the world have not resigned to be left with the false choice between poor connectivity, zero rating plans paid with personal data or no access at all. They have decided to become protagonists of their digital future and create their crowd-sourced infrastructures, known as Community Networks.⁷

Local communities, NGOs, small businesses, and administrations are building their own networks, to overcome lack of Internet coverage, developing services that cater for the needs of the local populations. These initiatives unleash new opportunities for education, trade, employment for the locals, in an open and decentralised fashion⁸.

Community networks are designed, owned, and managed by the locals for the locals. They represent a new paradigm, where connectivity is considered and is managed as a common good. They demonstrate that, when people have information on how to build their networks and are free to choose this option, they do so. In such context, people act as true Internet users: empowered prosumers, that do not need to trade privacy for apps and are free to access, create and share any content and innovation that correspond to their needs. As such, people become again the key engine of openness and the driving force of digital self-determination.⁹

7. See <https://comconnectivity.org/>

8. Belli (2017). « Network Self-Determination and the Positive Externalities of Community Networks ». In Belli (Ed). *Community Networks: the Internet by the People, for the People*. FGV Direito Rio.

9. Belli (2018). *Network self-determination: When building the Internet becomes a right*. IETF Journal.

Open floor to



MARIE-LAURE DENIS

President - CNIL

DATA PROTECTION BEING CHALLENGED BY THE COVID CRISIS AND NEW DIGITAL BEHAVIOURS

2020 was the most important year for the internet since the release of the smartphone in 2007. If it is still hard to measure all of its effects, the pandemic no doubt drove the most dramatic change in digital behaviours of the past several years, by developing new habits such as click & collect shopping and remote doctor's visits, and by inexorably consolidating other uses, such as streaming and remote working, which will cause a tremendous upheaval in how work and the workplace are organised.

By brutally recalibrating modern societies' priorities, this was also a year of notable developments in the digital ecosystem: the advent of the term "digital sovereignty" in French and European dialogues; the ability to entrust mobile phone and computer manufacturers, in some countries, with the contact tracing protocol to prevent contamination, and the surge in cyberattacks on companies, government agencies and hospitals who may have switched to an "all-digital" system a little too hastily. From a broader perspective, what marked this year was the increased conviction that, more than ever before, digital industry players' behaviour must align with the expectations of our fellow citizens.

CNIL was involved on many fronts, first by devoting a great deal of effort to managing the pandemic,

monitoring new information systems and one (national contact tracing) application, TousAntiCovid. This app came under especially close scrutiny in terms of default privacy protection mechanisms, in both its protocol and its development. CNIL also issued several opinions on the *Health Data Hub*, whose aim is to provide an infrastructure to foster health research. To this end, the question of transferring data outside the European Union for cloud IT services was raised, and the "Schrems 2" ruling from Court of Justice of the European Union in July 2020 confirmed that data protection requirements also apply when data leave our continent. The effects of this order, which challenges a host of businesses' data practices, are already being felt. We have seen a series of announcements over the past several months, proposing new personal data management schemes which, at minimum, protect these data from being unlawfully accessed in foreign countries and even, in certain case, guarantee that these data and services will be stored, processed and given customer support within the EU.

If it is not CNIL's task to pass judgement on this or that development's economic or industrial merits, these efforts do reflect the increased importance given to data

protection since the GDPR¹ came into effect in 2018. Here, we could also cite the controversy over the updated terms of use for WhatsApp, which drove Facebook to postpone their implementation by several months, or CNIL's imposition of two penalties, of 100 M€ and 35 M€ on Google and Amazon, respectively, after having ascertained their failure to obtain users' free and prior informed consent to drop advertising cookies.

Looking into the future, it is likely that digital behaviours, adopted during the lockdowns of the past year, will continue to develop, and create new challenges for regulators. To keep pace with this changing landscape, networks too need to evolve, on the mobile front with 5G but also on fixed networks, which are poised to switch over massively to fibre. The work that Arcep is doing on consolidating the measurement of fixed network QoS is particularly useful during this period, and the method employed, based on the introduction of APIs onto operators' equipment shows that regulators too can adopt new approaches. While this practice may raise some questions about the processing of subscriber data, CNIL is fully committed alongside Arcep to an exemplary approach to inter-regulation that seeks to establish operational rules that safeguard individuals' privacy.

1. See Lexicon.

PART 1

Ensuring the internet functions properly

19

CHAPTER 1

Improving internet quality measurement

CHAPTER 2

Supervising data interconnection

CHAPTER 3

Accelerating the transition to IPv6

IMPROVING INTERNET QUALITY MEASUREMENT

What you need to know

In summer 2021,

operators will need to demonstrate to Arcep that they have developed a box with the "Access ID card" API. The API will then be gradually deployed in users' boxes.

Ten 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 continues to improve: average speeds in Metropolitan France reached

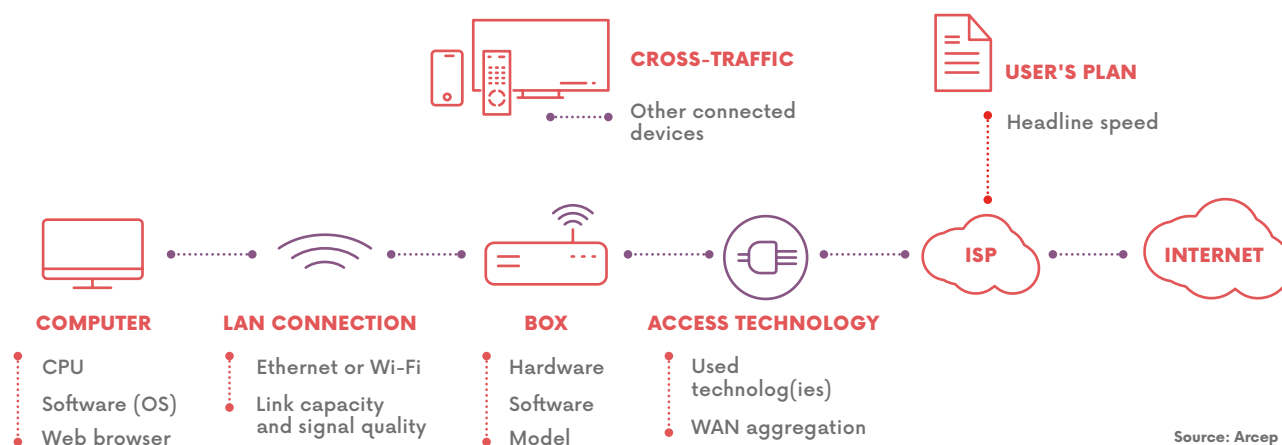
49 Mbit/s
in 2020.

Internet quality of service depends, first, on infrastructures' ability to provide increasingly high speeds, notably by deploying fibre 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 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.

20

CARACTERISTICS OF THE USER ENVIRONMENT



1 Potential biases of quality of service measurement

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

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

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

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

2 Implementing an API in customer boxes to characterise the user environment

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, fibre, 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-construction¹ approach initiated by Arcep involves some 20 players, including crowdsourcing measurement tools, ISPs,

consumer protection organisations and academia. The ecosystem reached a consensus on the implementation of an Application Programming Interface (API) that would be installed directly in operators' boxes, and could be accessed by tools that comply with the Code of conduct that Arcep published². This software interface will allow access boxes to transmit the information that make up the "Access ID card".

A public consultation was held on this topic in spring 2019: the 17 responses that Arcep received, and published³, made it possible to adjust the mechanism for implementing the API, working in concert with the ecosystem's players. Arcep adopted the corresponding Decision in late October 2019⁴, which the Government approved in an Order that was published in the Journal Officiel on 16 January 2020⁵.

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.

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

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

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

1. Description of the API co-construction process: https://www.arcep.fr/uploads/tx_gspublication/rapport-etat-internet-2018_conf050618.pdf#page=11

2. 2020 edition of the quality of service Code of conduct: https://www.arcep.fr/uploads/tx_gspublication/code-de-conduite-QoS-internet-2020_sept2020.pdf

3. Responses received to the public consultation: https://www.arcep.fr/uploads/tx_gspublication/reponses_consultation_publique_api_box-oct2019.zip

4. Arcep Decision No. 2019-1410 of 10 October 2019: https://www.arcep.fr/uploads/tx_gsavis/19-1410.pdf

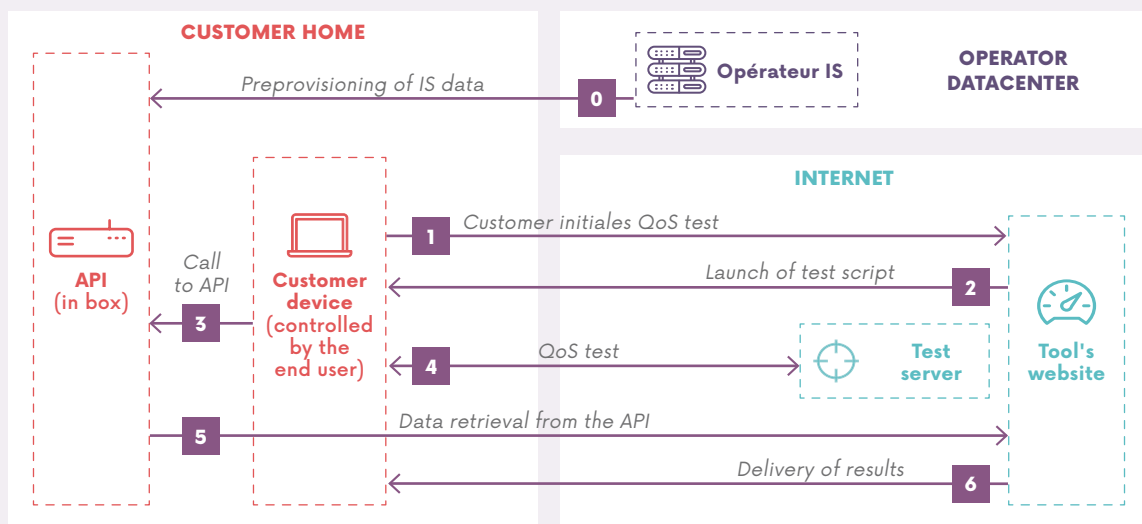
5. Order of 8 January 2020 approving Arcep Decision No. 2019-1410: <https://www.arcep.fr/fileadmin/cru-1624346775/reprise/textes/arretes/2020/arr-08012020-homolog-2019-1410-api-box.pdf>

MORE INFORMATION ON THE "ACCESS ID CARD" API

How does the API work?

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

HOW THE "ACCESS ID CARD" API WORKS



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

Source: Arcep

Which measurement tools have access to the API?

The API will be accessible to those measurement tools that have been declared compliant with the Code of conduct on Internet quality of service published by Arcep. The work done on the Code of conduct is detailed in the next section

What boxes will the API be implemented in?

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

July 2021. Arcep also encourages implementation of the API in all of their other box models, and in the boxes of operators that are not subject to the Decision.

Can the API be accessed from the Internet?

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

When will the API be available?

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

API DEPLOYMENT SCHEDULE



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:

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

All of the API's specifications that will be discussed and defined by the API supervising committee will be published in the coming months.

3 ACHIEVING 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 conduct⁶ for stakeholders involved in quality of service measurement.

This Code of conduct addresses two aspects in particular: first, requesting that the tools include a clear explanation of their methodological choices when publishing their results, so that any third party can analyse them. Second, establishing best practices that are vital to obtaining reliable results. This approach creates an incentive for stakeholders to satisfy a set of minimum requirements in terms of transparency and robustness, both in their test protocols and in the delivery of their findings.

The 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 work⁷. 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 aggregated publications, including a general commitment to use algorithms designed to exclude erroneous, manipulated or irrelevant results. Moreover, to guarantee statistical representativeness, tools that comply with the Code of conduct commit to publishing the number of tests performed and the factors that are likely to introduce a significant bias when analysing the compared categories.

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.

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

7. 2020 edition of the Code of conduct on internet quality of service: https://www.arcep.fr/uploads/tx_gspublication/code-of-conduct-QoS-Internet-2020_EN_sept2020.pdf

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

3.2 Tools compliant with 2020 edition of the Code of conduct

Arcep published the 2020 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:

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

- **nPerf**, developed by nPerf;
- **DébiTest 60**, the connection tester from *60 Millions de consommateurs* developed by QoS;
- **5GMark**, developed by QoS;
- **Speedtest**, developed by Ookla*;
- 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.

* 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.

Open floor to



JAMES CARROLL

Director of Strategic Initiatives - Ookla



QOS MEASUREMENT TO SERVING CONSUMERS

Our mission at Ookla is to help make the internet better, faster and more accessible for everyone. For over 15 years, Speedtest has helped consumers ensure they're getting what they pay for from their internet service provider (ISP) and mobile network operator. In turn, regulators, providers and operators use Speedtest Intelligence® data to monitor competitors and optimize their own networks for reliability and performance.

Working with Arcep on ensuring we are compliant with their code of conduct has been refreshing for us in Ookla. When our journey began 15 years ago we were focused on helping consumers and end users understand their internet connection and quality. At its heart the Arcep code of conduct is designed to better inform end users to allow them to make clear decisions. We are happy to work with a regulator who shares our passion for consumers and are also excited to see how this relationship can improve consumer education around internet connectivity.

As people and businesses rely more heavily on the internet for education, health and entertainment, access to broadband and mobile internet services doesn't just drive economic growth it also impacts public safety and quality of life. That's why providing universal access to fast, reliable internet service is a key priority for most regulators and governments around the world. Ookla® is fiercely committed to measuring the performance and availability of the internet worldwide and reporting on it transparently.



JANUSZ JEZOWICZ

CEO - SpeedChecker

THE RELEVANCE OF CHARACTERISING USER ENVIRONMENT TO IMPROVE THE RELIABILITY OF QOS MEASUREMENT

We have been following ARCEP's QoS code of conduct for the last few years and fully support the direction of the French regulator. While ARCEP's code of conduct is not compulsory for the QoS tools, compliance with the code gives significant benefits for the vendors: mainly the ability to connect to the Access ID API which will be offered by the operators in France in the coming years.

The Access ID project is an exciting new development in the QoS space which will offer next generation of tools for the consumers that will not only report on the internet speed but will help with troubleshooting. Currently,

customers who test the speed and get a low reading do not understand why. With most customers connecting over wi-fi it is not a surprise that a significant number of low-speed results are associated with poor wi-fi quality. This impacts the users and operators alike in terms of increased support calls and reputation issues.

At SpeedChecker we have been tackling this problem for some time by introducing a wi-fi test built into our mobile apps. Our wi-fi test can identify wi-fi bottlenecks and advise the user to focus on wi-fi improvements instead of complaining to the ISP. Due to technology limitations our wi-fi test

cannot work in the web browser where most of users still test the Internet. The Access ID approach will be usable on any platform, including web browsers, and will offer other accuracy improvements such as detecting other devices' traffic on the LAN, which can heavily influence the test result.

We see Access ID as a significant milestone towards more accurate crowdsourcing methods on fixed networks. Crowdsourcing QoS on mobile networks has been popular already for some time and we hope Access ID will encourage the industry to use this powerful concept for fixed networks as well.

Open floor to



ROXANNE ROBINSON

Director Government and Academia - SamKnows



THE STAKE OF INTERNET QUALITY OF EXPERIENCE MEASUREMENT

SamKnows measures, analyses and visualises internet quality of experience (QoE) and quality of service (QoS) in real time. Our measurement data is used globally in order to help ISPs improve network performance, regulators benchmark ISPs and ensure consumers can make informed decisions about their broadband connections.

QoS data has historically been a focal point for ISPs and regulators when commenting on internet performance but as speeds have increased over the years a change in how consumers use their internet connection is clearly visible. Measurements beyond speed, that look at how real applications

perform, give a more holistic view of performance and can highlight issues that focusing on speed alone can hide. SamKnows offers a huge range of QoE tests that measure the most popular services available to consumers today.

The pandemic has furthered this interest in QoE data. Home has become a place where people use their internet connection to work, educate their children, access healthcare, stay in touch with friends and family and entertain themselves by watching movies or playing online games. Measuring popular video conferencing services or gaming platforms gives real-time data to consumers who can

see how well their internet connection performs.

Analysis of both QoS and QoE data is significantly helped with the presence of contextual “environmental” information. The ARCEP access ID card API provides just that. SamKnows has used similar solutions with other ISPs in the USA and it is effective at providing accurate information. Providing this data alongside QoS tests helps make sense of the measurement results by putting them into context. Adding vital QoE metrics is the next step to giving a truly holistic view of user experience.



JOHN DAVIES

Strategic analyst - Tutela Technologies Ltd.

HELPING OPERATORS UNDERSTAND AND MEET THE GROWING DEMANDS AND EXPECTATIONS OF THEIR SUBSCRIBERS

The usage of mobile networks continues to grow and evolve, as do subscribers' expectations of their mobile operators. Whilst the ability to make a phone call remains important today, many subscribers are more aware of the limitations of networks when trying to join a family video call or when cloud gaming on the bus. In the near future this will evolve to use cases such as mobile augmented reality and synchronised connectivity over a range of consumer IoT¹ devices.

Tutela's goal is to measure networks in real-world conditions – providing data and analysis that enables operators to understand the real experience of subscribers. This spans traditional speed metrics through to how often

a users' network connection is suitable for different applications. The metrics we collect continue to expand to encompass the wide range of subscriber needs.

The foundation of this approach is a testing methodology built around transparency, quality and privacy. This is why Tutela is working closely with Arcep on its code of conduct to achieve our common goals of fair, reflective and robust network testing. Similarly, operators who rely on QoS data to direct their investments need data and analysis which provides high-quality insight into the subscriber experience, that is compliant with privacy regulations.

To give a real world view of performance Tutela collects data in the background while a subscriber is using their device in typical circumstances. This data enables operators to align their investments with subscriber outcomes – for instance, understanding when one aspect of QoS is good enough for current subscriber use cases and where investment will make a greater impact. As 5G welcomes in a new generation of subscriber needs, we look forward to working with organisations like Arcep to continue offering operators actionable insights into real-world network performance.

1. See Lexicon.



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 (speed, latency, etc.) that also includes usage (web browsing, video streaming, etc.) and net neutrality (port blocking, proxy detection, DNS hijacking, etc.) indicators. In early 2020, BEREC made the final changes to the tool's code, which is available on Git Hub: <https://github.com/net-neutrality-tools/nntool>.

This tool is made available to national regulatory authorities (NRA) 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.

The work done on the BEREC tool also served to highlight how important it is to update the QoS measurement

methodology recommended by BEREC in 2017 (BoR (17) 178¹), notably to take the latest technological developments into account, specifically in quality of service measurement indicators, and speed in particular. This update will also draw on the guidelines that BEREC published detailing the quality of service parameters published in 2020 (BoR (20) 53²). A report on the methodology will be published in early 2022, and could help inform the next edition of Arcep's Code of conduct on internet quality of service.

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

1. https://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/methodologies/7295-berec-net-neutrality-regulatory-assessment-methodology
2. https://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/9043-berec-guidelines-detailing-quality-of-service-parameters

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 target's capacity is less than or equal to the capacity of the line being tested.

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

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

The 2020 Code of conduct recommends a minimum capacity of 1 Gbit/s for the test server, to reduce the number of measurements where capacity proves a limiting factor.

4.2 Impact of the test server's location

The test server's location is fundamental for calculating latency, as it depends chiefly on the route the data travel between the customer and the test server¹⁰. 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.

10. In addition to latency tied to the access technology, most of the path between the customer and a server is over optical fibre.

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

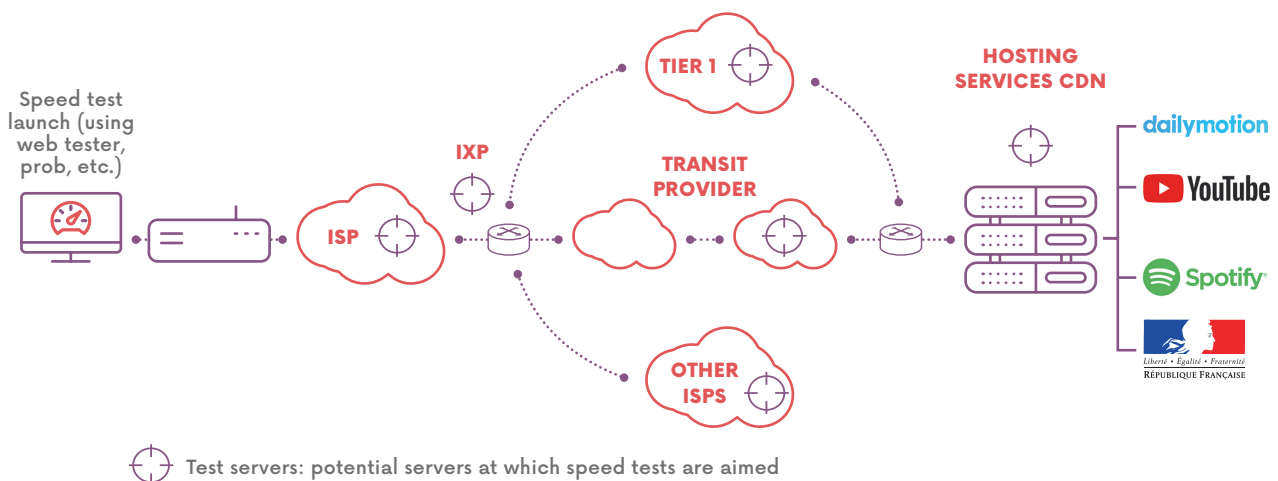
- on the user's ISP's network: the results of the test depend only on the ISP but it is not terribly representative of the actual experience of using Internet services, which are often hosted outside this simple network;
- on another ISP's network directly interconnected (via peering) with the user's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

- on a Tier 1¹¹ network: the tested network extends beyond just the ISP's network performance, and the measurements are even more representative of the actual user experience if the test targets are located at an IXP;
- close to CAPs' servers: the tested network is the one employed end-to-end up to a given web host. The tests are thus very representative of one particular type of use (the Netflix speed index, for instance, only measures the quality of the connection to its own service).

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

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



Source: Arcep

11. Tier 1 networks are the networks that are capable of interconnecting directly with any other Internet network (see lexicon).

EXAMPLES OF BIAS WHEN MEASURING INTERNET QUALITY OF SERVICE

The elements and results presented below serve to illustrate the potential impact of the web browser chosen by the user to perform speed measurements, under a given test configuration. They should only be considered under the chosen test configuration and, in any event:

- do not make it possible to compare the performance of the tested web browsers, but rather aim to underscore the potential bias induced by browsers when running a speed tests;
- are not representative of the quality of service perceived by end users, nor of the actual maximum speed that the browser can support thanks to its internet connection.

The same reservations apply to the other parameters being studied (speed test tools, operating systems, ad blockers, etc.).

On a great number of speed tests running at 1 Gbit/s, the speed limitation is not tied to the operator's network or to the test server being used, but rather to the user's computer. This phenomenon is even more prevalent on 10 Gbit/s connections, where the hardware used by the client performing the test are typically a source of limitation.

The versions of web browsers released in late May 2021 introduced significant changes, notably in terms of performance and design.

The elements set out below are intended to highlight the impact that a browser can have on internet speed tests, by testing the performance of the new versions of the most popular browsers with two of the most widely used multi-host speed tests in France (referred to hereafter as "Tool No. 1" and "Tool No. 2") and to compare the version of these two same tools that are installable on Windows 10 and Ubuntu (hereafter: "Installable Tool No. 1" and "Installable Tool No. 2", respectively).

Established test environment

The PC used to perform the tests detailed here below is an Intel Nuc (mini PC) from 2015¹, equipped with a Celeron N2820 processor, whose performance is limited but representative of millions of entry-level laptop computers (especially in the popular ultraportable segment). The PC has 4 GB of RAM and an SSD hard drive, which is representative of this type of computer used for desktop applications. It is installed with a dual Windows 10 + Ubuntu 18.04 LTS Boot, which are the two operating systems most commonly pre-installed on this type of PC.

To concentrate on the limitations introduced by the client, these tests are performed by connecting the client directly to the test server, using an Ethernet cable. A set latency of 10 ms is added via NetEm².

This configuration creates the ability to eliminate, to a very large degree, potential network-related measurement biases.

Before performing the test, all available updates are installed, and any "maintenance" and "checking for updates" operations that may be running in the background are forced to execute, to avoid them being run during the test, as these background processes can affect the results.

The PC is then restarted and left idle (with browser open) for 10 minutes between each series of tests. The data published are the average of the data collected on 20 speed tests.

1. An Intel Nuc DN2820FYKH is used, with the latest Intel drivers and the most recent BIOS available.

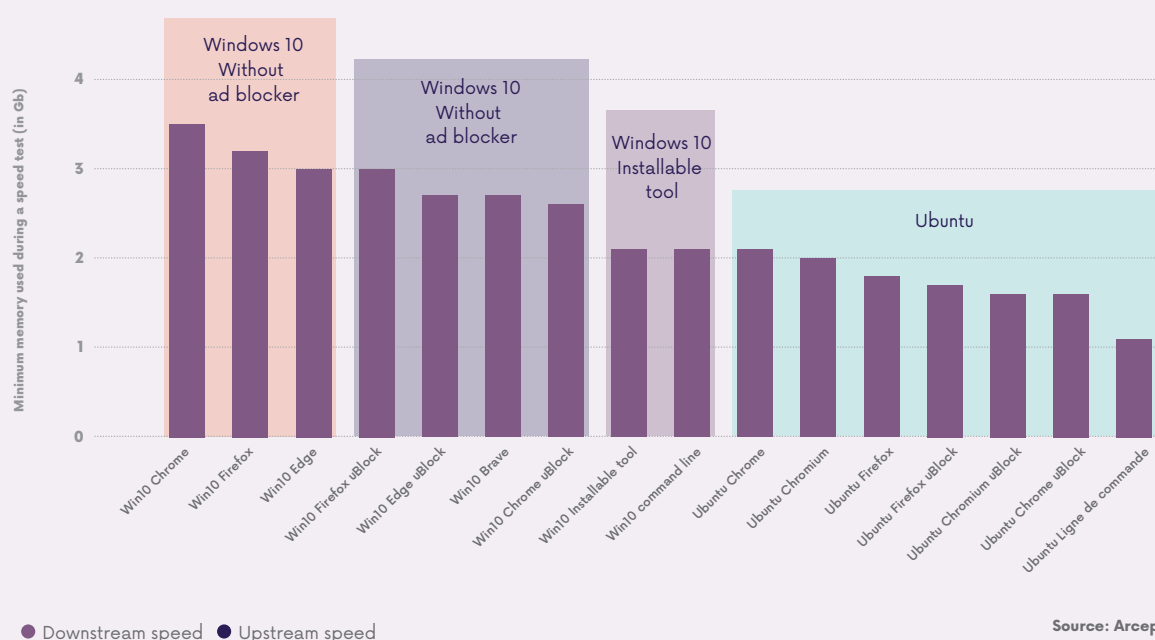
2. The "sudo tc qdisc add dev eth0 root netem delay 10ms" command is used on the server (Ubuntu 20.04 LTS server) to delay each packet sent on the server's 10 Gbit/s network card by 10ms.

The use of random access memory (RAM) during a test can be significant. If there is a shortage of RAM, performances will be diminished since the system calls on available memory space located on the hard drive, which is much slower than RAM.

We have logged the maximum amount of memory used during the speed test. It varies between 1.1 GB and 3.5 GB depending on the browser being used. This includes the

memory used by the operating system⁶. It is therefore important that a user who has a PC with 4 GB of RAM first quit all of their software and close all their browser tabs before running a speed test. Note that, with certain tools, memory use can vary depending on connection speed. 4 GB of RAM may therefore be inadequate to measure a speed of 1 Gbit/s with a web browser running on Windows 10.

MEMORY USED DURING A MULTI-CONNECTION TEST



Measurement Tool No. 2

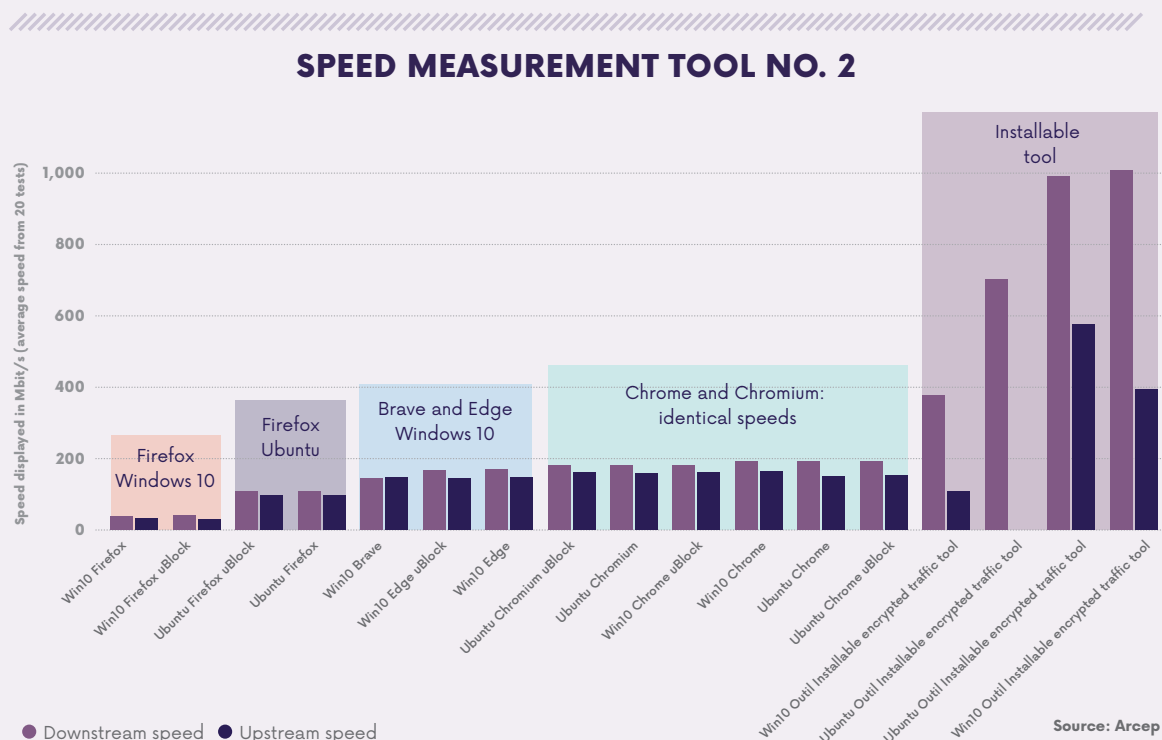
Tool No. 2 does not display any advertising during the speed test. Tests are performed with and without ad blockers, to highlight the potential impact of an ad blocker extension, which must inspect incoming connections to delete any elements on its filter list. The tests reveal that its impact is negligible: without adverts, speeds are not significantly slowed by uBlock.

Unlike Tool No. 1, Tool No. 2 does not offer the option of performing single connection tests. All of the tests are conducted with 16 parallel TCP connections. However, Installable Tool No. 2⁷ offers testing in HTTP and in HTTPS (with traffic systematically encrypted in the web browser).

6. On their own (i.e. with no other apps running) Windows 10 requires 1.9 Gb and Ubuntu 1.0 Gb of memory.

7. Installable Tool No. 2 is in beta testing, with the final version not available in June 2021. Its publisher informed us that the upstream part of the test had not been finalised, and that upstream performances should be improved in the final version.

Below are the results of the different series of tests, ranked by increasing download speed:



The following conclusions can be drawn from these tests:

- Firefox on Windows 10 runs very slowly under test conditions: at less than 40 Mbit/s downstream. Speeds are slightly faster with Ubuntu, but still remain below 108 Mbit/s. This limitation can induce a strong measurement bias.
- Brave⁸ and Edge enable a downstream speed of between 143 and 170 Mbit/s.
- Chrome and Chromium achieve better downstream speeds: between 181 and 192 Mbit/s. All of these nonetheless remain very far from the actual throughput of 1 Gbit/s.
- Installable Tool No. 2 makes it possible to achieve maximum speed when traffic is not encrypted (HTTP): in excess of 992 Mbit/s⁹. When traffic is encrypted (HTTPS), speeds decrease: down to 376 Mbit/s in Windows 10 and 703 Mbit/s in Ubuntu. This is much faster than encrypted traffic on a web browser (192 Mbit/s at best).

Conclusion

To perform a test using a very basic PC or to perform a test at more than 1 Gbit/s, an installable tool is the best choice to achieve the most reliable measurement. N.B. even if the test is more reliable than in a web browser, other biases outside the reach of your ISP can influence speed tests:

- biases tied to software installed on the computer, such as anti-virus, firewalls or VPN, all of which can dramatically deplete a speed test. These biases can be eliminated by using a bootable USB drive within a dedicated environment¹⁰;
- biases tied to operating systems;
- biases tied to the choice of test server (see the section above on this topic);
- biases caused by the local network or network card (Wi-Fi or wireline) of the PC being used. For instance, a 10 Gbit/s network card can be hampered by the link to connects the network card to the processor.

8. The Brave web browser has a native ad blocker, which is enabled by default, which makes it impossible to run the nPerf test. Tests were therefore performed with this ad blocker disabled.

9. This speed is higher than the maximum theoretical speed that can be achieved on a 1 Gbit/s network card, but the installable version is in beta testing. So the final version was not available disponible in June 2021.

10. See Arcep tutorial on "How to create a bootable USB drive to perform a reliable QoS test".

5 Arcep's monitoring of mobile internet quality

If mobile operators' coverage maps – which are produced based on operators' digital simulations and verified by Arcep – provide necessary information on the entire country, they also only give a simplified picture of mobile services' availability. 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.

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 2020, more than a million measurements were taken on 2G, 3G and 4G 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 mon-reseamobile.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 mon-reseamobile.fr since July 2018.

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

5.1 In Metropolitan France, every operator's quality of service continues to improve, albeit at a slightly slower pace

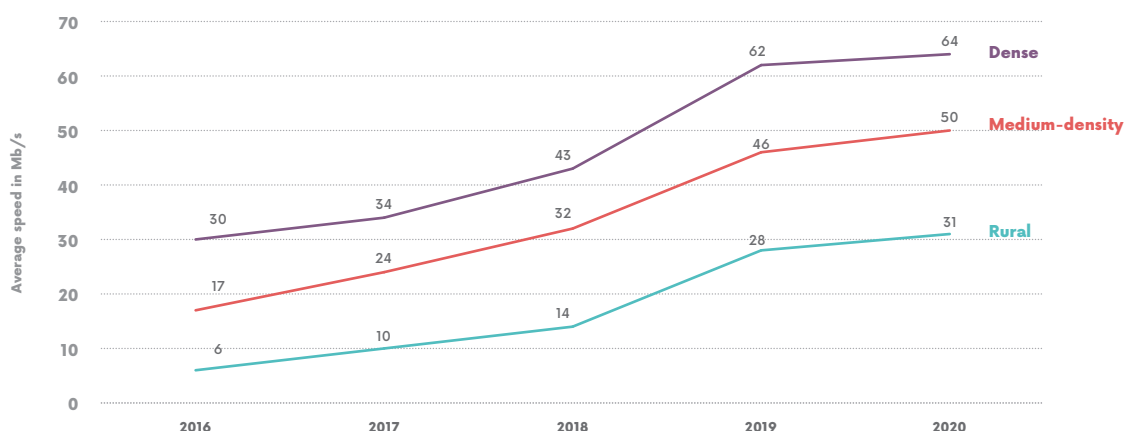
The quality of every operator's mobile internet services continues to improve overall, and this in every type of area: rural, medium density and high density, but at a slower pace than in previous years. This can be attributed to the Covid-19 crisis and to the introduction of stricter measurement protocols, to more accurately reflect the user experience (particularly new configurations for the speed test servers). Downstream speeds thus stand at an average 49 Mbit/s, compared to 45 Mbit/s in 2019.

Also worth noting this year: internet quality of service in metros improved. In 2020, Paris and Lyon joined Toulouse and Rennes on the list of "4G metros" after having completed their subway systems' 4G coverage schemes: in late 2019 for Lyon and June 2020 for Paris.

5.2 Disparities in the progress of internet quality of service in the overseas departments

Certain indicators such as average speed continue to improve, but web browsing and streaming appear to be stagnating, and in some cases have fallen below 2019 levels. This can be explained by the period during which audits were performed (September-December in 2020, instead of July-August in 2019) and to the impact of the Covid crisis, which put an added strain on the networks.

PROGRESSION IN AVERAGE DOWNLOAD SPEEDS, BY TYPE OF AREA



Source: Arcep

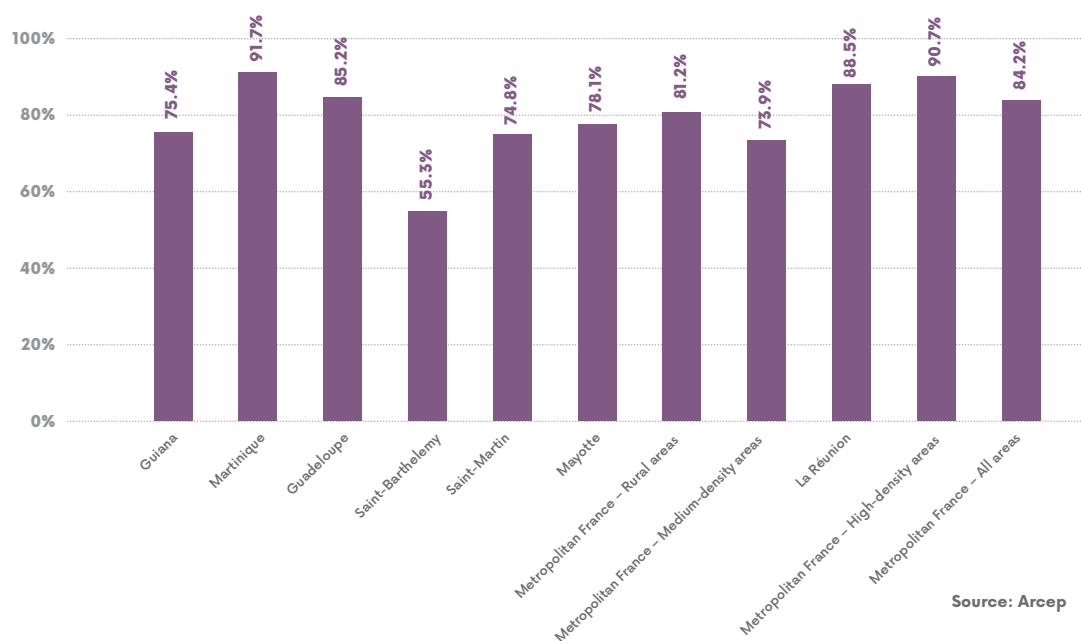


A new indicator for the Arcep campaign, in Metropolitan France and overseas: percentage of tests that exceed 3 Mbit/s

The indicator that displays *average speed* is an interesting piece of information, but illustrates only one aspect of quality of service. For instance, an operator that provides very limited coverage but very fast connections to those users who are covered may have a similar average speed indicator as an operator that provides very broad coverage, but at lower speeds. The quality of the user experience will therefore differ between these two operators.

To complete the information provided by average speeds, in 2020 Arcep introduced a new indicator: *percentage of connection speeds above the minimum threshold*. In the findings of this audit, this threshold is set at 3 Mbit/s as, in most cases, a connection of more than 3 Mbit/s is enough to sustain “standard” mobile internet use, such as web browsing, reading e-mails and watching most videos in 720p without any significant slowing.

PERCENTAGE OF TEST WITH A DOWNLOAD SPEED ≥ 3 MBIT/S



5.3 Improving “Mon réseau mobile”

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

It began by publishing a “regulator’s toolkit” to address the needs of local authorities wanting to perform their own measurements, particularly to identify coverage needs under the New Deal for Mobile. The 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. A number of pioneering entities have already employed this document to conduct their own local connectivity measurements, including national railway company, SNCF, and several local authorities. Arcep has been engaged in an ongoing dialogue with these players and, since April 2020, “Mon réseau mobile” has been further enhanced by the measurements obtained by different regions: Cher, Hauts-de-France, Pays-de-la-Loire and Auvergne-Rhône-Alpes. These data were updated in March 2021, alongside the addition of data to

“Mon réseau mobile” from private sector player, QoSi – Mozark Group, which shared the results of its own self-funded measurement campaign with Arcep. The tool will continue to become more information-rich by incorporating mobile QoS measurements that have been performed in compliance with the “regulator’s toolkit”.

Arcep has also published a “Code of conduct” for players who provide apps for testing the quality of users’ mobile experience, such as crowdsourced app-based tests that anyone can perform on their mobile phone. The goal is to ensure a minimum set of requirements in terms of the relevance, presentation and transparency of the test results. To date, five players have declared themselves compliant with the 2020 version of the Code of conduct (5GMark (QoSi), nPerf, 60 Millions de consommateurs, Speedtest by Ookla and Tutela). The solutions they provide have been adopted by several regions such as Hauts-de-France and Ile-et-Vilaine.



J’alerte l’Arcep

Launched in October 2017, the “J’alerte l’Arcep” platform is available to any citizen wanting to report an actual problem encountered with their mobile Internet, fixed Internet or postal services. In 2020, Arcep produced a scorecard of its pro-consumer actions and its “J’alerte l’Arcep”^{*} reporting platform. The Authority received more than 33,000 reports in 2020. Of these, 40% concerned quality and availability issues with fixed or mobile services.

These reports provide valuable feedback for Arcep’s diagnostic capabilities. They help make it possible to quantify and identify the problems that users are encountering, to then steer Arcep’s actions towards the most appropriate solutions possible. User reports also help Arcep departments identify possible violations of its open Internet and net neutrality policies (cf. Chapter 4).

The platform was also employed during the Covid-19 crisis, notably to forward alerts to operators that had

been flagged as top priority (from medical or paramedical workers and institutions, local authorities, government agencies). Some 50 alerts from these entities were forwarded. Operators handled each one individually.

Arcep launched a new version of its “J’alerte l’Arcep” reporting platform in November 2020, using three years of hindsight and scorecards to improve the quality of the user experience and process alerts more efficiently. The platform is opening up to new groups of users who will be able to alert the regulator (print media distribution sector, app developers, telecom operators and consumer associations). The user pathway for filing a report was also made more fluid and accessible to people with disabilities. Other data-driven regulation tools developed by Arcep are also set to be integrated

(Mon réseau mobile, Carte fibre, Ma connexion internet and Wehe). And, lastly, Arcep’s data processing was revised to make it more efficient.

^{*} 2020 scorecard of Arcep’s pro-consumer actions, and of the “J’alerte l’Arcep” platform: <https://en.arcep.fr/news/press-releases/view/n/data-driven-regulation-031120.html>

Tutorial



HOW TO IMPROVE THE QUALITY OF YOUR WI-FI CONNECTION

The two most common solutions for connecting a computer to an ISP's box (router) are Wi-Fi and a direct connection via Ethernet cable. The Ethernet cable, plugged into the box – possibly using the wired Ethernet pre-installed in new or renovated housing – is the recommended solution whenever possible. Direct Ethernet access typically provides more stable access, faster speeds and leaves Wi-Fi spectrum free for devices that need it. Fewer and fewer laptop computers have an Ethernet port, although USB adapters are available to connect PCs that do not have one. 1 Gbit/s Ethernet is standard today, but we are starting to see 2.5 Gbit/s Ethernet in new products and some boxes are already compatible with it.

FIVE TIPS FOR GETTING A BETTER WI-FI SIGNAL

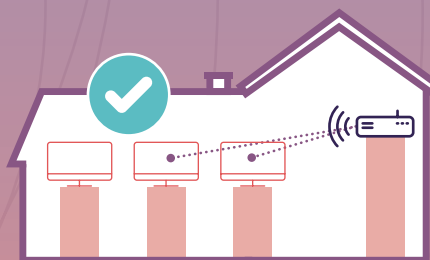
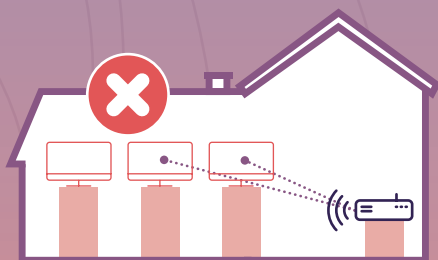
01. Place the box in a central room in the home

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



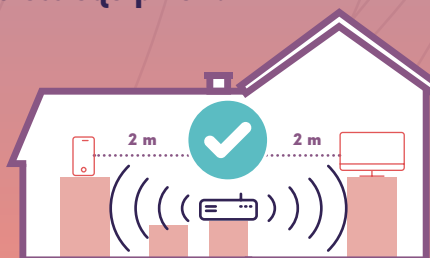
02. Place the box in the most open location possible

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



03. Keep the box far away from other wireless equipment

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

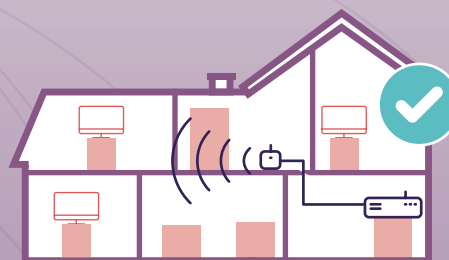
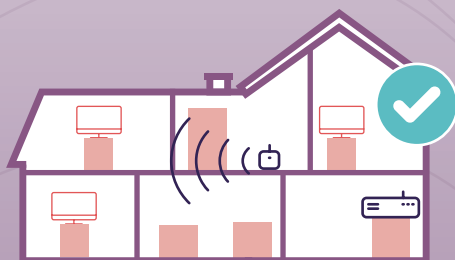
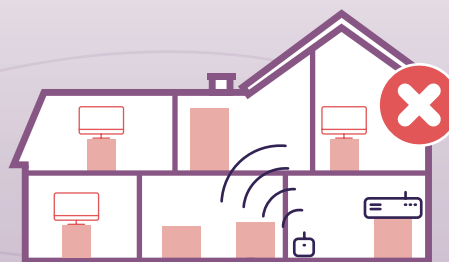


04. Use a Wi-Fi repeater

If the internet connection is slow in certain rooms that are far from the box, a Wi-Fi repeater or extender is recommended to extend the Wi-Fi coverage.

For it to work, the Wi-Fi repeater must be placed mid-way between your box and the area of the home to be covered. If it is too close to the box, it will not extend your Wi-Fi signal. If it is too far, it will have trouble capturing your box's Wi-Fi, and the repeated speed will be slow.

To achieve the fastest connection, it is best to connect the Wi-Fi repeaters with a long cable running to the box: the Ethernet cable can carry the signal up to a maximum 100 metres, without any speed loss.



05. When buying a new computer, check that it is compatible with Wi-Fi 6 (802.11ax) or the latest Wi-Fi 6E standard

It is recommended to choose computers that are compatible with the Wi-Fi 6 (802.11ax) or the Wi-Fi 6E standard. This standard is more powerful than its predecessors, as it increases speed and decreases latency. Added to which, it is backwards compatible with all of the older standards, including Wi-Fi 5 (802.11ac) and Wi-Fi 4 (802.11n).

Wi-Fi 6E is a Wi-Fi 6 standard that adds compatibility with the 6 GHz frequency bands, divided into three super-wide 160 MHz channels, to deliver faster speeds and free up lower frequencies for incompatible equipment.

SHOULD I USE WI-FI OR MY MOBILE OPERATOR'S 4G/5G NETWORK WHEN I'M AT HOME?

Wi-Fi offers users a number of advantages, and is among the best practices for curtailing the digital environmental impact:

- Typically faster and more steady speeds than 4G, provided the box delivers superfast access and powerful Wi-Fi (Wi-Fi 5 or Wi-Fi 6). Latency, i.e. the time it takes the signal to travel to the server, is also shorter over FttH than with 4G or even 5G.
- There are generally no data caps on fixed access boxes, whereas virtually every mobile plan carries "fair use" provisos, expressed in an allowance of x number of GB of traffic, beyond which users are either billed for the extra traffic or their connection is slowed.
- Lighter use of the device's battery: Wi-Fi consumes less energy than using the mobile network does. Putting less strain on the battery means a longer lifespan for your device.
- Lower energy consumption on the operator's network:
 - Power consumption on a wireline network depends very little on how that network is being used: 1.8W per line, per year for ADSL and 0.5W per FttH line per year, on the operator's network side of the equation¹.
 - On cellular networks, energy consumption depends much more heavily on usage, i.e. around 600 Wh per GB used¹.
- It is also an act of solidarity to switch over to Wi-Fi, to reduce the saturation level in certain mobile cells, and so reducing the risk of diminishing the connection quality of fellow cell users, who have no other connection option.

1. Source: Arcep brief "Digital tech's carbon footprint" – 21 October 2019.

SUPERVISING DATA INTERCONNECTION

What you need to know

Inbound traffic to the main ISPs in France increased by more than

50%

in a single year, to reach

27.7 Tbit/s

at the end of 2020.

Traffic coming from the main French ISPs' on-net CDNs increased by

82%

in a single year, to reach

7.1 Tbit/s

at the end of 2020.

50%

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

Interconnection¹ is the cornerstone of the Internet. It refers to the technical-economic relationship that is established between different actors to connect and exchange traffic. It guarantees a global network mesh and enables end users to communicate with one another other².

1 Datacentres' role in data interconnection

A datacentre is an installation that houses a large number of connected computers that work together to process, store and share data. Internet service providers (ISPs), content delivery networks (CDNs), internet exchange points (IXPs), transit providers, hosting services, content and application providers (CAPs), as well as businesses rely heavily on datacentres, which constitute one of the central components in the supply of online services. As a result, datacentres have taken hold as essential players in the digital landscape in general, and the internet ecosystem in particular.

In addition, the number of datacentres in France has continued to grow over the past several years, chiefly around its largest cities, such as Paris and Marseille. Today, we are seeing a decentralisation trend in France, particularly as part of the ongoing digitisation of SMEs and local authorities, and the potential uses of the internet being opened up by 5G³.

The key considerations in a datacentre's design and operation include:

- Safety and security: guaranteeing physical security and safety, access control, redundant/backup infrastructure, and protection against natural phenomena (lightning and flooding);
- Energy: guaranteeing an uninterrupted power supply;
- Management of environmental factors: providing the right balance between cooling, regulating humidity levels and airflow regulation;
- Interconnection: providing the ability to connect to networks securely, with a sufficient network capacity.

1. Definitions of the technical terms related to interconnection that are employed here can be found in the Barometer of data interconnection in France: <https://www.arcep.fr/cartes-et-donnees/nos-publications-chiffrees/linterconnexion-de-donnees/barometre-de-linterconnexion-de-donnees-en-france.html>

2. N.B. this report refers only to data interconnection on the internet network, and does not address the interconnection of two operators' networks for the purposes of voice call termination.

3. Map of colocation datacentres in France: <https://www.datacentermap.com/france/map.html>

There are several categories of datacentres, with different sizes, locations and business models.

A datacentre is said to be neutral or carrier-neutral if it provides the ability to contract one's provider of choice to supply internet connections. Some datacentres, on the other hand, include internet access in their solution (e.g. some transit providers' datacentres).

Datacentres have two main, separate roles: hosting and interconnection. Interconnection (or central) datacentres such as Telehouse TH2, Equinix PA2/PA3, Interxion Marseille, Netcenter SFR in Lyon, Netcenter SFR in Courbevoie and Interxion PAR2, play a central role in interconnecting different players. Veritable hubs, or crossroads, between the different internet and digital players, they concentrate many members and give service providers and users the ability to interconnect, whether through public peering at an IXP, private peering or transit, depending on the players'

business choices⁴. Providing a range of services (*colocation*⁵, cross-connect⁶, internet exchange point, etc.), these datacentres promote the supply of direct interconnection to their clientele, delivering the ability to relay traffic between these players without going through the internet or other networks.

As usages and behaviours evolve, with businesses' digital transformation and the emergence of new technologies, datacentres' have an increasingly crucial role to play, to optimise interconnection and improve quality of service for end users.

In light of these stakeholders' growing importance for electronic communications networks and services, in 2021 Arcep will conduct a study of the services that datacentres market to operators, in order to identify possible best practices or, on the contrary, points that warrant closer attention.



4. Cf. Interconnection for Dummies, Stéphane Bortzmeyer (in French): https://www.arcep.fr/fileadmin/reprise/observatoire/ipv6/2018-06_Interco_Pour_Les_Nuls_Bortzmeyer.pdf

5. Leasing a private or shared room in a datacentre to house computer equipment.

6. Direct connectivity options (optical fibre, coaxial cable or UTP/STP) between members.

Open floor to



SAMI SLIM

Deputy Director - Telehouse

INTERCONNECTION: A SOURCE OF STRENGTH FOR FRANCE AND ITS TERRITORIES

There is a good reason that some datacentres are called the network core. They are the vital organs to a country's digital health. They are the guarantors of its independence, of the diversity and vitality of its players, and of its weight on the international stage. Telehouse's history proves it.

Telehouse was the first company in the world to create a carrier-neutral datacentre (carrier hotel) during the wave of telecoms unbundling in the 1980s. Which put new entrants on an equal footing. Regional, national and international telcos were thus able to interconnect under the same conditions, with the same quality of service.

The datacentre then naturally became a marketplace. It created the ability to deploy denser and more secure connectivity between the players. To the point that TH2 became the most interconnected datacentre in France, and number four worldwide.

Beyond this point of pride, the issues at stake are also vital to France, namely strengthening its digital sovereignty. A global scale datacentre makes it possible to capture international traffic and to relocate to the interconnections relaying our data onto our own soil.

Added to which the legacy optical fibre architecture that runs through the whole of France, from Paris on out, notably via railway lines and motorways, automatically enables rural areas to benefit from the capital's connectivity, and continues to reduce the digital divide between Paris and the rest of the country.

And this goes both ways: the regions also feed the capital. Several cities in France provide Paris with a window on the world: Marseille onto Africa and the Middle East, Bordeaux to the Americas, Lyon to Eastern Europe and Lille to the Nordic nations. These metropolises are tremendous geographical assets that will make France a global digital crossroads.

THE MOST CONNECTED CITIES AND DATACENTRES IN THE WORLD IN 2020



CITY

International interconnection capacity (Gbit/s)*

1	Frankfurt, Germany 110,608
2	Londres, U.K. 74,834
3	Amsterdam, Netherlands 71,188
4	Paris, France 67,865
5	Singapore, Singapore 56,350

* Excl. domestic capacity



DATACENTER

Number of peers**

1	Telehouse London (Dockland) 821
2	Interxion Frankfurt (FRA1-14) 446
3	Equinix FR5 (Frankfurt, KleyerStrasse) 335
4	Telehouse Paris 2 (Voltaire) 282
5	Equinix Slough 224

** Source: Peering DB

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 2020. For confidentiality reasons, the published findings⁷ are aggregated results only of the main ISPs in France (Bouygues Telecom, Free, Orange, SFR).

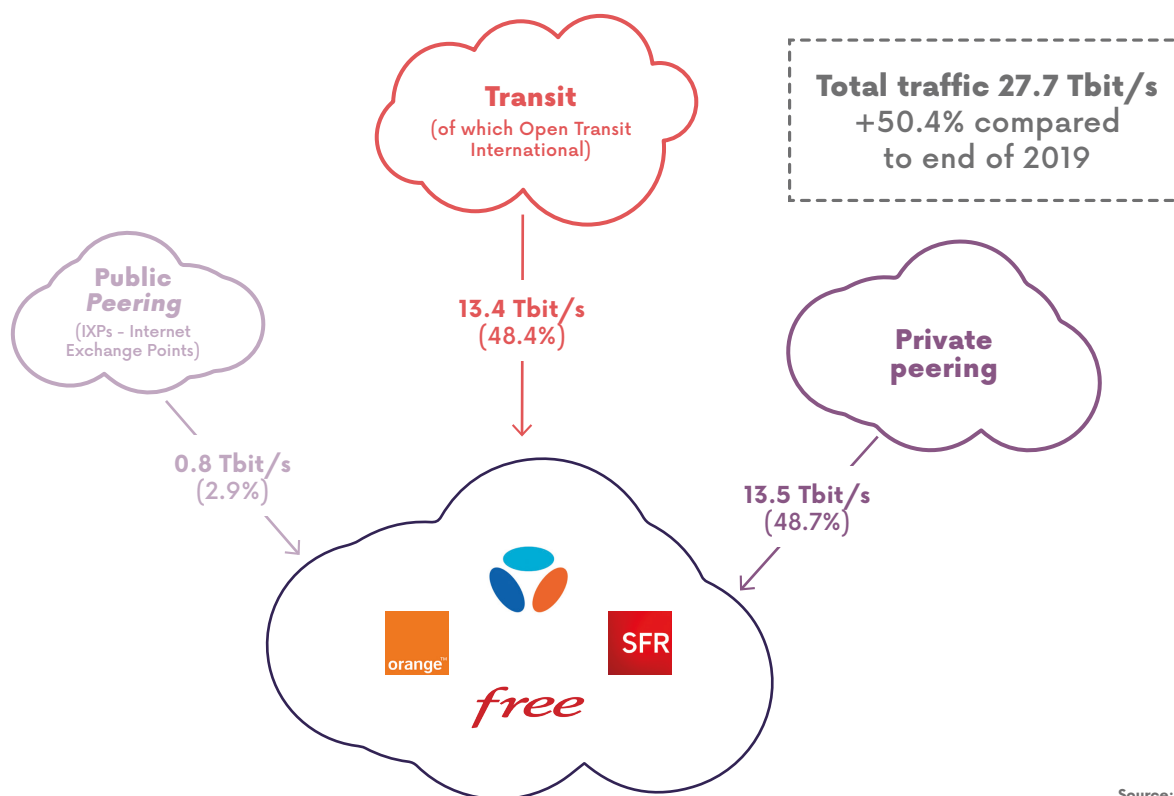
2.1 Inbound traffic

Inbound traffic to the four main ISPs in France increased from more than 18.4 Tbit/s at the end of 2019 to 27.7 Tbit/s at the end of 2020, which translates into more than 50% increase in a

single year (compared to 29% between 2018 and 2019). 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.

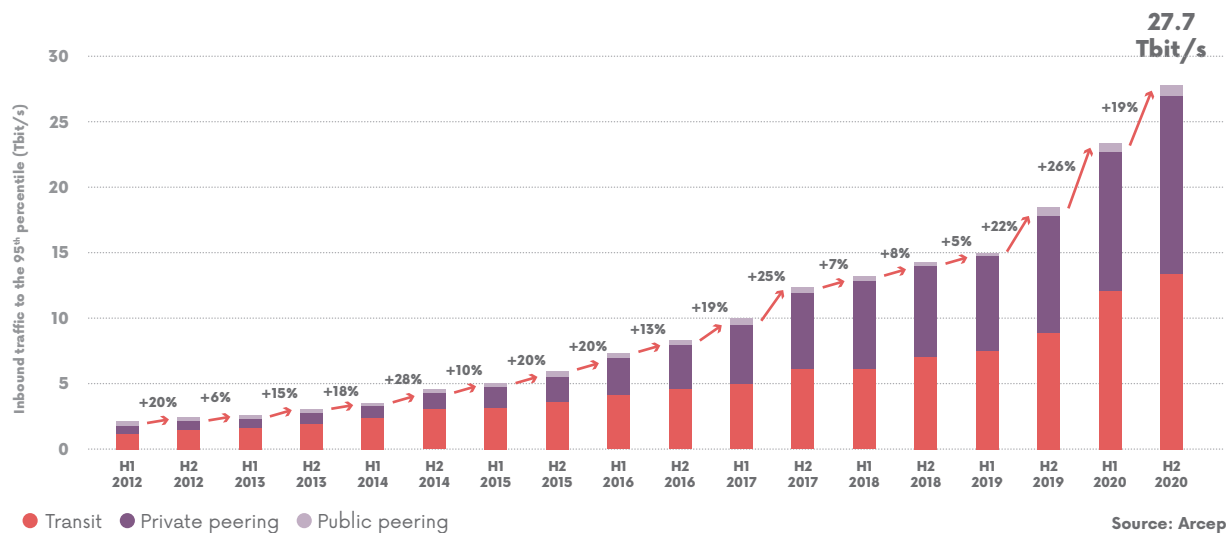
There was a significant increase in traffic (+ 26%) in the first half of 2020, which could, in part, reflect the increase in usage during the first lockdown in France.

BREAKDOWN OF INBOUND TRAFFIC (95TH PERCENTILE) ON THE NETWORKS OF THE MAIN ISPs IN FRANCE (END OF 2020)



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

INBOUND TRAFFIC TO THE MAIN ISPs IN FRANCE, FROM H1-2012 TO H2-2020



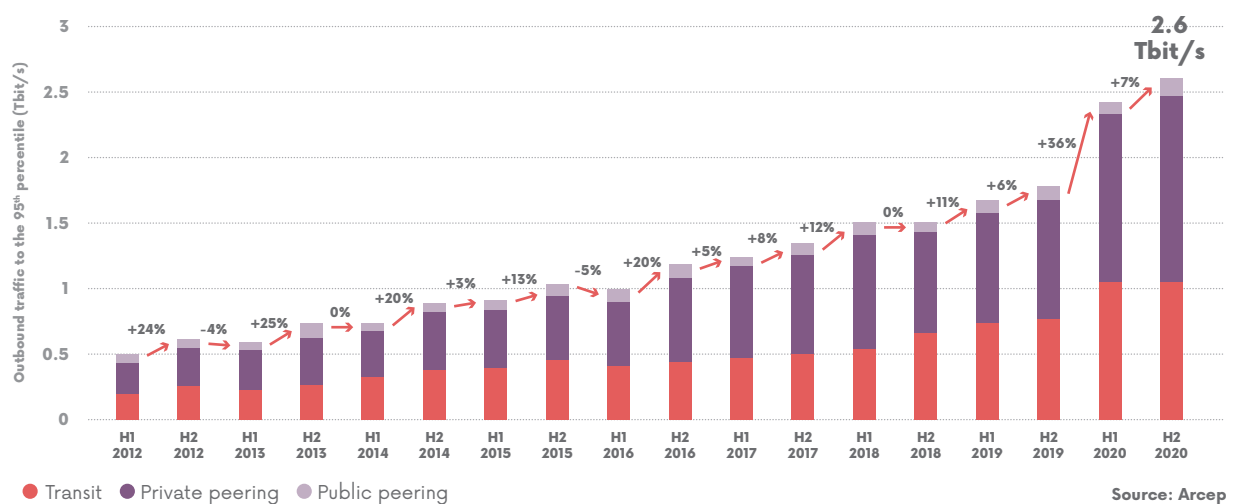
2.2 Outbound traffic

By the end of 2020, outbound traffic on the networks of France's four main ISPs stood at around 2.6 Tbit/s, or 46% more than at the end of 2019. This traffic quintupled between 2012 and 2020.

There is a particularly marked increase between the second half of 2019 and the first half of 2020, which could be linked to the start of the Covid-19 crisis and the lockdown in spring 2020.

42

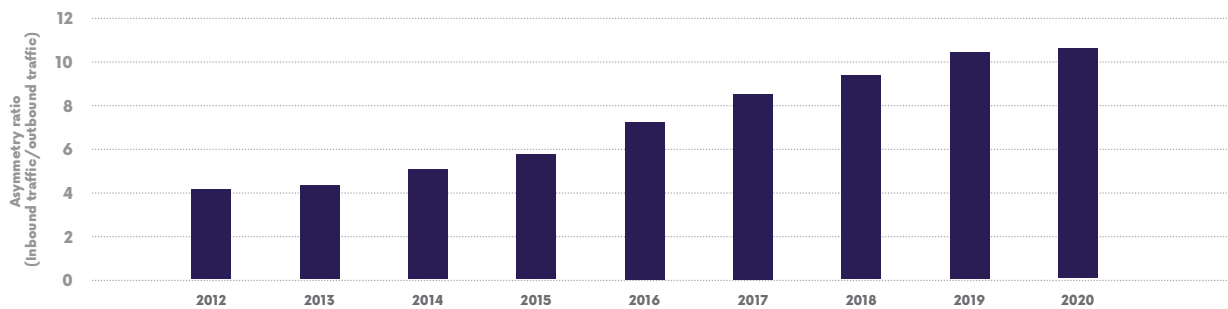
OUTBOUND TRAFFIC FROM THE MAIN ISPs IN FRANCE, FROM H1-2012 TO H2-2020



Outbound traffic is well below incoming traffic. Moreover, the asymmetry between the two has increased from a ratio of 1:4 in 2012 to one of more than 1:10 in 2020. This widening gap is

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

ASYMMETRY RATIO BETWEEN INBOUND AND OUTBOUND TRAFFIC AT INTERCONNECTION LEVEL FOR THE MAIN ISPs IN FRANCE BETWEEN 2012 AND 2020



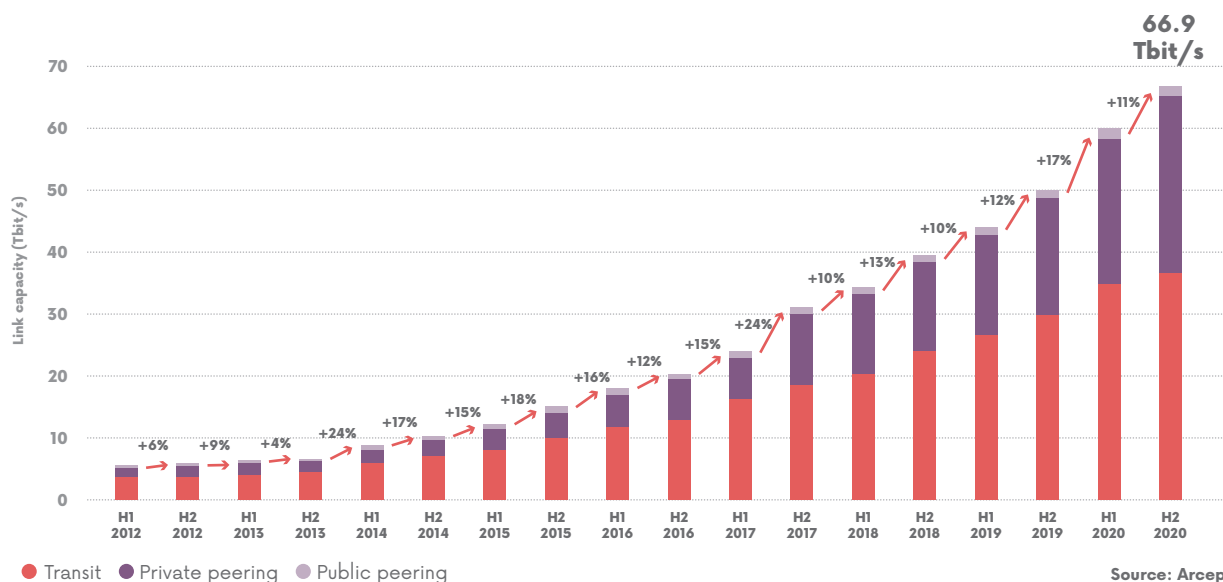
Source: Arcep

2.3 Evolution of installed capacities

Installed interconnection capacities have increased at the same pace as inbound traffic. Installed capacity at the end of 2020 is estimated at 66.9 Tbit/s, or 2.4 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 H2-2020



Source: Arcep

2.4 Evolution of interconnection methods

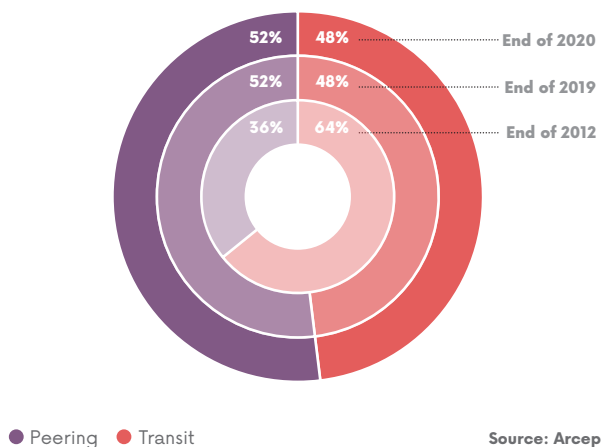
Peering vs. Transit

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 2019 and the end of 2020, a concomitant increase in transit and peering (private and public) was observed. The respective shares of peering (52%) and transit (48%) have not changed. This situation is mainly due to the substitution of part of the peering traffic with traffic coming from on-net CDNs.

EVOLUTION OF PEERING AND TRANSIT FOR THE MAIN ISPs IN FRANCE

(in proportion of inbound traffic volume)

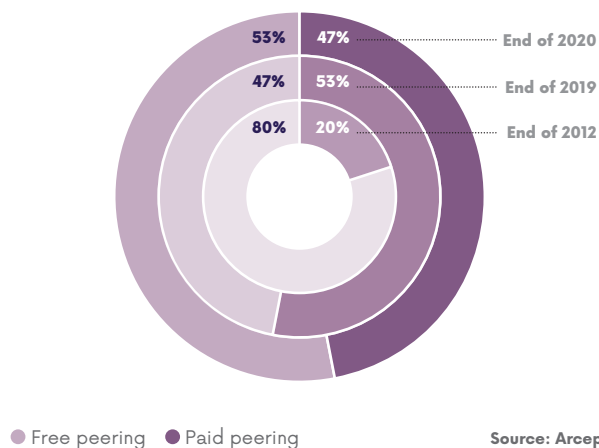


Free vs. paid peering

Contrary to the trend observed for several years, the share of paid peering decreased from 53% at the end of 2019 to 47% at the end of 2020. This situation 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)

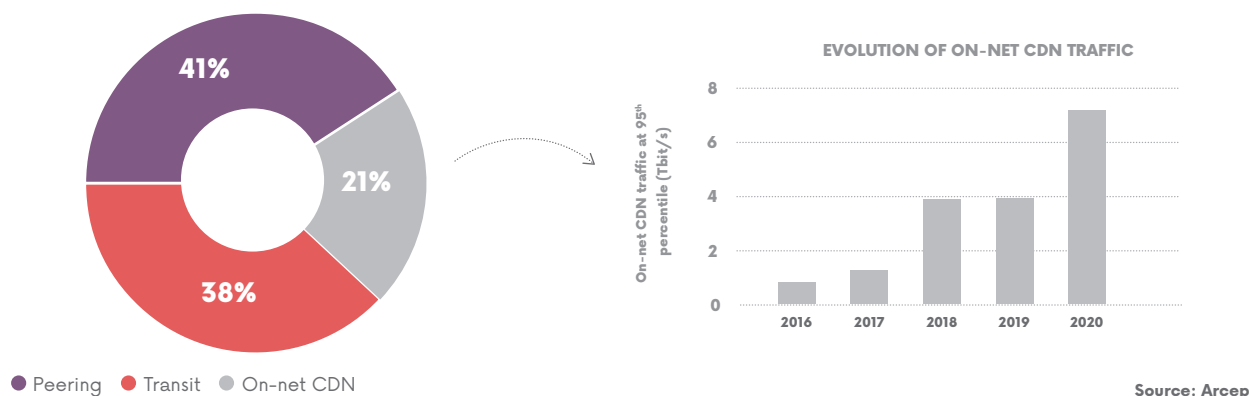


2.5 Traffic breakdown by interconnection type

Between the end of 2019 and the end of 2020, traffic coming from on-net CDNs the top four ISPs' customers almost doubled (+ 82%) to reach around 7.1 Tbit/s. The percentage of traffic from on-net CDNs (21%) also increased compared to last year (17%). This increase could be explained by the modification of uses during the Covid-19 crisis, in particular the increased consumption of video on demand services, which mainly use on-net CDNs in the different ISPs' networks.

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 40% of the inbound traffic being injected into their networks. In addition, the ratio of inbound to outbound traffic ranges from 1:5 and 1:11 depending on the operator. In other words, data made available through on-net CDNs are viewed between five and eleven times, on average.

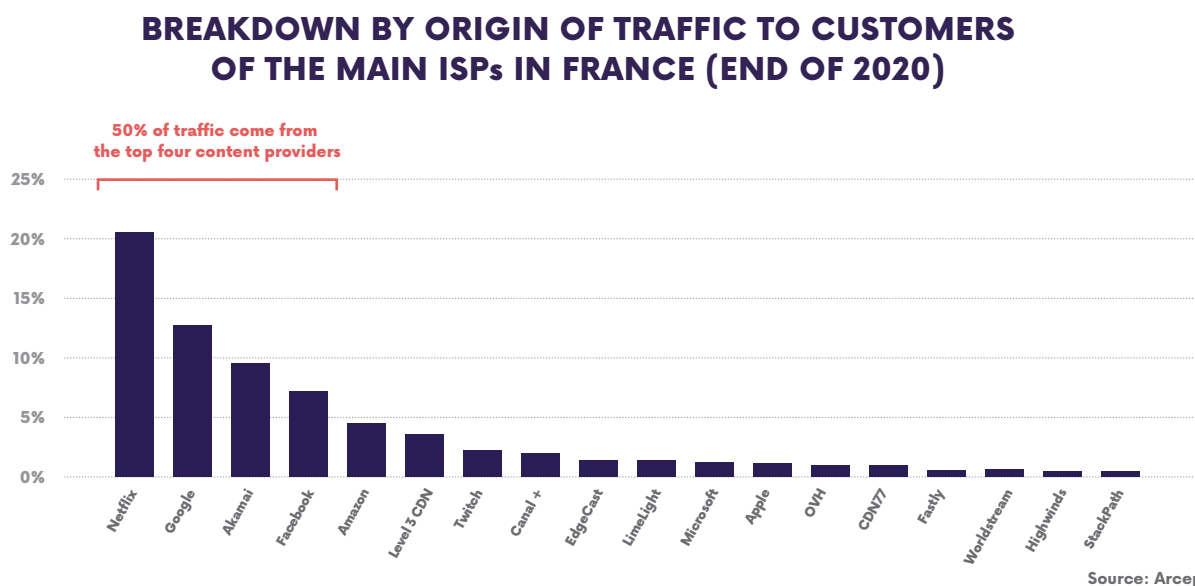
BREAKDOWN BY INTERCONNECTION TYPE OF TRAFFIC TO CUSTOMERS OF THE MAIN ISPs IN FRANCE (END OF 2020)



2.6 Traffic breakdown by origin

50% of all traffic to the customers of France's main ISPs comes from four providers: Netflix, Google, Akamai and Facebook. This testifies to the increasingly clear concentration of traffic around a small number of players, whose position in the content market is more and more entrenched. Added to which, the gap in the volume of traffic coming from Netflix compared to other service providers is actually widening.

The presence of several CDNs in the traffic breakdown presented below confirms the important role of these actors in the routing of internet traffic. For example, Disney + appears in this ranking through its various CDNs.



2.7 Evolution of costs

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

VAT) per month and per Mbit/s⁸.

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.

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

Open floor to



RAPHAËL NICOUD

President - Aqua Ray

AQUA RAY TALKS ABOUT OBTAINING TIER IV CERTIFICATION FOR ITS DATACENTRE

Aqua Ray renovated its Aurora datacentre in Ivry-sur-Seine. The project was successfully completed in January 2021 with the award of Tier IV certification by the Uptime Institute. Aqua Ray's Aurora datacentre is currently the only one in the Greater Paris region to be certified Tier IV.

WHAT IS TIER IV?

The Uptime Institute is an American company that developed what became a globally-recognised system which categorises datacentres by four levels of reliability.

This classification focuses on two main areas tied of datacentres' operation: electrical power and cooling the equipment they house.

If your datacentre is Tier I or Tier II, it means that it has to be shut down to perform maintenance on certain equipment.

From Tier III on up, planned maintenance work can be done on any link in the chain without interrupting operations.

Tier IV indicates that the datacentre is designed to handle virtually any incident or failure without affecting production.

So, a fire breaking out in a room with a UPS system, that suddenly destroys a converter or a battery bank, should not affect a Tier IV datacentre's operation, which is not necessarily true of a Tier III datacentre which may not have been designed for it.

TIER IV ELECTRICAL POWER

It is a common misconception: a site does not need to have a dual power supply from the public electricity network for a datacentre to obtain Tier IV certification. In fact, as paradoxical as it may seem, it does not even need to be connected to the grid at all.

What the Uptime Institute will verify, however, is your ability to ensure autonomous electricity production on-site, and which is capable of meeting 105% of the site's energy needs under the worst-case scenarios: maximum load, extreme weather and a broken-down generator, for instance.

No single technology has been imposed, and no particular technique is required, as long as your design creates the ability to meet the fault tolerance requirements. But the Uptime Institute will, for instance, check that every power cord is the right size, and that every cable can be cut without affecting operations.

At Aqua Ray, we opted for a very simple installation based on a 2N configuration of diesel generators: every power supply infrastructure is independent from the other (including the fuel tanks) and each is capable of satisfying 105% of the site's energy needs.

TIER IV DATACENTRE COOLING

Here again, no particular technique is imposed, provided you can demonstrate that the equipment housed in your datacentre will always be in a thermal environment that complies with ASHRAE guidelines (room temperature of between 18 and 27 degrees).

Unlike Tier III, Tier IV carries an additional requirement of continuous cooling. When an incident or maintenance occurs, there can be no interruption of the air conditioning system.

Designing a redundant, Tier IV-compatible chilled water system, including across the multiple valves, is both complex and costly. At Aqua Ray, we opted for a direct expansion system. Our 2N-formation air conditioning blocks are connected electrically to the "high quality" network, in other words behind the converters, which is not the classic configuration. This enabled us to meet the continuous cooling requirement.

OTHER WATCH-POINTS

The dual supply (redundant) network, the fire-resistant partitioning and the automated site surveillance/monitoring strategy are also part of the requirements. Even though the classification is a measure of service reliability and not, for instance, of safety levels. Access control and intrusion detection techniques, for example are not addressed. This is why, when we choose a datacentre, we should pay attention to these issues as well, in addition to the Tier III or Tier IV criteria, e.g. by checking that installations are ISO 27000 standards-compliant.

Open floor to



FRANCK SIMON

President - France IX Services

FRANCE-IX, MULTI-SERVICE REFERENCE PLATFORM A LEADER IN INTERCONNECTION IN FRANCE

THE ROLE OF FRANCE-IX IN PROVIDING INTERCONNECTION IN FRANCE, AND THE MERGER OF FRANCE-IX AND REZPOLE

When it was founded in 2010, France-IX was focused on building a neutral and independent structure, providing a high-quality service at a fair price, in line with the market, to attract international networks and to make it one of Europe's major interconnection hubs.

In 2020, France-IX reached maturity, with more than 450 connected networks (via its points of presence in Paris and Marseille) and a traffic level exceeding a Terabit per second. At the same time, competition between the main internet exchange points has increased: as a result, the time had come to rethink the France-IX strategy and to consolidate what made it special, namely the platform of reference for accessing French and French-language content and players.

Even if France-IX can rely on a network of operator resellers to cover sites where we are not physically present, it was important to increase the density of our national footprint.

To strengthen its position as the leading multi-service platform in France, the merger with Rezopole took hold as a natural choice, as the two structures shared the same associative DNA, and Rezopole managed to create the largest body of regional internet exchange points in France, in addition to its proven expertise in supplying

value-added services for its members. The France-IX product range was thus expanded, notably those aimed at businesses, while also covering a broader geographical area – our target being to cover two additional cities a year over the next three years.

HOW THE FIRST LOCKDOWN AFFECTED INFRASTRUCTURES

Managing the first lockdown was complex affair, as much in terms of ensuring continuity of operations, as business development. From the very first announcements hinting at an upcoming stay-at-home order, we began to prepare by preinstalling many 10 Gbit/s and 100 Gbit/s ports on all of our sites, which was what enabled us to process requests throughout the lockdown, despite the restricted access we had in many datacentres. That said, the traffic increase experienced by some was offset by a decrease in traffic for others during this period, and the traffic that stagnated from January to June 2020 did not really begin to climb until late summer, then continued to rise steadily up to December 2020.

FUTURE CHALLENGES FOR FRANCE-IX

In addition to expanding its geographical footprint, and the ability to provide its members with a highly interconnected platform (via gateways between cities), France-IX will also be developing its range of services: public

peering will be completed by private peering solutions, not least because a large percentage of exchanges employ this type of solution.

It is also important to continue to educate businesses on why they need to connect to platforms such as ours to support them in their digital transformations, through tailored training sessions.

Hosting solutions on-demand, provided in partnership with datacentres, to satisfy requests from international players wanting a one-stop solution, will also be possible.

We are working on redesigning our marketplace, as we have quite a lot of room to grow. Our resellers programme will also be reviewed, working with them to provide better training on our products and services, especially as resellers are demanding that resource ordering and delivery processes be automated (automatic circuit configuration) by incorporating APIs.

There are multiple challenges ahead for France-IX, all bound up with the necessary transformation of interconnection platforms: those that do not plan on diversifying their product line, or form partnerships with other structures to consolidate their positions will likely lose ground. The market is evolving, and exchange points are no longer structures dedicated solely to operators and content providers, even if they do remain the key players.

ACCELERATING THE TRANSITION TO IPv6

What you need to know

105
participants

on the IPv6 task force
co-chaired by Arcep
and Internet Society
France: join
the task force!



Operators that were awarded
5G frequencies must make their
mobile networks compatible
with IPv6 by

**31 December
2020.**

The rate of IPv6 use is increasing
in France, reaching

more than **42%**

in December 2020.

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 IPv4¹.

1 Phasing out IPv4: the imperative transition to IPv6

IPv4, which has been used since 1983, provides an addressing scheme of close to 4.3 billion addresses². 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)³ had already allocated between around 92% and 95% of their IPv4 addresses⁴.

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 surface⁵.

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 2020 the process was still only in the early part of the cohabitation stage⁶.

In the 2019 edition of its report on the state of the Internet in France, Arcep estimated that the stock of IPv4 addresses would be exhausted by the end of Q2 2020, but the pace at which the last remaining blocks of IPv4 addresses were acquired accelerated, and IPv4 addresses had in fact run out by the end of that year. 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 from the last remaining IPv4 addresses in their pool.

1. In some instances, particularly on mobile networks, IPv6 is deployed instead of IPv4, in which case protocol translation mechanisms are put into place on the network (NAT64 and DNS64) and on devices (464XLAT).

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

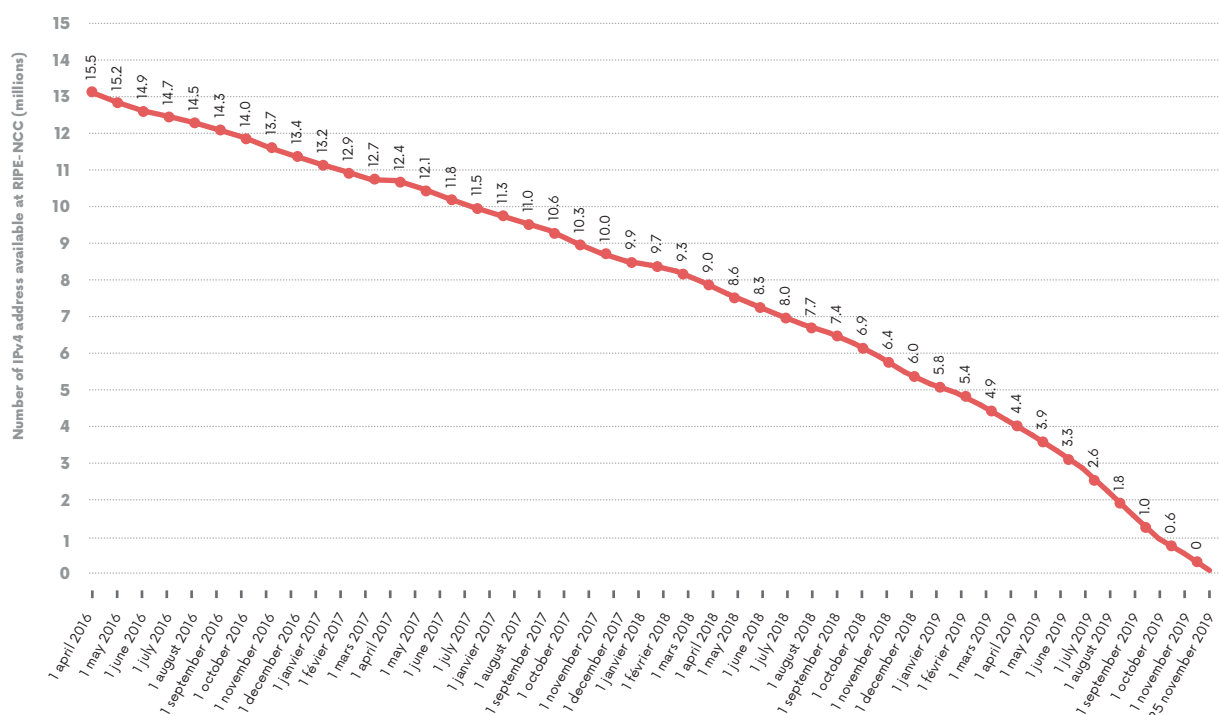
3. Free did not provide the number of IPv4 addresses already assigned.

4. Data collected by Arcep from ISPs, in accordance with Arcep Decision No 2020-0305.

5. IPv6 addresses are encoded over 128 bits. In theory, a maximum of 2128 (or approximately 3.4×10^{38}) addresses can therefore be assigned simultaneously.

6. N.B. the observations and work mentioned in this document concern only the Internet and do not apply to the private interconnection between two actors, in particular the interconnection of the networks of two operators for the termination for voice calls in IP mode.

TIMELINE OF IPv4 ADDRESS EXHAUSTION



Source: RIPE-NCC data

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

If continuing to have the Internet operate in IPv4 will not prevent it from functioning, it will prevent it from growing. 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. Added to which, IPv4 address bought on the secondary market can block access to certain banking and video on demand services if the address's geolocation has not been updated.

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

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.



What are the most plausible IPv4 exit strategies?

There is no IPv4 exit strategy as yet, and it is still very hard to predict what it might be. If we nevertheless try to imagine what the different stages in such a scenario might be, they could go as follows:

1. Almost all of the consumer Internet access plans being sold are IPv6-enabled, in addition to IPv4.
2. Almost all of the Internet access plans being sold to consumers and businesses are IPv6-enabled by default. IPv4 connectivity is still included.
3. A substantial percentage of websites are hosted in IPv6 only, despite the pockets of resistance to IPv6 in the access that some companies provide to their staff. These sites can no longer be accessed from an enterprise that blocks IPv6.
4. A substantial percentage of ISPs no longer offer IPv4 connectivity. It is no longer possible to view websites that are hosted only in IPv4.
5. Most websites abandon the now defunct IPv4. IPv4 is no longer used on the Internet, but can continue to be used for private networks.



BEREC IPv6 workshop

As Europe had been coping with the shortage of IPv4 addresses for more than a year, the transition to IPv6 became a major innovation and competition issue. In this context, BEREC has organised an internal workshop on 7 October of last year, in order to take stock of the state of IPv6 deployment in Europe. The workshop's main goals were to deliver a snapshot of IPv6 in Europe, highlight problems caused by delays in IPv6 deployment, gather information on the actions being taken by Member States/NRAs to foster the transition to IPv6, share best practices and discuss the actions that could be taken through BEREC to advance IPv6 deployment in Europe.

In addition to testimonials from the Belgian (BIPT), Finnish (Traficom) and French (Arcep) regulators, on the actions they are taking to foster deployment, RIPE NCC, Internet Society and Europol all brought their expertise on the subject, underscoring the common objective of achieving ubiquitous IPv6 deployment, to guarantee the Internet's future development. The workshop was an opportunity to present the findings of an internal questionnaire given to BEREC members prior to the workshop. The questionnaire concerned the impact that the shortage of IPv4 addresses has had at the national level, national actions being taken, the different legal frameworks in place to govern IPv6 deployment, and proposed courses of action to be taken within BEREC to accelerate the transition to IPv6.

During the workshop, BEREC reiterated how vital IPv6 is for the Internet, and its role as a key prerequisite to achieving a digital Europe. Nevertheless, three quarters of people in the European Economic Area (EEA) today do not have access to IPv6, and there are tremendous disparities in IPv6 deployment levels in the different countries. Some countries have switched around half of all users to IPv6 (Belgium, Germany, Greece, Switzerland, France) while others have not yet begun to deploy the protocol (Malta, Montenegro, Serbia, etc.). Sizeable disparities between the countries also exist when it comes to data collection, the effects of the IPv4 shortage, NRAs' power to influence the transition to IPv6 and the measures taken at the national level to further this transition.

Several proposed courses of action to be taken within BEREC emerged following the workshop, starting with increasing Member States' NRAs' awareness of the benefits of making the transition to IPv6, and creating a platform for sharing experiences and best practices.

As a follow-up to this workshop, two more workshops were scheduled to provide fuel for the BEREC work programme for 2022: an outside workshop bringing together IPv6 stakeholders from across Europe, in May 2021, and an internal workshop in June 2021.

The aim of the various IPv6-related actions being taken by BEREC is to share best practices and encourage industry players to accelerate the transition, so that the Internet can continue to serve as a driving force for innovation and growth.

Open floor to



ALEXANDRE PETRESCU

Research engineer - Alternative Energies and Atomic Energy Commission (CEA)

IPv6 ADDRESSING ISSUE FOR CARS CONNECTED TO MOBILE NETWORKS

IPv6 is the acronym commonly used to refer to the internet's network layer communication protocol, i.e. Internet Protocol version 6. This protocol's design is fundamentally the same as that of its predecessor. One very important difference is the length of the addresses (128 bits for IPv6). This protocol was developed with one very heavy requirement: to be able to handle a very large number of computers, far more than were available 40 years ago. At the same time, it had to provide complete one-to-one reachability between two connected computers. It is sizeable challenge that was more than met. There nevertheless remain other challenges for IP when it comes to mobility.

Today, cars are connected to the internet using IPv4 and NAT. Their fundamental property is to be mobile across vast regions. But the internet's addressing and routing system is in fact designed for fixed entities, even if it is deployed on a very large geographical scale. Some of the fundamental ingredients of IP, such as the use of finite routing tables, and mostly static graphs for routing algorithm, makes it very hard to establish stable connections for automobiles. On the other hand, mobile operators' cellular networks are very good candidates for providing these cars with coverage, using wireless technology. Added to which, the mobility characteristics of mobile networks' link layer protocol can overcome some of IP's lack of mobility features.

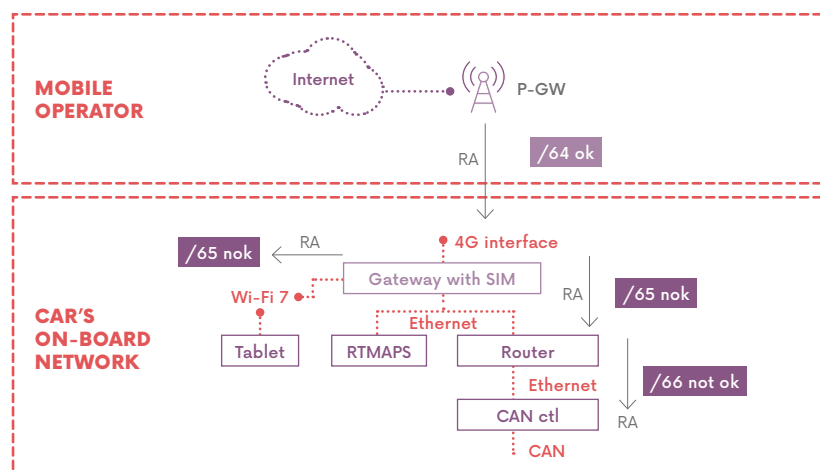
Despite that, in today's IP specifications and deployment there are still addressing issues that make it impossible to use IP in cars connected to mobile networks. One addressing issue is the 64 bits limit. This issue is caused by:

- The Internet's IP addressing architecture (RFC4291) and that of the Ethernet ID interface (RFC2464) for the most widely used protocol, Stateless Address Autoconfiguration (SLAAC), both impose a strict limit within the address, up to the 64th bit. SLAAC cannot be used with a /63 or /65 prefix. The DHCPv6-PD (Prefix Delegation) protocol is blocked by the manufacturers of popular mobile modems.
- Mobile operators in France and around the world offer a prefix

that is exactly 64 bits¹ in length for each human user. This is particular to mobile operators: fixed operators, e.g. for home (or domotics) networks, were already offering prefixes shorter than /64, e.g. /56 for CPE in the home.

- A connected car has several computers on-board, grouped into sub-networks. For cost reasons, only one of these networks, the gateway, is directly connected at the cellular network link level, and is the only one to have authentication credentials such as a SIM card.

All of these elements combined **make it impossible to use IPv6 in cars connected to the internet**. This is illustrated by the rectangles indicating “/65 nok” in the following diagram:

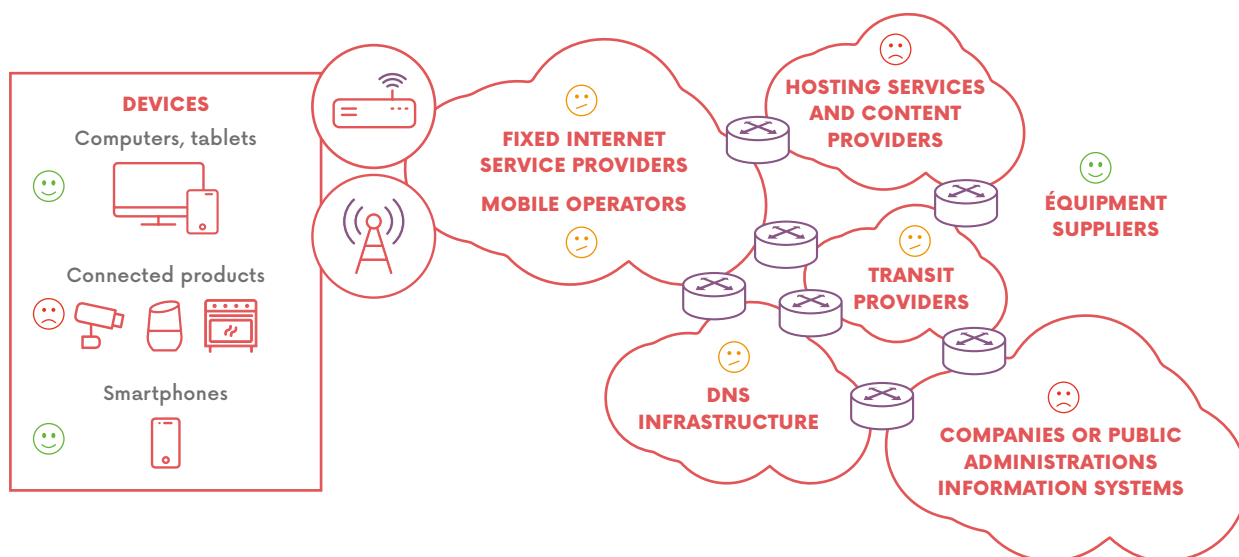


1. Ideally, an operator would offer a prefix shorter than /64 to a car's gateway, e.g. one that is /56 long. This would allow the gateway to form /64 sub-prefixes to be used in the car's sub-networks with the SLAAC protocol.

2 Barometer of the transition to IPv6 in France



STATUS OF THE TRANSITION TO IPv6 FOR THE DIFFERENT ECOSYSTEM ACTORS



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

Source: Arcep

52

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 France⁷. Arcep published the 2020 edition of the barometer on 4 December 2020.

The 2020 edition of the barometer has been enriched compared to previous editions thanks, on the one hand, to the 2020 information-gathering campaign being expanded to include the main operators in the “business” market and, on the other hand, to the addition of indicators on the progress of the transition to IPv6 by the various Government websites and online services. As detailed here below, not all stakeholders are at the same stage of the transition.

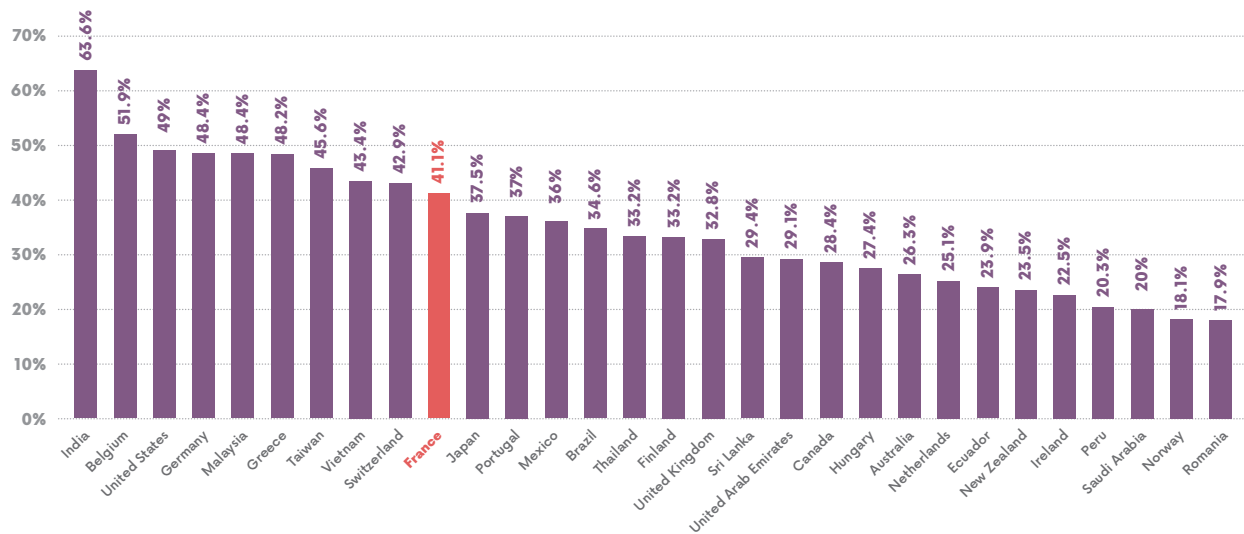
It is worth noting that, during the first lockdown in France due to the Covid-19 pandemic, the rate of IPv6 use rose from around 37% to 43% between mid-March and the end of April 2020. This rate dropped slightly after the lockdown, which can be attributed in particular to the surge in residential Internet traffic during the lockdown, which is more widely IPv6-enabled than business Internet access. This rate increased again following some mobile operators' transitions at the end of 2020.

France is among the Top 10 worldwide in terms of IPv6 adoption. According to the four main sources of publicly available data used to assess IPv6 adoption (Google, Akamai, Facebook and Apnic)⁸ France ranks fifth in Europe, behind Belgium, Germany, Greece and Switzerland.

7. Arcep Decision No. 2020-0305 on implementing surveys in the electronic communications sector.

8. Based on the median of “Google IPv6 adoption”, “Akamai IPv6 adoption”, “Facebook IPv6 adoption”, “Apnic IPv6 preferred” data from October 2020. Aggregation of national data is prorated based on the number of Internet users (source: Wikipedia, data as of 20/10/2020). 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.

TOP 30 COUNTRIES IN TERMS OF IPv6 ADOPTION



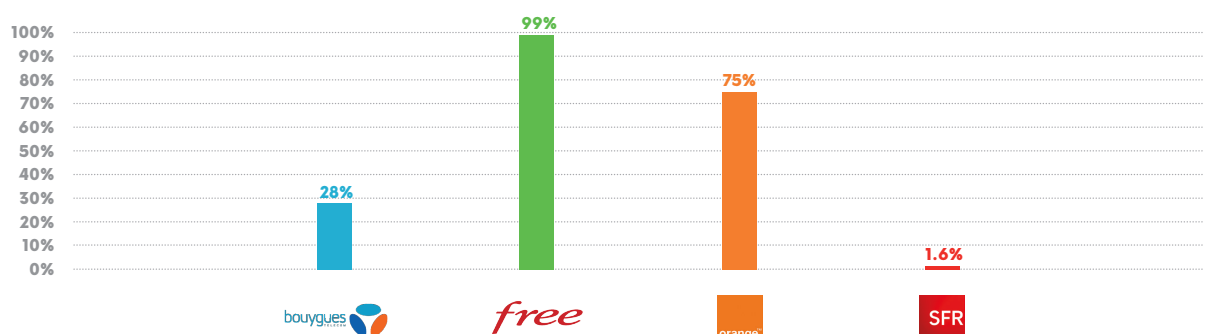
Source: median of "Google IPv6 adoption", "Akamai IPv6 adoption", "Facebook IPv6 adoption", "Apnic IPv6 adoption" data from October 2020. Pertains only to the 100 countries with the most internet users.

The barometer provides a detailed look at the status of the transition for each of the ecosystem's stakeholders.

2.1 Fixed Internet service providers

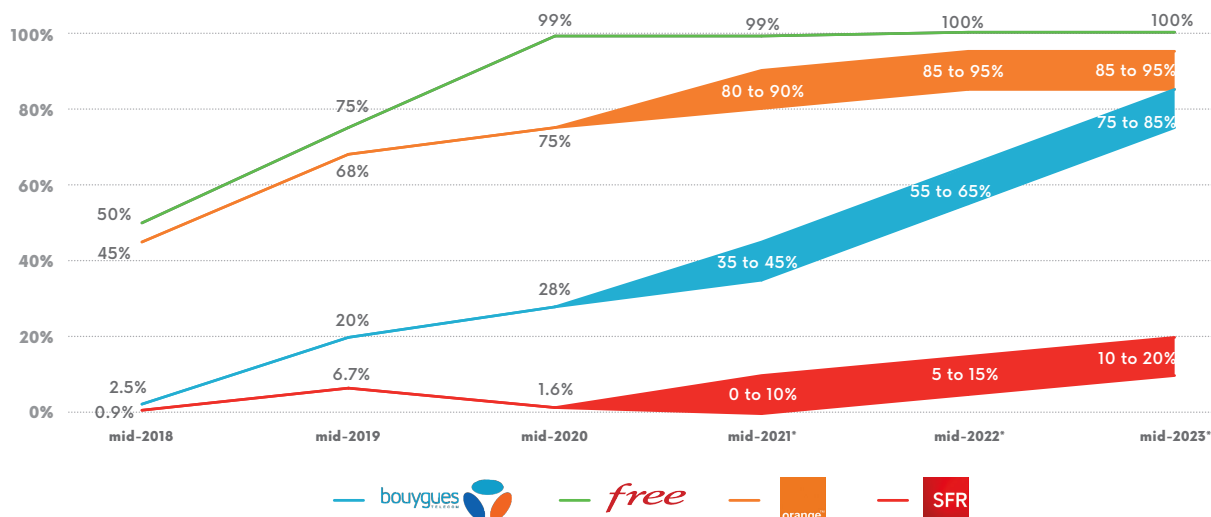
The following charts provide a snapshot of the current status of IPv6 deployment, along with forecasts for the main operators' fixed network in France.

FIXED NETWORK: PERCENTAGE OF IPv6-ENABLED CUSTOMERS



Source: data as of the end of June 2020, 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 2020, collected by Arcep from operators.

Arcep has observed progress on the fixed networks of the main telecom operators in France, but is calling on them to maintain and step up their efforts:

- The percentage of IPv6-enabled SFR customers, all technologies combined, has decreased from 6.7% in mid-2019 to 1.5% in mid-2020. This decrease, which is due chiefly to the decline in the number of IPv6-ready FttH customers, is a source of concern, given the exhaustion of IPv4 addresses. Upcoming activations also remain inadequate: between 5% and 15% by mid-2022 and between 10% and 20% by mid-2023. Arcep is thus urging SFR to accelerate the transition to IPv6 on its fixed network, especially 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 activate IPv6 per default.
- Despite an increase in the number of activated IPv6 customers and the encouraging forecasts (between 75% and 85% by mid-2023) the pace of Bouygues Telecom's IPv6 deployment is still too slow to cope with the IPv4 shortage. Bouygues Telecom is once again being urged to increase the number of IPv6-ready customers, and to step up deployment efforts on its fixed network.
- The percentage of Free and Orange customers who are IPv6-enabled is relatively high (around 99% and 75%, respectively) in addition to having increased. Projections for mid-2023 are encouraging: 100% for Free and between 85% and 95% for Orange.

- Bouygues Telecom, Free and SFR are being urged to begin the transition on 4G fixed wireless as soon as possible. Orange in particular, whose 4G fixed wireless customers are all IPv6-ready, is being encouraged to perform IPv6 activation by default on this technology.

In general, IPv6 is enabled by default for these four operators and therefore does not require any action from the user.

Regarding operators with between 5,000 and 3 million customers on fixed networks, those that had already begun their transition are moving ahead with their IPv6 deployment, with notable initiatives from Coriolis, K-Net and OVH Telecom which continue the transition to IPv6 they began several years ago. Noteworthy too are Orne THD, which completed the migration of its customers to the new protocol in 2019, and Vialis which began its transition this year. Even though several other operators plan to accelerate their transition in 2021 (Coriolis Telecom, Vialis and Zeop) and one (Ozone) is set to begin its transition next year, the pace of deployment still seems insufficient in light of the IPv4 addresses shortage. More detailed information is available in the IPv6 barometer⁹.

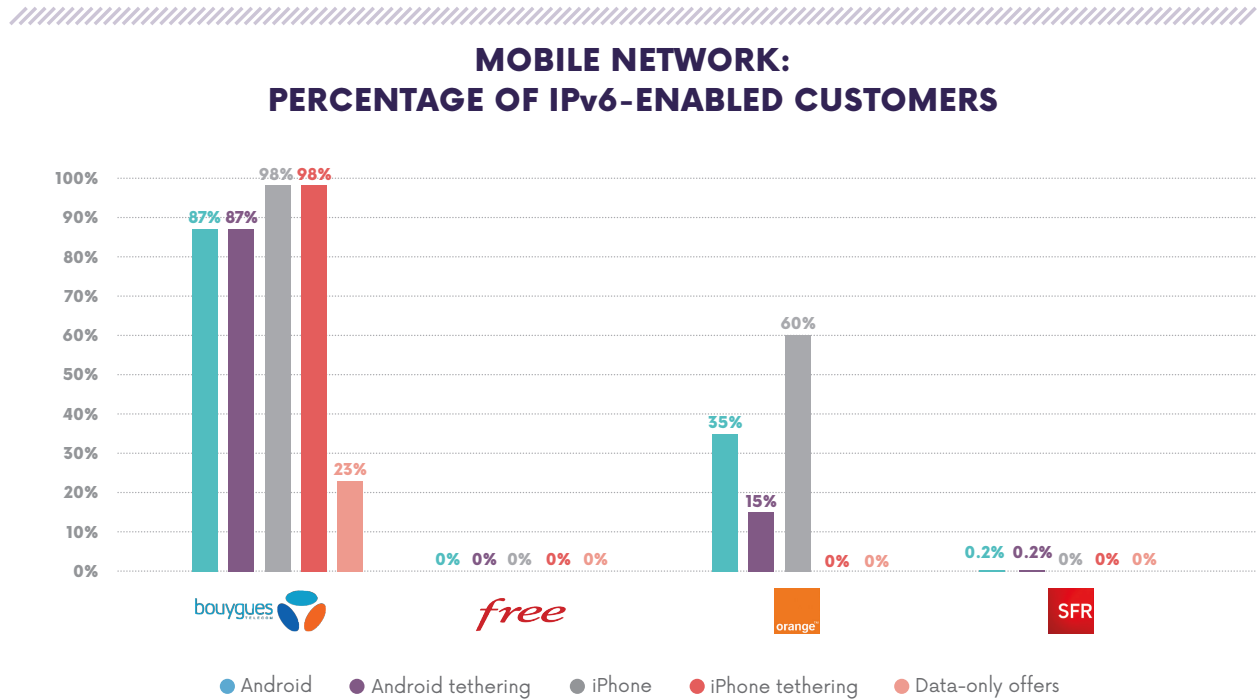
As mentioned earlier, to improve its monitoring of the transition to IPv6, Arcep expanded its information gathering to include operators who market solutions designed for business customers – aka “Pro” plans – on their fixed network. Arcep's central conclusion regarding fixed network “Pro” plans is that deployment is falling short, and urges operators to include IPv6 solutions in their plans for businesses. More detailed information is available in the IPv6 barometer¹⁰.

9. 2020 Arcep IPv6 Barometer, “Operators with between 5,000 and 3 million customers on fixed networks”: https://www.arcep.fr/fileadmin/reprise/observatoire/ipv6/Arcep_2020_Barometer_of_the_Transition_to_IPv6_dec2020.pdf#page=9

10. 2020 Arcep IPv6 Barometer, “Operators providing ‘Pro’ plans on their fixed networks”: https://www.arcep.fr/fileadmin/reprise/observatoire/ipv6/Arcep_2020_Barometer_of_the_Transition_to_IPv6_dec2020.pdf#page=10

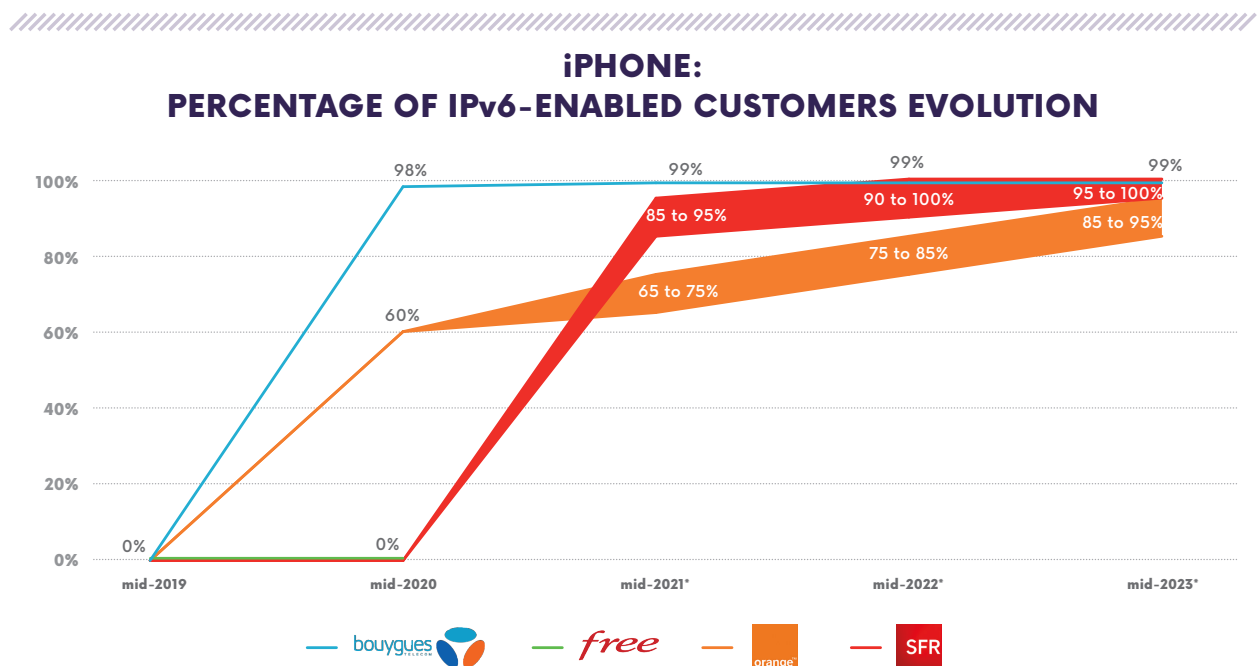
2.2 Mobile operators

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



Source: data as of the end of June 2020, collected by Arcep from operators.

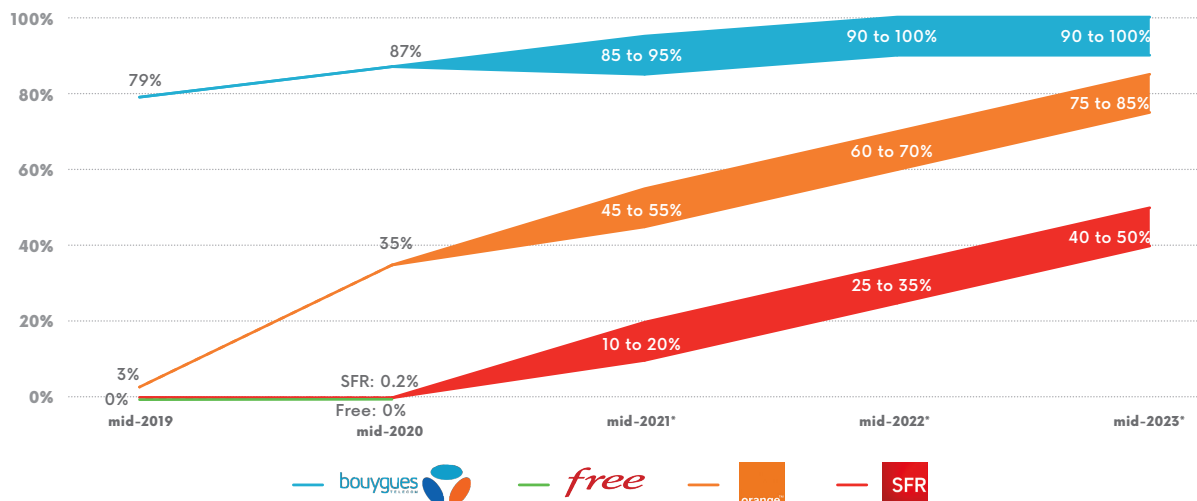
55



* Figures subject to change

Source: data as of the end of June 2020, collected by Arcep from operators.

ANDROID: PERCENTAGE OF IPv6-ENABLED CUSTOMERS EVOLUTION



* Figures subject to change

Source: data as of the end of June 2020, collected by Arcep from operators.

Despite the delay in IPv6 deployment on mobile networks, Arcep notes the encouraging forecasts and invites operators to continue working to accelerate the pace of the transition:

- Bouygues Telecom has achieved a noteworthy deployment on mobile networks, with 87% of Android customers and 98% of iPhone customers IPv6-enabled in mid-2020.
- IPv6 on the Orange mobile network is also worth noting (35% of Android customers and 60% of iPhone customers IPv6-enabled). Orange is invited to continue its IPv6 activation of mobile devices.
- SFR activated 100% of IPv6-ready customers in November 2020. All SFR customers with an iPhone switched to IPv6-enabled with the iOS 14.3 update, released in December 2020. In the first half of 2021, SFR began activating IPv6 with the update of some recent Android devices. SFR is being encouraged to accelerate the rate of IPv6 activation of Android devices.

- It is particularly unfortunate that Free Mobile is only at the start of its mobile network transition and, to date, has not been able to provide any forecasts.
- Operators are all being called on to accelerate the pace of IPv6 deployment on all of their products, notably their “data only” plans.

Zeop is the only mobile operator with between 5,000 and 3 million customers that has begun to enable IPv6 on its network (23% in mid-2020) and has a target of 40% of customers IPv6-enabled by mid-2021. The remaining operators do not plan to have deployed IPv6 by mid-2021. Mobile networks' IPv6 deployment is even more behind than it is on fixed networks, and operators with between 5,000 and 3 million mobile customers are urged to begin the transition to IPv6 very soon. More detailed information is available in the IPv6 barometer¹¹.

There are sizeable disparities between operators when it comes to IPv6 deployment on their mobile network “Pro” plans. Operators are invited to initiate and accelerate IPv6 deployment on all of their “Pro” plans. More detailed information is available in the IPv6 barometer¹².

11. 2020 Arcep IPv6 Barometer, “Operators with between 5,000 and 3 million customers on mobile networks”: https://www.arcep.fr/fileadmin/reprise/observatoire/ipv6/Arcep_2020_Barometer_of_the_Transition_to_IPv6_dec2020.pdf#page=16

12. 2020 Arcep IPv6 Barometer, “Operators providing ‘Pro’ plans on their mobile networks”: https://www.arcep.fr/fileadmin/reprise/observatoire/ipv6/Arcep_2020_Barometer_of_the_Transition_to_IPv6_dec2020.pdf#page=17

Open floor to



FRÉDÉRIC LASOROSKI

Head of Network Performance - Bouygues Telecom



IPv6-COMPATIBLE NETWORKS ARE INEVITABLE

Mobile internet use and data connectivity needs have exploded over the past 15 years, with the advent of smartphones, 4G boxes, smart devices, connected cars... At the same time, new generation mobile networks have come to cohabitate with their predecessors – from 2G to 5G – multiplying the need for IP addresses, and creating serious management challenges for operators. Bouygues Telecom understood more than 10 years ago that IPv6-compatible networks would become inevitable.

But there were two problems, which restricted and delayed its implementation:

- The need for IPv4 and IPv6 to cohabitate on fixed and mobile

networks, using complex and costly mechanisms to do so;

- IPv6 support on customer devices and boxes.

Equipment suppliers were quick to implement IPv6, followed by application providers, but the very lengthy lack of transition mechanisms on devices prevented a large-scale commercial implementation from happening. On mobiles, implementation of IPv6-only became possible with the integration of 464XLAT in Android 4.3.

Bouygues Telecom was able to rise to these many challenges! Over the past several years, it has upgraded its entire network to IPv6. Back in

November 2015, Bouygues Telecom, the first operator in France to launch a VOLTE service commercially, activated IPv6 on IMS APN. The implementation then expanded to include the mobile data service: for Android devices starting in November 2017, then iOS in September 2019. As of 31 January 2021, amongst Bouygues' consumer clientele, 89% of Android devices and 98% of iPhones have firmware that activates IPv6 by default for their mobile data service. Today, Bouygues Telecom continues to deploy IPv6 in every market segment. The tremendous increase in the number of connected objects has led Bouygues Telecom to incorporate IPv6 by default in all of its IoT products.



PATRICK AINARD-SIMONET

IPv6 project leader - mobile network - Orange

MOVING TOWARDS AN IPv6-ONLY MOBILE NETWORK

Having anticipated the expected shortage of IPv4 addresses, several years ago Orange began evolving its mobile network to make it IPv6-compatible, even if there is an IPv4 address sharing mechanism on the mobile network that makes for more cost-effective management of the scarce resource that is IPv4 addresses.

The goal was to make our consumer clientele IPv6-enabled in a transparent way, in other words without them having to do anything and without compromising quality of service. In 2019, Orange began activating IPv6, and today more than half of our customer use smartphones configured for IPv6-only use, without this switch

having resulted in an increase in customer service calls.

At the same time, Orange expanded IPv6 access to business and corporate customers, and to Machine-to-Machine and Internet of Things (IoT). It's also worth mentioning that Orange made the necessary upgrades to its network to satisfy certain businesses' own particular architecture, but they also need to have a compatible infrastructure to inter-operate with our network in IPv6.

Regarding IoT, IPv6 will create the ability to have the colossal number of addresses needed, so it is in both operators' and businesses' best

interest to adopt the protocol. Orange is ready, but change also needs to happen at the customer equipment level.

To conclude: while our network was IPv4-only just a few years ago, today IPv4 and IPv6 are cohabitating on it, which creates a degree of complexity, especially in terms of operation. The next stage will be to have an IPv6-only network. And this is where the IPv6 task force that Arcep created has a vital role to play, by encouraging every stakeholder to deploy IPv6. We need everybody to be on board to be able to make that transition to IPv6-only and reap all of the benefits that the new protocol has to offer.

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



Operators awarded 5G frequencies must comply with an IPv6-compatibility obligation

Arcep introduced an obligation for operators who are awarded a licence to use 5G frequencies in the 3.4 – 3.8GHz band in Metropolitan France to be IPv6 compatible¹: “The licence-holder is required to make its mobile network compatible with the IPv6 protocol as of 31 December 2020”. As stipulated in its reasons, the goal is to ensure that services are interoperable and to remove obstacles to using services that are only available in IPv6, as the number of devices in use continues to soar, and because the RIPE NCC has run out of IPv4 addresses.

The impetus behind this obligation was the emergence of online services that were only available in IPv6 (i.e. no

IPv4 connectivity). Some web hosting plans no longer include IPv4 by default² and IPv6 is the only option available to access the NAS of a customer connected to an ISP that uses Carrier Grade NAT (CGN)³. Which is why it is important that every customer be able to activate IPv6 on their mobile plan, to be able access the entire Internet.

In its public consultation on the award of new frequencies (700 MHz, 900 MHz and 3.5 GHz), Arcep also proposed an obligation of IPv6 compatibility:

- for mobile networks in Reunion and Mayotte⁴;
- for mobile networks in the Antilles and in Guiana⁵.

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

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

3. See lexicon.

4. Arcep public consultation of 18 December 2020 on the procedure for awarding frequencies in the 700 MHz and 3.4 – 3.8 GHz bands in Reunion, and 700 MHz and 900 MHz band frequencies in Mayotte.

5. Arcep public consultation of 2 October 2020 s on the procedure for awarding frequencies in the 700 MHz and 3.4 – 3.8 GHz bands in the Antilles and in Guiana.





Tutorial



HOW TO ACTIVATE IPv6 ON YOUR MOBILE PHONE

On its website,¹ 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 make that change. Reminder: the main operators' IPv6 activation policies are as follows²:

MOBILE NETWORK: IPv6 ACTIVATION POLICY

				
IPv6 enabled by default on Android	Android 4.4 or higher, via device manufacturer update	Not provided	Samsung: Android 9 newer.	Non (activation par le client depuis son terminal*)
IPv6 enabled by default on Android, with a shared connection	Android 4.4 or higher, via device manufacturer update	Not provided	Samsung: Android 10 newer.	Non (activation par le client depuis son terminal)
IPv6 enabled by default on iPhone	iPhone 5S and newer, running iOS 12.2 or higher	Not provided	iPhone 7 and newer, running iOS 13 or higher	iPhone 6S and newer, running iOS 14 or higher
IPv6 enabled by default on iPhone, with a shared connection	iPhone 5S and newer, running iOS 12.2 or higher	Not provided	iPhone 7 and newer, running iOS 14 or higher	iPhone 6S and newer, running iOS 14 or higher
IPv6 enabled by default on data plans only	Progressive update of compatible devices	Not provided	New products from January 2021 onwards	No (customer performs activation on their device)

Source: data as of end of June 2020, collected by Arcep from operators.

If your mobile offers you an 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>.

1. (in French) <https://www.arcep.fr/demarches-et-services/utilisateurs/activer-ipv6-mobile.html>

2. More detailed information is available in the 2020 barometer of the transition to IPv6 in France.

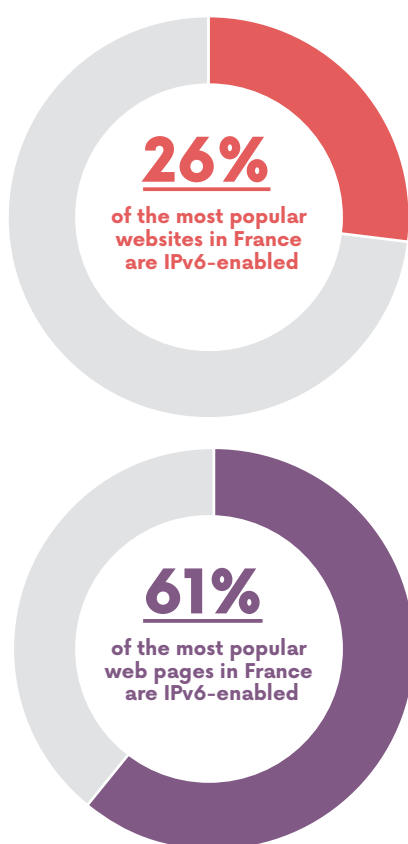
2.3 Web hosting

Web hosting services continue to constitute one of the main bottlenecks in the migration to IPv6: only 26% of the most popular websites in France, according to Alexa rankings, are IPv6-enabled¹³. A site is considered IPv6-enabled if its domain name is mapped as being IPv6 (AAAA) in the DNS server record.

Note that the percentage of web pages that are IPv6-enabled (IPv6 content) is significantly higher than that (61%)¹⁴. The reason is that many of the smaller content providers operate websites (generally small number of pages viewed) that are not IPv6-compatible.

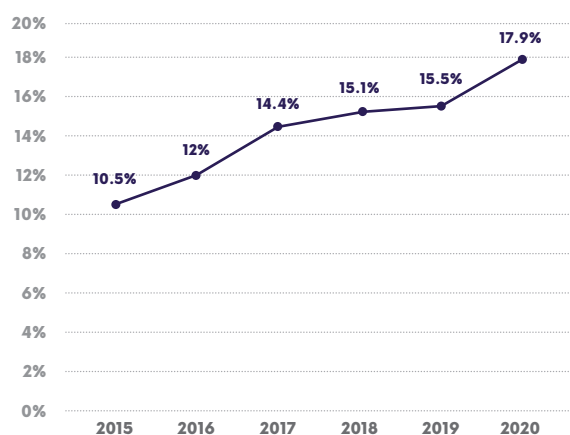
The percentage of IPv6-enabled sites stands at a mere 17.9% when looking at the 3.62 million .fr, .re, .pm, .yt, .tf, and .wf¹⁵ websites. This percentage has been increasing since 2015, but the pace of this increase appears far from fast enough to enable a complete transition in the next few years.

Even if several hosting services include IPv6 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 activated by default. Among that Top 10, only IONOS 1&1 and Cloudflare have more than three quarters of their sites IPv6 enabled, which make them examples to follow.



Source: 6lab Cisco as of 11/02/2020 (6lab.cisco.com). Data of the top 730 websites in France as ranked by Alexa (www.alexa.com/topsites/countries).

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



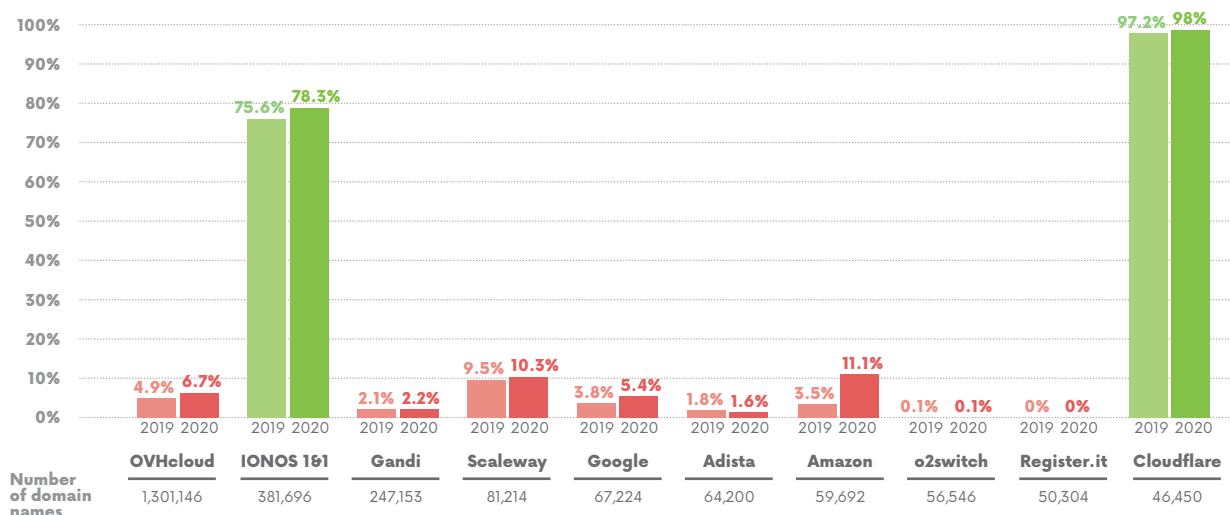
Source: Afnic data, August 2020.

13. Cisco 6lab as of 02/11/2020 (https://6lab.cisco.com); Data on the top 731 websites in France, Alexa rankings: <http://www.alexa.com/topsites/countries>

14. *Ibidem*.

15. Afnic data, August 2020. For these data, the Top 10 and Top 100 are defined in terms of the number of domain names hosted.

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



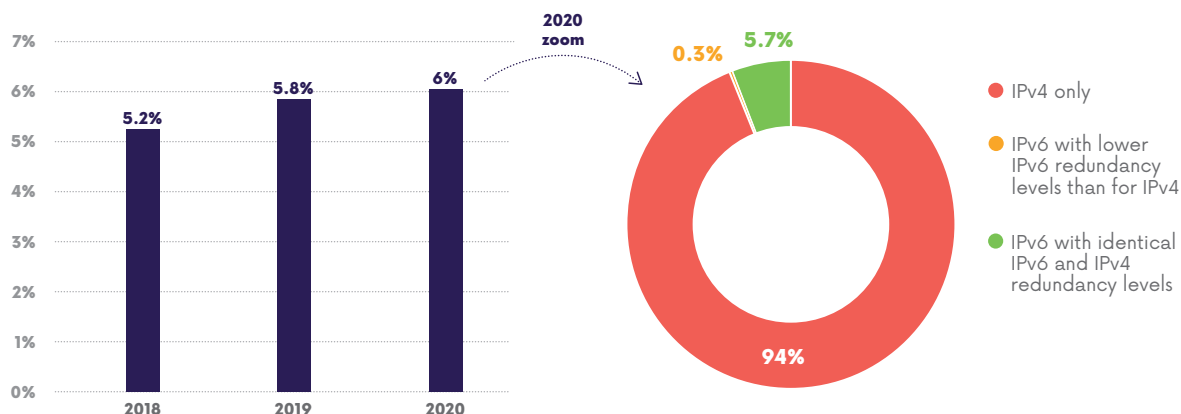
Source: Afnic data, August 2020.

2.4 Mail hosting

The transition of the main mail hosting services is also proving very slow: only 6% of mail servers on .fr, .re, .pm, .yt, .tf and .wf domain names are currently IPv6-enabled (compared to 5.8% as of 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 issues¹⁶.

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.

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



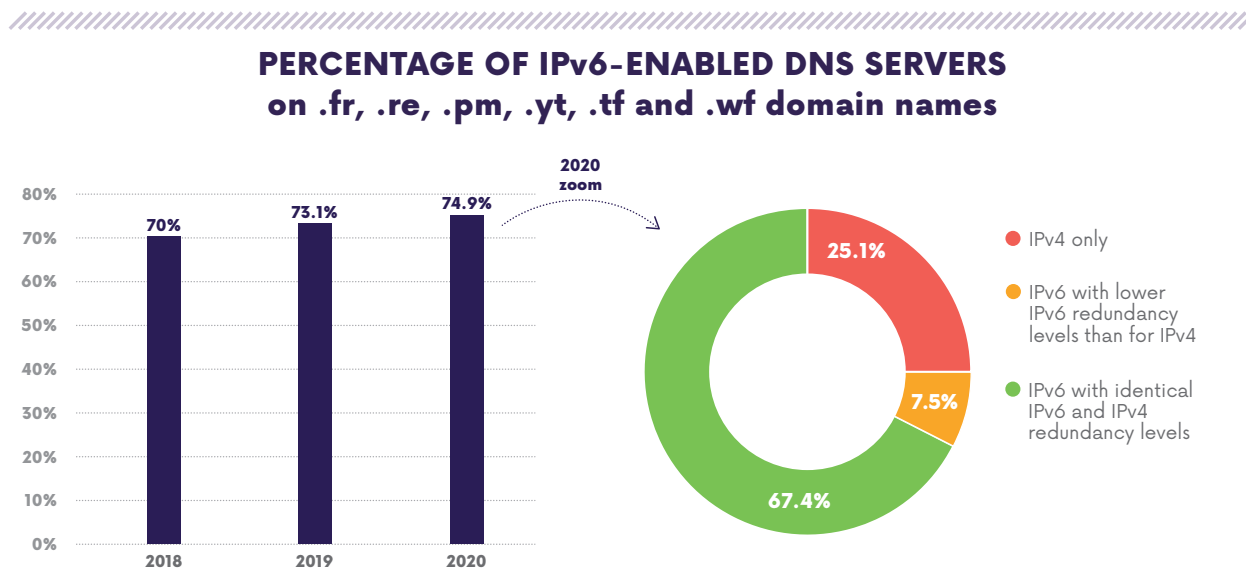
Source: Afnic data, August 2020.

16. Afnic data, August 2020.

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 servers¹⁷ supporting IPv6. Around 67%¹⁸ of DNS servers guarantee an IPv6 resilience equivalent to IPv4 (identical redundancy levels).



Source: Afnic data, August 2020.

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, this year the barometer has been enhanced with indicators on the progression of French government websites' and online services' transition to IPv6. The current study pertains to the 243 sites with the .gouv.fr suffix and available in HTTPS¹⁹.

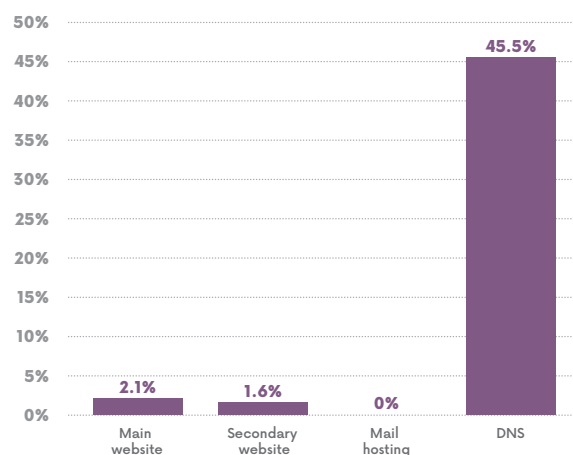
DNS servers' transition to IPv6 is relatively well advanced, with 45.5% of them being IPv6-enabled. Mail hosting, on the other hand, is still entirely in IPv4 and the percentage of government websites using IPv6 stands at only 2.1% for the main websites²⁰ and 1.6% for secondary ones²¹ (cf. annex for details on the websites and online services in question).

Even if some sites are available in IPv6, it is regrettable that the vast majority are still using only IPv4. The level of IPv6 deployment on government websites and online services thus remains very inadequate, 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 website²².

The next barometer will be published in the second half of 2021.

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



Source: tests performed by Arcep in November 2020, based on Afnic data.

17. An authoritative DNS (domain name server) is the primary DNS server for a domain, in other words the one that holds the domain name resolution information.

18. Afnic data, August 2020

19. 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.

20. Main site: the site suggested/linked to by default by a search engine.

21. 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).

22. https://www.arcep.fr/fileadmin/reprise/observatoire/ipv6/Arcep_2020_Barometer_of_the_Transition_to_IPv6_dec2020.pdf



US government working to migrate all federal government systems and services to an IPv6-only environment

On 19 November of last year, the Office of the President of the United States published a memorandum¹ that seeks to complete Federal government systems' and agencies' transition to the IPv6 protocol, the goal being to update guidelines on the operational deployment and use of IPv6 across all federal information systems and services.

The US government memo highlights the fact that all of the measures put into place to prolong the life of IPv4 addresses increase the network infrastructure's cost and complexity, and raise significant technical and economic barriers to innovation. It also states that a complete transition to IPv6 is the only viable option for ensuring future growth and innovation in Internet technology and services.

This approach is not new for the United States. It is in fact drawing on initiatives that began in 2005 to advance the adoption of IPv6, and consolidated by a memorandum in 2010 that sought to make government services (e.g. web browsing, e-mail, DNS, ISP, etc.) IPv6 native, and to upgrade internal client applications that communicate with public Internet services and enterprise networks handling native IPv6.

Building on this, the 2020 memorandum lays down the steps to complete IPv6 deployment in every federal system and service, and groups together proposals to help federal agencies overcome the barriers preventing them from migrating to IPv6-only. To this end, it lists a set of specific measures the agencies must take to achieve the transition to IPv6, including:

- prepare an IPv6-only infrastructure by establishing a clear timetable with specific deadlines (e.g. migrate at least 80% of IP-enabled assets on Federal networks are operating in IPv6-only environments by the end of 2025; identify and justify federal information systems that cannot be converted to use IPv6 and provide a schedule for replacing or retiring these systems;
- ensure that future acquisitions of networked information technology included 1Pv6 requirements;
- issue periodic updates to incorporate the latest Internet IETF² specifications relevant to IPv6 technology, placing special emphasis on security, IoT, adoption of cloud-based services, SDN³ and virtualised networks.
- ensure adequate security, notably by including IPv6 in all security projects, using IPv6-compatible security solutions capable of operating in an IPv6-only environments, and by following best practices for the secure deployment and operation of IPv6 networks;
- define roles and responsibilities across the government, with a list of actions to be led by the different federal administrations and agencies, to support the transition to IPv6.

This memorandum thus clearly states that "The strategic intent is for the federal government to deliver its information services, operate its networks, and access the services of others using only IPv6".

1. <https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-07.pdf>

2. Internet Engineering Task Force.

3. See lexicon.

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 Handbook for businesses: “Why switch to IPv6?”²³

The purpose of this handbook²⁴ 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?

Regarding this last question, the following table provides a few points of comparison between the two transition processes:

	DUAL-STACK	IPv6-ONLY
IPv4/IPv6 access	<ul style="list-style-type: none"> - Access to both IPv4 and IPv6, enabling a gradual transition 	<ul style="list-style-type: none"> - No IPv4 access: address translation mechanisms such as NAT64+DNS64 or dedicated reverse proxies are required to access IPv4-only resources
Configuration	<ul style="list-style-type: none"> - Need to configure both IPv4 and IPv6 	<ul style="list-style-type: none"> - Need for every station to be IPv6-enabled before IPv4 can be phased out (typical example for systems that rely on SIP telephony) - The simplest configuration
Security	<ul style="list-style-type: none"> - Different firewall security policies - Different services available on dual stack servers - Double the number of defined IPS/IDS rules 	<ul style="list-style-type: none"> - A single security configuration

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 for the information system of a corporation with 18 million IP addresses, and which has exhausted its 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 resource, and security issues have been reported on the LAN connections of Internet boxes that are IPv6-enabled;

- Digdeo, a freeware services company that has committed to no longer rely on IPv4 NAT²⁵ 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 at the same time, during a match.

23. https://www.arcep.fr/uploads/tx_gspublication/guide-entreprises-IPv6_dec2020.pdf

24. 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.

25. See lexicon

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 are invited share their interest in joining the task force with Arcep with the QR code.



The “objectif IPv6” MOOC: using education to help drive the transition to IPv6

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

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

- starting with a video that explains the key concepts, a complete course then details the operational implementation process;
- a set of practical exercises gives students the opportunity to apply the IPv6 protocol in a functional virtual network on a workstation;
- more in-depth exercises include an examination of case studies encountered in the field.

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

This MOOC allows students taking the course to:

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

A seventh, updated course will be available soon.

Tutorial



IPv6-ONLY ACCESS AND 464XLAT MECHANISMS

Bouygues Telecom, Free and Orange provide their mobile customers with Internet access in IPv6 by default, without offering native IPv4, which requires them to use a mechanism for accessing Internet resources that are only available in IPv4. SFR, meanwhile, uses a dual stack (IPv4+IPv6) system.

01. The DNS64+NAT64 duo: a solution to enable IPv6-only customers to access sites that are hosted only in IPv4

Because a sizeable percentage of websites can only be accessed in IPv4, Bouygues Telecom and Orange provide DNS64: the DNS solver does not send an IPv4 address for IPv4-only sites, but rather a synthetic IPv6 address, one that points to an NAT64 gateway installed on the operator's network. The NAT64 gateway creates the ability to communicate the IPv6 network stack of a client with IPv4 Internet. The gateway performs a classic network address translation (NAT) but by replacing the private IPv4 address with an IPv6 address.

02. Encapsulation of the destination IPv4 address in the IPv6 address

The DNS64 generates an IPv6 address that uses the 4:ff9b::/96 prefix reserved for this purpose. The final 32 bits are the 32 bits of the IPv4 site's address. The NAT64 gateway on the operator's network recovers the destination IPv4 address in the destination IPv6 address it has received. It therefore knows to perform an NAT on the fly to the destination IPv4 address, and to send the packet on the IPv4 Internet.

03. Some applications are not compatible with DNS64: birth of 464XLAT

Some applications and services may not work with a customer-side IPv6 address. This is true of applications that use a literal IPv4 address (<http://87.65.43.21>) instead of using DNS names that would be solved by the DNS64. There is, for instance, a strong likelihood that a peer-to-peer application will use a literal IPv4 address instead of a domain name. One can also get stuck in IPv4 when an application does not employ the operating system's DNS64 but rather its own DNS solver, which is not DNS64.

464XLAT was initially created by developers with Nokia N900 phones who wanted to use T-Mobile's IPv6-only service in the US. Several applications did not work, despite the carrier having a DNS64 and an NAT64 gateway. These developers began experimenting with translating IPv4 to IPv6 locally on the Nokia N900 smartphone in August 2010. This allowed a range of applications to run properly on IPv6-only networks, which could otherwise have required IPv4. This same idea and this same code were then ported to Android and incorporated into the Android Open Source¹ project in November 2012. Which gave birth to RFC6877², which was published in April 2013.

The 464XLAT is installed by default starting with Android Jellybean 4.3, released in July 2013. Users had to wait for the release of RFC7278³ in June 2014 to be able share an IPv6 connection when there is only a single /64 prefix assigned to the device, and its default integration starting with Android Lollipop 5.1 released in 2015.

1. Software submission needed for the Android Open Source project CLAT.

2. RFC6877: "464XLAT: Combination of Stateful and Stateless Translation".

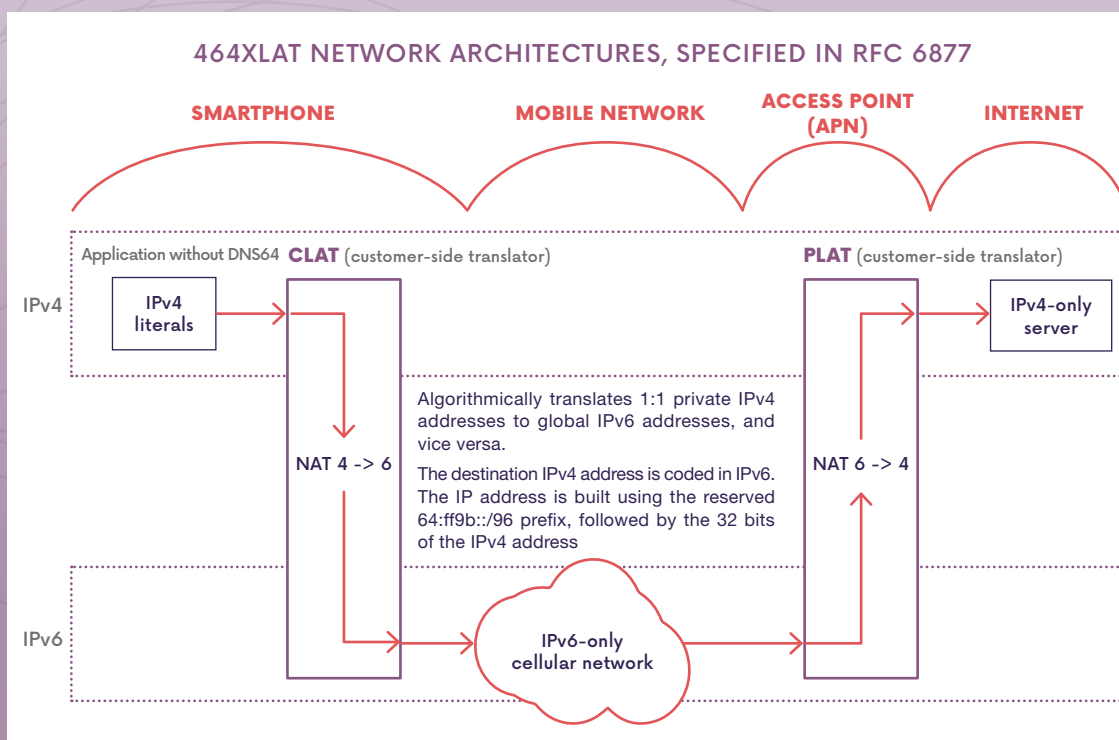
3. RFC7278: "Extending an IPv6 /64 Prefix from a Third Generation Partnership Project Mobile Interface to a LAN Link".

04. 464XLAT: a solution for customer-side IPv4 use

464XLAT consists of introducing the CLAT (customer-side NAT) into the customer's operating system for applications that appear to have a functional private IPv4 address, while the device is connected to an IPv6-only network.

Because the IPv4 addresses used by the smartphone typically belong to the small 192.0.0.0/29 range, they are the same IP addresses for each device. The CLAT translates IPv4 addresses into IPv6 algorithmically for outgoing traffic, as the DNS64 would do using the reserved 64:ff9b::/96 prefix, or another prefix found out through a DNS request towards a specific domain name: ipv4only.arpa (see RFC 8693). In any event, the final 32 bits are the 32 bits of the IPv4 site's address.

On the ISP side of the equation, it is the PLAT, the NAT64 platform that recovers the destination IPv4 address in the destination IPv6 address that it has received, to form a destination IPv4 address sent over the IPv4 Internet.



67

05. Can an operator not employ DNS64? (all traffic going to IPv4 servers goes through 464XLAT)

Yes, it is possible not to resort to DNS64, which has the advantage of allowing the customer to enable DNSSEC⁴, but the drawback of having to add an imperceptible latency and potentially have an impact on the device's battery⁵. The load on the processor can also negatively affect very high speed connections using CLAT: this is why most ISPs install DNS64, which typically enables them to process more than 99% of IPv4 traffic without losing speed or affecting the device's autonomy.

Without DNS64, devices have not CLAT, or cannot enable it, which means they have no IPv4 connectivity.

06. Why is the public IPv4 used by DNS64 in Android different from the one used for 464XLAT?

A large portion of Android devices use different IPv6 source addresses for CLAT and for traffic streams being relayed directly to the Internet. The operator's NAT64 gateway will assign a different source IPv4 address to streams coming from two distinct IPv6 sources. As a result, the source IPv4 address used for the device will be different depending on whether the request is treated via DNS64 or the CLAT.

4. See lexicon.

5. Source: RFC8683 Using 464XLAT with/without DNS64.

Open floor to



PASCAL RULLIER

CEO - Blue Networks Technologies



IS IPv6 THE PROTOCOL OF THE FUTURE?

Some operators and web hosting services believe it is, and will remain so. The biggest challenge lies in marketed services' ability to integrate IPv6. Some of the hardware installed in 2021 is not yet IPv6-compatible. Even though the shortage of IPv4 addresses and the strong encouragement from RIPE for everyone to deploy IPv6 is making the transition to IPv6 inevitable. Sticking with IPv4 will mean hunting around "for scraps" or trying to find workaround¹. So why not take the plunge?

IPv6 needs to be deployed at every level: at the hardware level, choose hardware that manages IPv6 properly, but also get proper IPv6 training. When

deploying hardware, IPv6 needs to be integrated systematically, in the same way as IPv4. Same thing at the services level: for instance, when entering a v6 DNS don't forget its reverse v6 entry². On the applications front, developers too need to integrate the IPv6 network layer as they once did with IPv4. Its permanent integration will become more and more natural over time.

BLNT, a network operator and installer, systematically integrates IPv6 in the dark or lit fibre networks it deploys or leases to municipalities or public service contractors. On leased networks, as with an activated FttH solution, the technical specificities for

IPv6 do function, but only on paper for now. Implementation may be either not yet complete, or too complex an undertaking. Keep it simple! As with FttO where the building operator handles only network transport, an operator-installer implements above IPv4 and IPv6 at the same time.

Likewise, service providers do not use IPv6, preferring instead to reroute ports to private, internal IPv4 addresses. It's time to switch³.

- 1 "IPv6, the future of the Internet?" by Cécile Motange
- 2. "RFC 8501: Reverse DNS in IPv6 for Internet Service Providers" by Stéphane Bortzmeyer
- 3. "Enterprises: why switch to IPv6?" document produced by the IPv6 task force



JACKY HAHN

Director of TV, Internet and Telephony - Vialis

DEPLOYING IPv6 ON VIALIS NETWORKS

Vialis, a 100% Alsatian operator, is present on the cable network in Colmar and the surrounding area, on the public-initiative FttH network in Alsace, and provides its expertise to a large number of white label partner networks. Vialis began acquiring its first IPv6 addresses from RIPE back in 2015, and even though the pace of deploying these IP addresses to our customers has accelerated over the past year, it has been a long haul.

Our goal is to deploy IPv6 in a way that is entirely transparent for end customers, by guaranteeing complete continuity and irreproachable quality of service, equal to what we provide today on all of the networks we service. The range of technologies that Vialis manages required us to introduce testing models, starting in 2015, and create the ability to validate a CGNAT

(Carrier Grade NAT – IP translation and sharing) solution. Customers have not encountered any major problems using this temporary solution for "classic" internet applications: internet access, messaging, streaming.

Our approach to IPv6 deployment is as follows:

1. Validate the supply of IPv6 transit with suppliers and interconnection points.
2. Verify that all network equipment and customers are IPv6 compatible. This is a mammoth task, requiring perform equipment upgrades during non-office hours, and systems upgrades working on older generation hardware.
3. Create of a true, redundant IPv6 platform for DNS, DHCP, etc. services.

4. Configure IPv6 routing for every piece of PoP and core network equipment.
5. Activate IPv6 for test customers on an identified network, and ensure it is fully functional.
6. Deploy IPv6 across the entire network.

To achieve a smooth and steady transition, we are keeping IPv4 alongside IPv6 deployments, while assisting our customers and partners, and guaranteeing that all of our Internet, Telephone and Television services continue to run at full capacity. We are still on target to reach our goal of 50% deployment by June 2021, and this despite the current circumstances.

Open floor to



BENOÎT DESMARECAUX

CTO - iBloo Pro



TEACHING IPv6 BEFORE START TALKING ABOUT IPv4

IPv6 is a way of thinking about and designing a network that is totally different from IPv4.

A still misunderstood technology, IPv6 “scares” a lot of people (the public, businesses, IT companies). We are always afraid of the unknown.

We have implemented IPv6 on our network, right up to the customer level, from the dual-stack design of our backbone. And we noticed that IPv6 makes a whole lot of things easier, including:

- Equipment addressing, thanks to the DHCPv6-PD protocols.
- Routing: our equipment is therefore less of a drain on resources
- Security since:

- Today, a hacker can scan ports on an IPv4 /22 block in no time, not so an IPv6 /32 block
- Easier firewall management since there is no more private IP, or NAT/PAT (Network Address Translation/Port Address Translation)
- No more management of NAT/PAT resource sharing, or of traceability should a legal case arise.

To guarantee a successful adoption of IPv6 France, it is crucial for public institutions to create a post-secondary training programme for their teachers/instructors.

As today:

- IPv6 is still barely addressed in post-secondary programmes, even

in specialised network courses, even though it should be an automatic, if not essential part of the curriculum.

- Local IT service companies who are serving members of the public or even local small and medium businesses do not have the necessary IPv6 knowledge, and so avoid it.
- Government services are lagging behind. E.g. far too few pool.ntp.org timeservers are IPv6 compatible.

We believe that, for IPv6 to accede to its rightful place, we need to start teaching it, even before we start talking about IPv4. So that IPv6 becomes a reflex, and IPv4 a “workaround” and not the reverse.



LAURENT PAVOINE

Director of Sales - K-net

IPv6 ON ACTIVATED PUBLIC INITIATIVE NETWORK OFFERS

The vast majority of the infrastructure operators we work with have done extensive work on IPv6! Which has allowed us to now have more than 85% IPv6-ready customers.

Despite an overall satisfactory level of operation, we are nevertheless encountering several issues, depending on the infrastructure operator, some of which are not yet offering IPv6.

- Covage has deployed IPv6 very efficiently on most of its networks, and there are only a few updates still to perform – all of which have been planned and scheduled.
- Altitude has been switching to a new architecture over the past several

years, and IPv6 works well. There are still a few customers left to switch over before June 2021.

- Axione works perfectly and entirely in IPv6.
- SIEA has installed IPv6 in most of its networks and discussions are underway about a DHCPv6 migration in the remaining service areas.
- Among the national infrastructure operators we work with, there are now only two that have not yet implemented IPv6.

The stock of available IPv4 addresses is running out very quickly. IPv4 speculation is going great guns,

as addresses are now trading for around \$30 per address.

If infrastructure operators are well aware of the urgency and benefits of IPv6, content providers too still need to support this technology. This is the main area where IPv6 adoption in France lags somewhat behind. If Big Tech companies like Google, Apple, Facebook, Amazon and Microsoft are all IPv6-ready, there are still (far too) many sites that remain accessible only in IPv4. And it is this reality that, today, is preventing us from offering all of our subscribers IPv6-only services, as they would only have access to a portion of the Internet.

PART 2

Ensuring internet openness

70

CHAPTER 4

Guaranteeing net neutrality

CHAPTER 5

Platforms: internet
access gatekeepers

GUARANTEEING NET NEUTRALITY

What you need to know

12

months

of monitoring networks' resilience during the Covid-19 crisis, for Arcep and its European counterparts.

December 2020:

launch of a new version of **Wehe** which includes an improved comparison test and a new port blocking test.

304

user reports

filed in 2020 through the "J'alerte l'Arcep" platform.

European Regulation No. 2015/2120 guarantees open Internet access to every citizen living in the European Union. Arcep is responsible for enforcing the net neutrality regulation in France, and for guaranteeing that Internet service providers (ISPs) comply with it. The Authority has a range of technical, regulatory and collaborative tools at its disposal to fulfil its responsibilities, and which it employs to this end.

1 Net neutrality and the Internet's founding principles

The Internet's founding principles, starting with its openness by design, make the Internet 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 net neutrality principle 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. Net neutrality thus seeks to ensure that the Internet continues to operate in accordance with the founding principles that govern it.

1.1 An Open Internet by design

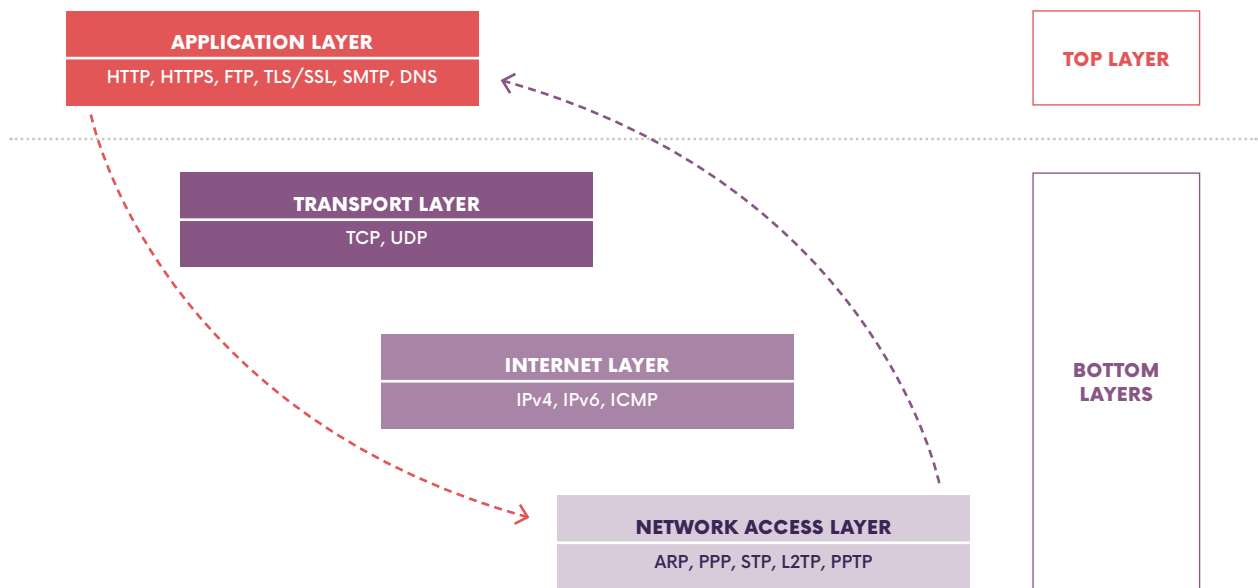
The Internet is an open access network which is based on a horizontally layered network architecture. Each network layer operates independently and serves a separate function in the Internet's operation, like physical network access, data transport or running an application. The actual separation of the network layers comes from the use of communication standards – called network protocols – that are specific to each network layer, and allow the elements in the same layer to communicate together. Ultimately, the Internet's architecture is based on a common theoretical model: the TCP/IP model, named after its two main protocols¹.

Several principles that are inherent to the Internet functioning derive from the TCP/IP model: the layering principle, the "best effort" principle governing data delivery, the end-to-end and the network transparency principles.

Each network layer operates independently: the segmentation of the Internet functions means that the bottom layers are dedicated to routing the data entrusted to them (addressing and relaying the transmitted information), leaving to the top layer the responsibility for the other functions (processing and presentation of the relayed data), i.e. running an application (cf. simplified diagram of the TCP/IP model). To prevent the data from getting lost when passing through the successive network layers, each layer adds essential information to the data being delivered, which is gathered in the header of each data packet being relayed by the previous layer (cf. simplified diagram of the encapsulation mechanism).

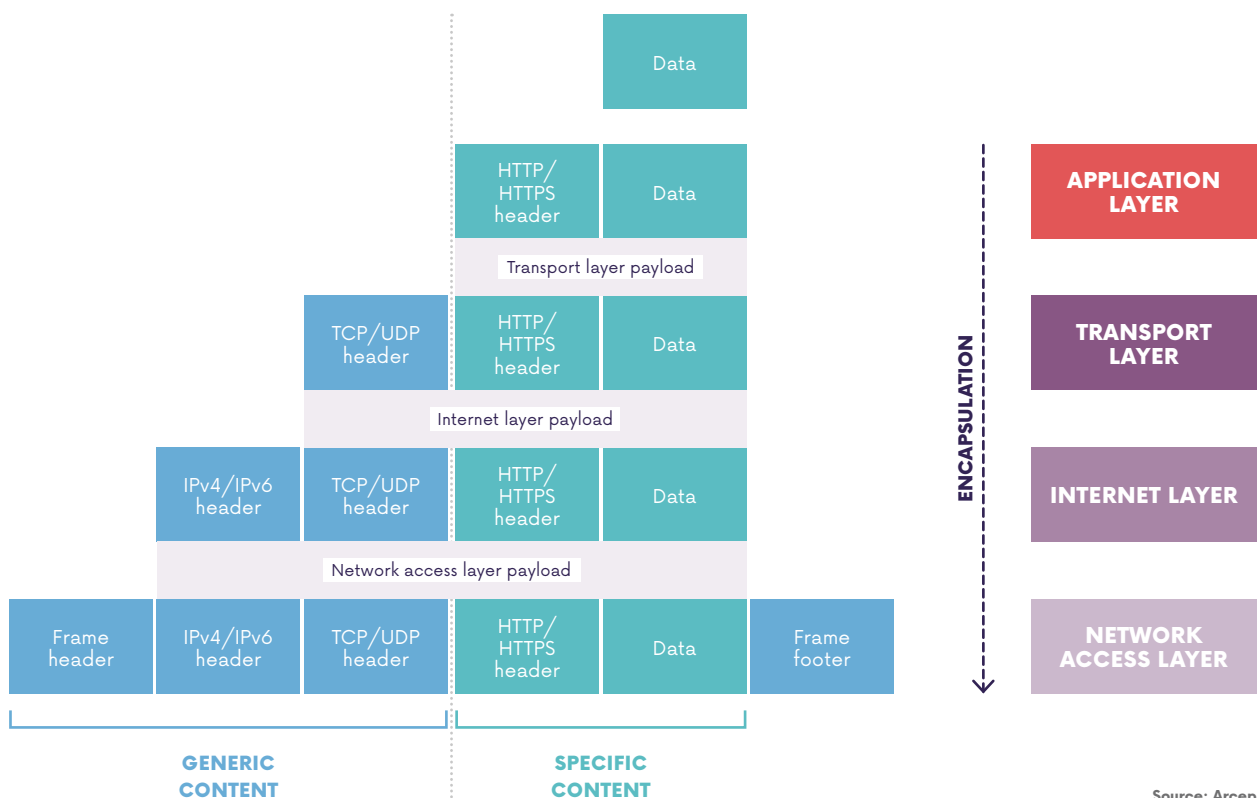
¹. TCP/IP are the commonly used protocols. Other operating protocols do exist, in particular the UDP protocol. See the simplified diagram of the TCP/IP model for a non-exhaustive list of other protocols used in the different network layers.

SIMPLIFIED DIAGRAM OF THE TCP/IP MODEL



Source: Arcep

SIMPLIFIED DIAGRAM OF THE TCP/IP MODEL'S DATA ENCAPSULATION MECHANISM

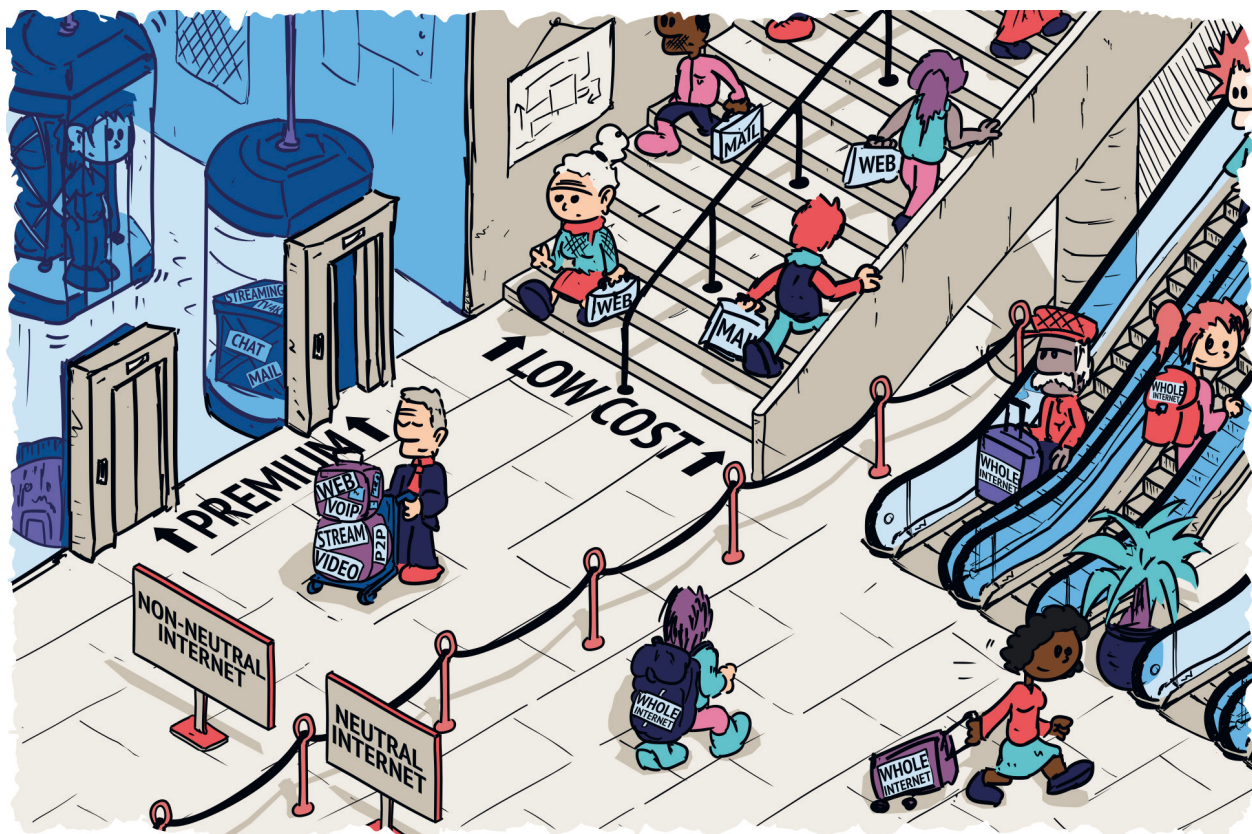


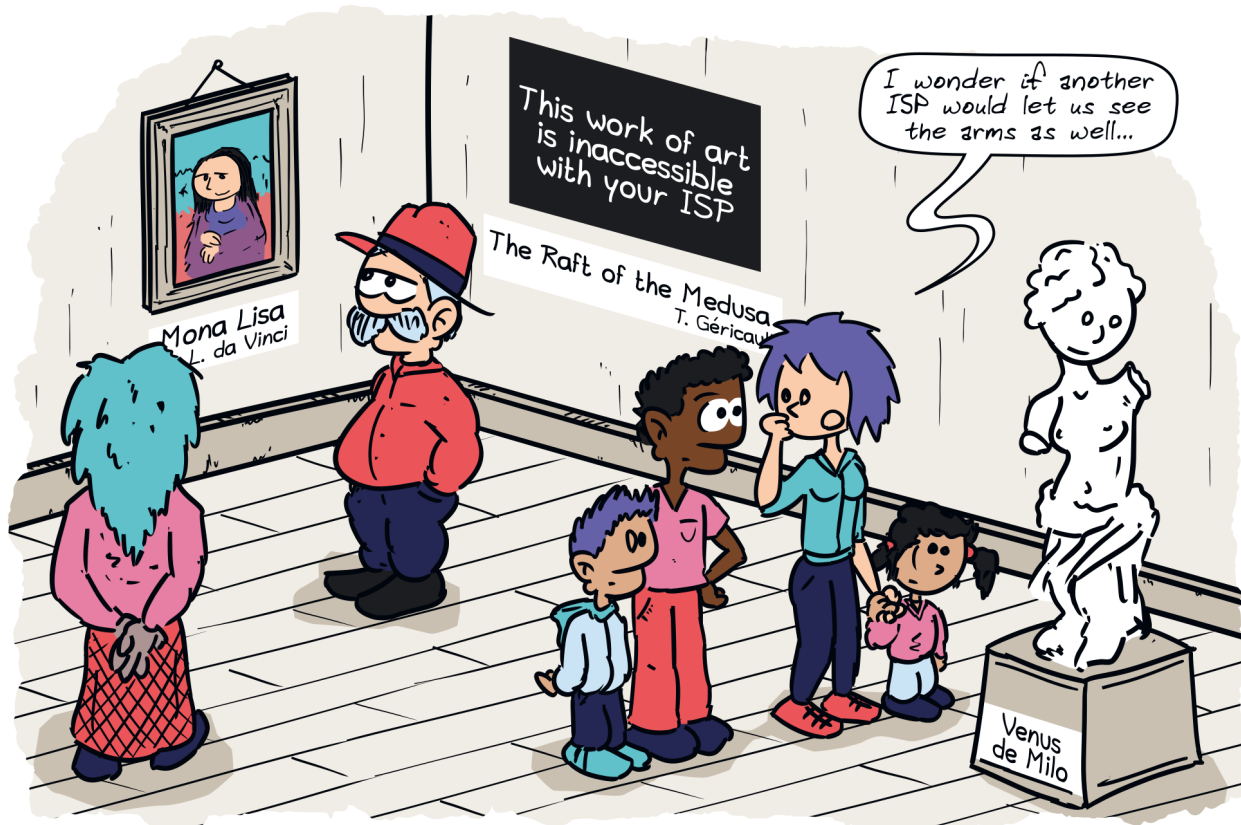
Source: Arcep

A network layer will only use the information stored in the header that is specifically dedicated to that layer. For instance, the transport layer will use the information stored in the “transport” header to transport the data it receives, but is theoretically unable to know whether the data received from the application layer belong to an e-mail, a video or a web page. This means that the data are, *de facto*, relayed as well as possible and without differentiation through the different layers along their path, in accordance with the best effort principle. In keeping with the end-to-end principle, only the services in the application layer are verifying the integrity and the compliance of the data. Lastly, because the different Internet functions are segmented into network layers, the bottom network layers’ operation is transparent for services running at the application layer. This means that the end users are, in theory, free to use the device and operating system of their choosing, since they work independently from the bottom network layers’ operations.

1.2 An open Internet by default fosters innovation

The Internet’s TCP/IP-based architecture creates the ability to layer its functions and to employ common operating conventions known as network protocols. This uniformity provides an homogeneous framework in which end users’ content, services and applications receive equal treatment on both the access and distribution sides of the equation. Therefore, the Internet encourages end users to be active participants in the creation of new contents at the application layer level, by providing them with a familiar framework and by allowing them not to take into account the bottom network layers’ operations (cf. network transparency principle). Moreover, the use of common network protocols, which are generally used within a given layer, reduces the cost of creating new services, which fosters innovation. As a result, the Internet continues to be an ecosystem functioning as an engine of innovation.





1.3 Net neutrality safeguards the Internet's founding principles

The Internet's founding principles, which are outlined above, embody the essence of the net neutrality principle: to guarantee the circulation of contents, services and applications in the best possible way, regardless of the origin and content of the packets being transported ; to use only the IP headers required to transport the data packets² and to ensure that end users can employ the device of their choice. Ultimately, net neutrality is a regulatory framework that safeguards the Internet's openness by design, and so generates significant positive externalities in terms of innovation and protects end users' rights.

The Internet's core operating principles promote a non-discriminatory routing of data streams, by treating equally the distribution and the access to all online content, services and applications. This freedom gives every end user the ability to choose how they use the Internet. This ability to receive and communicate freely contributes directly to promoting a number of end users' rights: safeguarding the diversity and pluralism of media content, freedom of expression and the freedom to access information. Protecting net neutrality also means protecting end users' ability to exercise their fundamental rights.

The year 2020 was nevertheless marked by a series of transgressions on net neutrality in several countries around the world, threatening to limit their populations' fundamental rights.

In Asia, several countries are continually adopting practices that have been denounced as undermining the Internet's openness, by controlling their citizens' access to content and information.

In China, access to the Internet is filtered by the Great Firewall of China, which monitors all of the information coming in and going out of the country. In Myanmar, government authorities have ordered the Internet to be shut down several times, in addition to restricting the use of social media and to curtailing communications between protesters and supporters of the previous head of the country. In Vietnam, authorities throttle access speeds on certain social networks to pressure them into giving in to censorship requests.

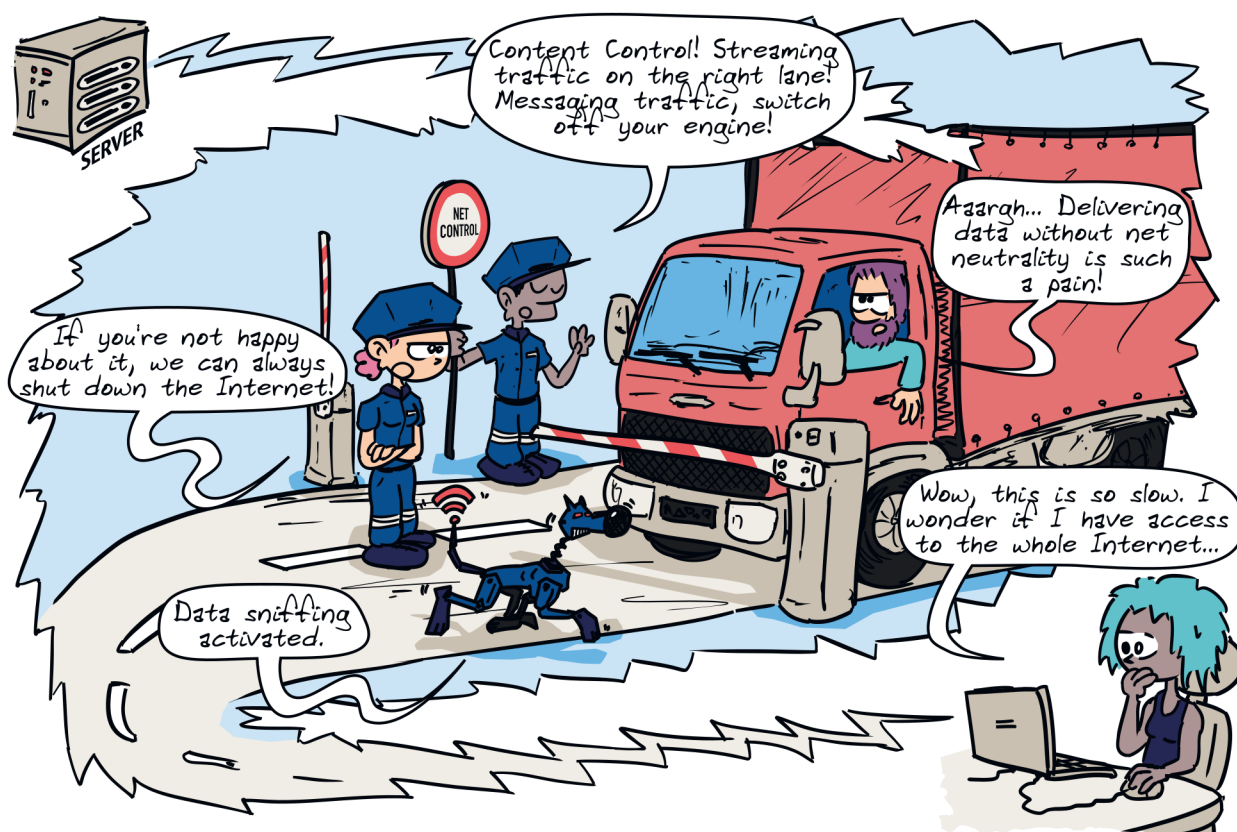
Several practices in the Middle East have been criticised: some States restrict their population's access to the entire Internet. In Iran only a "national" Internet, whose content has been approved by the government, should become available to Iranians. In Qatar, some services, such as VoIP³ calling, are banned completely. And, finally, in the United Arab Emirates, local users are unable to access a range of contents that has been deemed politically sensitive, as well as VoIP and VPN⁴ services, whose use is punishable by law.

The United States has also come under fire for the restrictions imposed on access to certain online services. On 6 August 2020, the US Administration issued an order banning two Chinese applications, TikTok and WeChat, from being available to download on app stores, saying they were a national security threat. But several federal judges blocked the order, concluding that such a move from the government raised serious freedom of expression concerns, that once again illustrates how close the ties between fundamental rights and net neutrality are. In addition, the appointment of the new acting Chair of the Federal Communications Commission (FCC), Ms Jessica Rosenworcel, who is a proponent of net neutrality, could lead to a very different regulatory policy than the one enforced by the FCC over the past several years.

2. Cf. page 66 of the 2020 Report on the State of the Internet in France.

3. See Lexicon.

4. See Lexicon.



UNESCO's work on Internet Universality

This tie between having an open Internet and protecting fundamental rights and freedoms was also reaffirmed by Unesco when defining Internet Universality indicators. In a report published in 2019¹, Unesco lists more than 300 indicators which are split into five categories.

The four principles identified as key to Internet Universality are summarised as the R-O-A-M principles, which are:

- R** – that the Internet is based on Human Rights
- O** – that it is Open
- A** – that it should be Accessible to all , and
- M** – that it is nurtured by Multistakeholder participation.

To these principles have been added Cross-Cutting Indicators concerning gender and the needs of children, sustainable development, trust and security, and legal and ethical aspects of the Internet.

These principles are meant to help national governments support the development of an open Internet, that upholds end users' fundamental rights.

1. UNESCO's Internet Universality indicators: a framework for assessing Internet development, 2019, <https://unesdoc.unesco.org/ark:/48223/pf0000367617>

Open floor to



WINSTON MAXWELL

Director of law and digital technology studies – Télécom Paris – Institut Polytechnique de Paris

WHAT IS NET NEUTRALITY'S FUTURE IN THE UNITED STATES?

Net neutrality in the US has been boxed into a narrow debate about whether internet access providers are “common carriers” under the US Communications Act. The FCC has flipped back and forth on this issue depending on which political party controls the White House, and each of the FCC decisions has been challenged in court. The US has never passed a law on net neutrality, leaving the federal regulator with only a few statutory ‘hooks’ on which to hang a neutrality policy. Will the election of Joseph Biden change things, perhaps permitting the adoption of a national net neutrality law? Probably not.

Net neutrality remains politically divisive, and many things have changed since the FCC’s 2015 net neutrality order. Internet access providers, whether fixed or mobile, still have bottleneck control over access to the internet, and still have the means and incentive to discriminate. But there have been few instances of actual blocking or improper discrimination at the access network level. Today’s questions revolve around zero rating, and how future 5G differentiated service levels will fit with neutrality principles. Most instances of discrimination and abuse of bottleneck power have occurred at the level of major social media platforms, leading to calls for regulation of “Big Tech”, including even the break-up of certain large platforms.

The Biden administration will support net neutrality, but may not make it a priority, preferring instead to focus

on platform regulation, the roll-out of 5G, cybersecurity and closing the digital divide. When the Trump administration FCC annulled the Obama administration FCC’s 2015 net neutrality order, California adopted its own law on net neutrality, which the Trump administration promptly acted to block in court. The Biden administration recently withdrew the federal government’s lawsuit against California, leaving California and other states free to apply their own net neutrality laws. California’s law resembles Europe’s, and will serve as a useful test for how net neutrality can deal with new 5G services, for example. The new FCC could potentially re-enact the old 2015 order, calling internet access providers common carriers, but without a new federal law, the FCC will remain on fragile ground.

The fierce debate on platform regulation leads us to ask whether neutrality might transcend internet access providers, potentially applying to large social media platforms and mobile operating systems as well. The harms that net neutrality is intended to prevent also exist at other levels of the internet ecosystem. For example, the problem of giving undue preference to content providers that have some capitalistic or contractual link with the internet access provider also exists for certain platforms and mobile operating systems. The problem of limiting the choice of content that internet users can consult or publish also exists, albeit in different forms, at different

levels of the internet ecosystem. Stifling innovation, another net neutrality concern, finds its way into the platform debate.

Might we be able to create common neutrality principles that apply to all bottleneck players in the internet value chain? Coming up with common principles will not be easy, because the problems are not identical between social media, mobile operating systems and access networks. Nonetheless, by focusing on the harms caused by all forms of bottleneck power on the internet, net neutrality might be transformed into guiding principles of internet fairness that apply to platforms, mobile operating systems and access networks alike. A major new aspect in the debate relates to freedom of expression on the internet. During the internet’s youth, any form of content filtering was considered an unacceptable interference with freedom of expression and the proper functioning of the marketplace of ideas. More recently, open and unfiltered discourse on social media has led to extreme and manipulative content drowning out all the rest, posing a threat to democratic institutions, the very thing that freedom of expression and net neutrality are meant to protect. Any new approach to neutrality should take this shift into account, and consider how online content moderation at any level of the internet ecosystem can support free speech values while not leading to a meltdown of democratic processes, reasoned debate and belief in science.

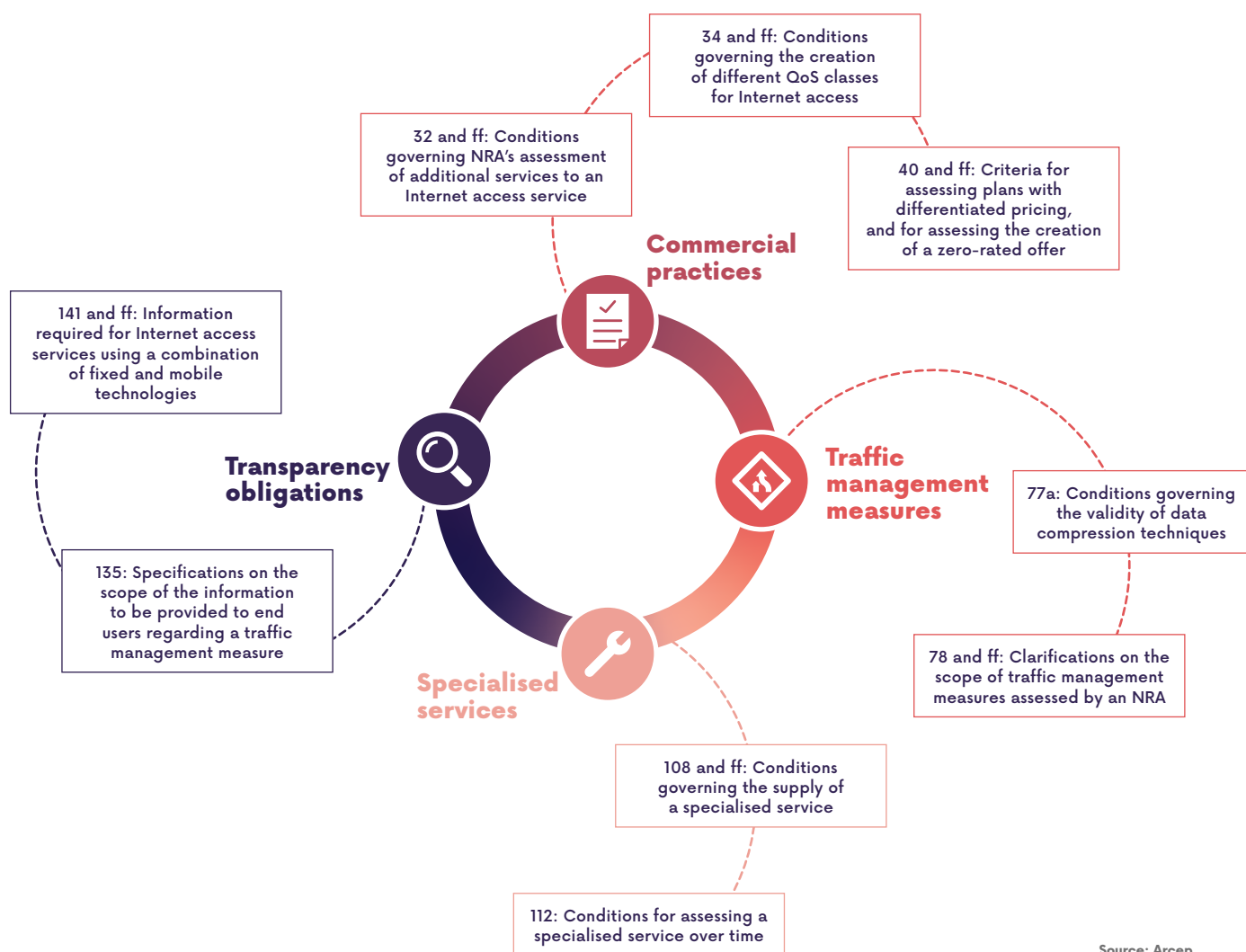
2 Renewed active participation at the European level

In 2020, Arcep and its counterparts actively contributed to finalising the revised guidelines on the Open Internet Regulation. Published on 16 June 2020, these guidelines have kept the same structure as the previous ones, which themselves followed the Open Internet Regulation's structure based on four main themes: commercial practices, traffic management practices, specialised services and transparency obligations. A number of clarifications have been made, notably regarding the analysis of zero-rated offers, the conditions for creating different quality of Internet access services, and the criteria used to analyse specialised services.

Revising the guidelines also provided Arcep and its fellow regulators with an opportunity to discuss Internet service providers' (ISPs)

access to domain names (or URLs) for traffic management or billing purposes. One should bear in mind that the Open Internet Regulation authorises ISPs to access only the information contained in the IP packet's header and the transport layer protocol's header, which therefore precludes them from using information belonging to the specific content⁵. To deepen their knowledge of this topic, on 12 November 2020, Arcep and its European counterparts continued their dialogue with the ecosystem by hosting a virtual workshop via BEREC, devoted to traffic identification mechanisms on networks. Several stakeholders (equipment suppliers, content providers and operators) were given an opportunity to present their views on the issues surrounding traffic identification and pertaining to the Open Internet Regulation's provisions⁶.

MAIN REVISIONS TO THE OPEN INTERNET GUIDELINES



5. For a detailed explanation of the difference between generic and specific content, see page 66 of the 2020 report on the State of the Internet in France.

6. BEREC public virtual workshop on traffic identification - BEREC (europa.eu).

BEREC REPORTS ON NETWORK RESILIENCE IN EUROPE DURING THE COVID-19 CRISIS

- **MARCH 2020**
 - 19 | Joint Statement from the Commission and the BEREC on coping with the increased demand for network connectivity due to the Covid-19 pandemic BoR(20)66
 - 25 | BEREC Summary Report on the status of internet capacity in light of the Covid-19 crisis BoR(20)82
 - 27 | BEREC Summary Report on the status of internet capacity in light of the Covid-19 crisis BoR(20)73
- **APRIL**
 - 01 | BEREC Summary Report on the status of internet capacity in light of the Covid-19 crisis BoR(20)77
 - 03 | BEREC Summary Report on the status of internet capacity in light of the Covid-19 crisis BoR(20)78
 - 08 | BEREC Summary Report on the status of internet capacity in light of the Covid-19 crisis BoR(20)80
 - 15 | BEREC Summary Report on the status of internet capacity in light of the Covid-19 crisis BoR(20)81
 - 17 | BEREC Summary Report on the status of internet capacity in light of the Covid-19 crisis BoR(20)83
 - 22 | BEREC Summary Report on the status of internet capacity in light of the Covid-19 crisis BoR(20)85
 - 24 | BEREC Summary Report on the status of internet capacity in light of the Covid-19 crisis BoR(20)86
 - 29 | BEREC Summary Report on the status of internet capacity in light of the Covid-19 crisis BoR(20)87
- **MAY**
 - 07 | BEREC Summary Report on the status of internet capacity in light of the Covid-19 crisis BoR(20)88
 - 14 | BEREC Summary Report on the status of internet capacity in light of the Covid-19 crisis BoR(20)89
 - 20 | BEREC Summary Report on the status of internet capacity in light of the Covid-19 crisis BoR(20)90
 - 28 | BEREC Summary Report on the status of internet capacity in light of the Covid-19 crisis BoR(20)117
- **JUNE**
 - 04 | BEREC Summary Report on the status of internet capacity in light of the Covid-19 crisis BoR(20)119
 - 11 | BEREC Summary Report on the status of internet capacity in light of the Covid-19 crisis BoR(20)120
 - 18 | BEREC Summary Report on the status of internet capacity in light of the Covid-19 crisis BoR(20)127
 - 25 | BEREC Summary Report on the status of internet capacity in light of the Covid-19 crisis BoR(20)133
- **JULY**
 - 30 | BEREC Summary Report on the status of internet capacity in light of the Covid-19 crisis BoR(20)142
- **AUGUST**
 - 27 | BEREC Summary Report on the status of internet capacity in light of the Covid-19 crisis BoR(20)146
- **SEPTEMBER**
 - 30 | BEREC Summary Report on the status of internet capacity in light of the Covid-19 crisis BoR(20)177
- **OCTOBER**
 - 29 | BEREC Summary Report on the status of internet capacity in light of the Covid-19 crisis BoR(20)202
- **NOVEMBER**
 - 30 | BEREC Summary Report on the status of internet capacity in light of the Covid-19 crisis BoR(20)233
 - 30 | Overview of the Member State experiences related to the regulatory and other measures in light of the Covid-19 crisis BoR(20)234
- **DECEMBER**
 - 17 | BEREC Summary Report on the status of internet capacity in light of the Covid-19 crisis BoR(20)249
- **MARCH 2021**
 - 31 | BEREC Summary Report on the status of internet capacity in light of the Covid-19 crisis BoR(21)58

Source: Arcep

National regulatory authorities (NRAs) also worked closely together on the resilience of networks in Europe during the Covid-19 public health crisis. From the very first weeks, Arcep and its counterparts maintained a bi-weekly, then later monthly, then quarterly report on their national networks' resilience. In addition to this regular reporting, NRAs discussed possible traffic management measures to allow operators to handle the increased demand for connectivity, particularly with the widespread adoption of remote working,

remote medical visits and online learning. BEREC members and the European Commission published a joint statement on 19 March 2020⁷, which offered a reminder that the Open Internet Regulation does include provisions that allow operators to take exceptional traffic management measures to prevent or mitigate the effects of imminent, exceptional or temporary congestion on their network. Ultimately, an increase in traffic did occur on every network in Europe during the Covid crisis, but without any major congestion being observed.



First interpretation from the Court of Justice of the European Union of the net neutrality regulation

In late 2018 and early 2019, the Budapest High Court requested a preliminary ruling from the CJEU on several questions regarding national operator Telenor's zero-rating offers (Cases C-807/18 and C-39/19)¹.

The Hungarian operator was selling plans under which access to certain online services was not deducted from customers' data allowance, and customer's connection to these services was not throttled or blocked once the data cap had been reached. The operator justified this practice by saying that its customers had subscribed to its plans of their own free will, and the ban on discrimination set forth in Article 3.3 of the Open Internet Regulation did therefore not apply. It further argued that an assessment of Article 3.3 would not be possible until after having assessed whether these plans had or not a limiting effect on end users' exercise of their rights, as prohibited under Article 3.2.

In its judgement, the Court of Justice did not side with operator Telenor, and concluded that the continued operation of a zero-rated app after the data cap had been reached – while access to the rest of the Internet is slowed down or blocked, – is incompatible per se with Article 3.3, without requiring the NRA to assess this practice beforehand, with regard to Article 3.2.

If zero-rated pricing practices are not contrary, per se, to the Open Internet Regulation, the Court did stipulate that an operator cannot use contractual freedom and Article 3.2 to justify the implementation of traffic management measures, as described above. By the same decision, the Court specified that a business practice that gives a customer unrestricted access to only certain zero-rated applications is likely to limit the exercise of end users' rights as laid down in Article 3.1.

1. CJEU, 15 September 2020, *Telenor MagyarországZrt./Nemzeti Média-és Hírközlési Hatóság Elnöke*, (joined cases, C-807/18 and C-39/19).

7. Joint Statement from the Commission and the Body of European Regulators for Electronic Communications (BEREC) on coping with the increased demand for network connectivity due to the Covid-19 pandemic.

Open floor to



VÉRONIQUE NEY & KLAUS NIEMINEN

Co-chairs of the Open Internet working group - BEREC

In 2020, National Regulatory Authorities (NRAs) had to deal with the effects of the Covid-19 crisis on the management of Internet Service Providers (ISPs) networks. In a joint statement¹ with the European Commission on 19 March 2020, BEREC committed to a special reporting mechanism to ensure regular monitoring of the internet traffic situation in each Member State in order to be able to respond swiftly to possible capacity issues that could arise from increased internet usage due to emergency Covid-19 measures across the European Union.

In the joint statement, BEREC stated that “pursuant to the [Open Internet] Regulation [(EU) 2015/2120], operators are authorised to apply exceptional traffic management measures, *inter alia*, to prevent impending network congestion and to mitigate the effects of exceptional or temporary network congestion, always under the condition that equivalent categories of traffic are treated equally. This could become relevant, following the confinement measures taken to

address the Covid-19 crisis. Operators can avail themselves of this exception, if such traffic management measures are necessary to solve or to prevent the congestion and they can only be maintained for as long as necessary”. The joint statement lists considerations that operators should take into account in case of impending network congestion. It also calls on operators to closely cooperate with NRAs and to inform them in a timely manner on any measures taken in order to ensure the necessary transparency for individuals and businesses and to enable NRAs to efficiently and effectively perform their monitoring tasks.

Data gathered from European operators indicated that internet traffic increased during the lockdown period. However, this increase in internet traffic did not lead to general network congestion. Since April 2020, traffic volumes began to stabilise and an increasing number of NRAs reduced the frequency of gathering data from operators on the status of their networks.

BEREC, in close cooperation with the BEREC Office², published the first monitoring report on 8 April 2020 and published an update on a weekly basis until the end of June 2020. These reports summarised the status of internet capacity and the actions taken by different NRAs and operators.

Since May 2020, the reports also include information on other measures in the electronic communications sector implemented by NRAs, government bodies and institutions and operators since the outbreak of the pandemic. Between July and December 2020, the reports were released on a monthly basis. As of 2021, the summary reports are issued on a quarterly basis with the next iteration to be expected at the end of June.

All of the reports published by BEREC³ can be found on the BEREC website. 33 NRAs have contributed to the information gathering exercises.

1. https://berec.europa.eu/eng/document_register/subject_matter/berec/others/9236-joint-statement-from-the-commission-and-the-body-of-european-regulators-for-electronic-communications-berec-on-coping-with-the-increased-demand-for-network-connectivity-due-to-the-covid-19-pandemic

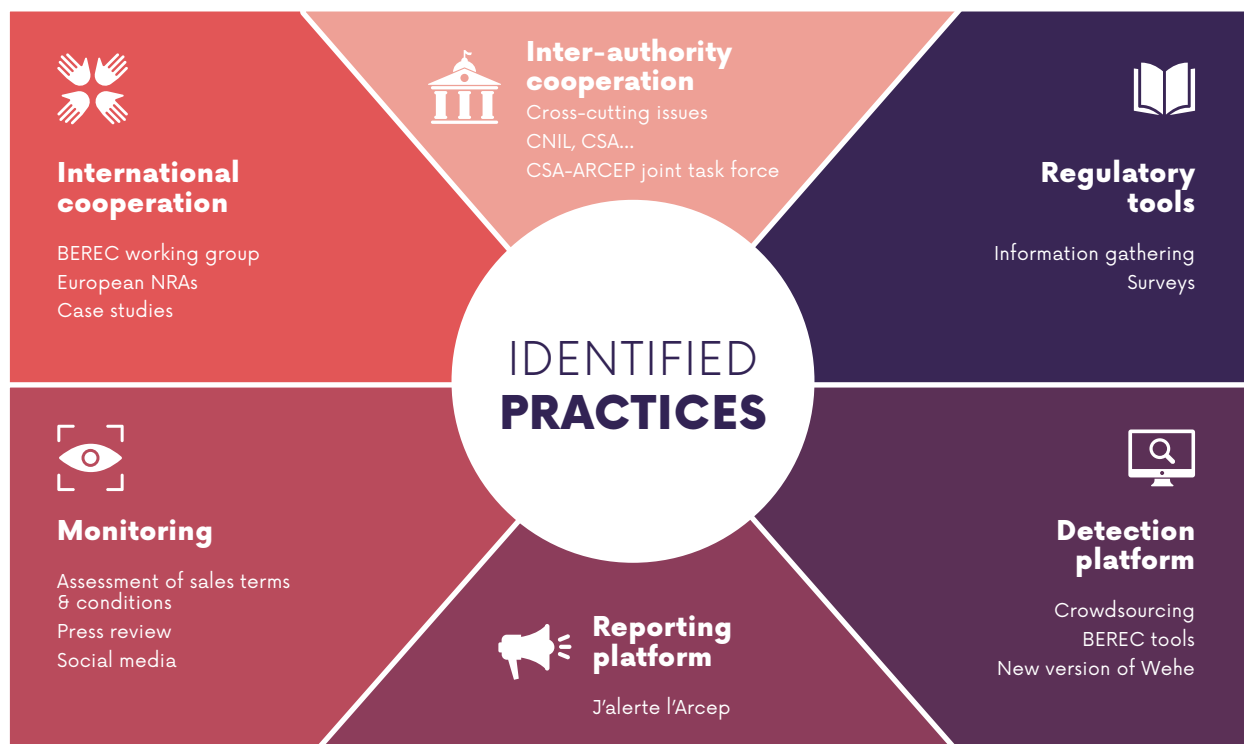
2. The BEREC Office, the Agency for Support for BEREC, was established by Regulation (EU) 2018/1971 of the European Parliament and of the Council of 11 December 2018.

3. For example, the December report is available at https://berec.europa.eu/eng/news_and_publications/whats_new/7877-berec-publishes-an-updated-summary-report-on-the-status-of-internet-capacity

3 An ever-evolving toolkit

To safeguard net neutrality, Arcep has created a toolkit that helps getting 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

As part of the Authority's monitoring responsibilities, Arcep departments review ISPs' terms and conditions of sale on a regular basis. Arcep continued its monitoring work in 2020, in particular regarding the Internet access plans provided by French overseas operators.

As an adjunct to this work, Arcep also has regulatory tools that help gather information from ISPs on their network management rules.

In late 2017, the "J'alerte l'Arcep" online alert platform was added to the Authority's toolkit. In 2020, 304 net neutrality-related reports were filed on the "J'alerte l'Arcep" website. These users reports in turn enabled Arcep to identify possible net neutrality infringements rapidly, and to encourage a swift resolution of the problems detailed in the next section.

Last year, Arcep also continued to work closely with fellow regulatory authorities in France, and notably French Broadcasting Authority, CSA, with which it formed a common task force in late 2020. Cooperation between national authorities allows to combine each other's own particular expertise, and thereby achieve a deeper, more detailed regulatory analysis of common and cross-cutting issues.

Cooperation between NRAs also increased at the European level in 2020, particularly because of the Covid-19 crisis. Arcep and its counterparts held a series of discussions within the BEREC, in particular regarding the resilience of their networks in Europe. At the same time, Arcep strengthened its cooperation with several national regulatory authorities through bilateral discussions on particular case studies, which helped better understand national cases that are similar to those encountered by its fellow NRAs.

DIFFERENT MEDIA SERVICES TESTED BY WEHE



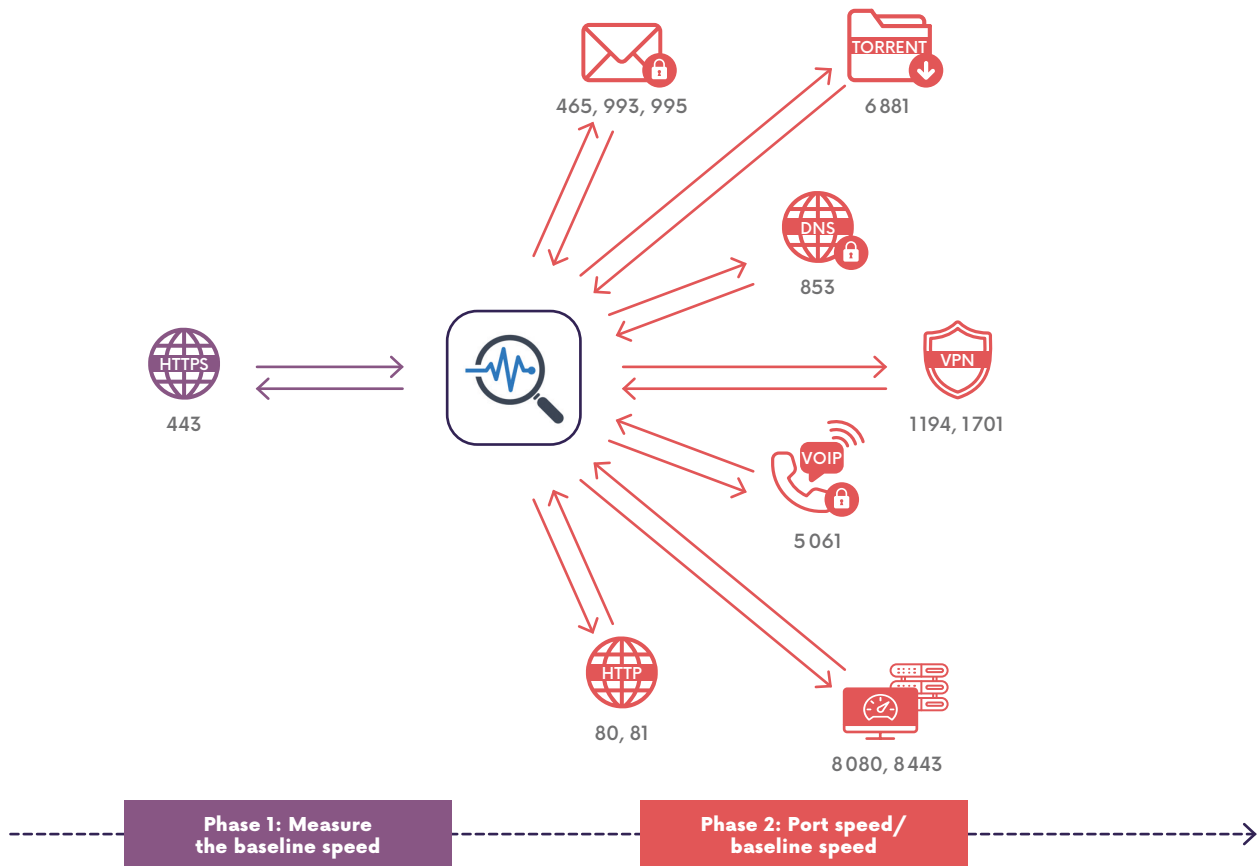
Source: Arcep

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 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 updating work on Wehe, whose new 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.

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.

HOW WEHE'S PORT TESTING WORKS



Source: Arcep

Open floor to



DAVID CHOFFNES

Associate Professor- Northeastern University

THE LAUNCH OF A SIGNIFICANT UPDATE OF WEHE IN 2020

The Wehe app, which allows users to run tests from their mobile devices to identify net neutrality violations, has seen a number of big improvements over the past year as part of our collaboration with Arcep. The most notable differences entail *what* net neutrality violations are tested and *how* we test for them.

In terms of *what* we test, we included new apps to test (including videoconferencing apps, given their popularity during the pandemic) and ones that are more popular in France than in the rest of the world. These tests check whether an Internet provider is giving certain apps better or worse performance based on the data they exchange with servers.

We also deployed a new type of test---one that looks for changes in performance based on the port number used by applications (e.g., port 80 for HTTP, port 443 for HTTPS). Port-based tests required us to address new challenges, since unlike content-based tests, it is not clear which ports should be considered as a “control” for which traffic should be left unchanged by an Internet provider. To solve this problem, we used port 443 (HTTPS) traffic as a *baseline*. It may be prioritized or deprioritized relative to other traffic, so we simply show users the performance of network traffic for each port *relative*

to the performance of port 443. Another challenge we encountered is that some Internet providers block network traffic that is unexpected (e.g., sending HTTPS traffic on ports other than 443), presumably for security reasons. We adapted our tests to account for such cases. There were a number of other challenges, such as determining how much data to send during a test, and what thresholds to use for detecting a net neutrality violation. Through close collaboration with Arcep and access to servers inside of France, we were eventually able to address these issues.

Over the past year, the Wehe team also completed a deployment of Wehe servers to Measurement Lab (M-Lab), which provides access to hundreds of servers around the world. This deployment also raised a number of challenges, such as changing the Wehe apps and server software to be compatible with the new environment, protecting user privacy by ensuring minimal data collection from the platform, and configuring those new server resources so that they could handle the load from many concurrent users. There were several bumps along the way, but the deployment of Wehe to M-Lab has been a success. Note we still use servers outside of M-Lab, to ensure our tests aren’t blind to any

differentiation based on which cloud servers run our server software.

Our team also worked on improvements to reliability and usability for our Android and iOS apps. This included fixing bugs and crashes, improving translations, and providing more information about the status of each test that a user runs. We also added a button to alert Arcep about any observed differentiation that might indicate a net neutrality violation. We continue to work on improving the reliability and interpretability of our app, and we thank all our users and partners at Arcep for their patience and bug reports that help to make the app work better.

Looking back, Wehe users have collectively run nearly 2 million tests for net neutrality since 2018, providing policymakers, regulators, and average citizens with the data they need to understand deployed differentiation practices. Going forward, we expect to provide support for stakeholders to understand compliance with local regulations, continue to make our data and analysis publicly available to guide future protections for net neutrality, and work with all parties to help preserve a free and open Internet that supports the kind of innovation and fairness that underlies its enormous positive impact on the world.

4 Status report on observed practices

In 2019, the competent Arcep body began examining whether all of the Internet plans being marketed in France's overseas departments were net neutrality compliant. In 2020, Arcep contacted all of the overseas operators to draft a status report on this issue. There were several exchanges during the year, particularly on the general terms and conditions of some mobile Internet access plans. Ultimately, most of the points raised were not technically implemented according to the questioned operators. These clauses were therefore rectified following discussions with Arcep departments. A proactive dialogue with Arcep departments is still ongoing with two operators, however, one of which is amending its plans and practices to better align with the Open Internet Regulation.

Arcep also paid close attention to the reports it received from users regarding possible infringements of the net neutrality principle, via the "J'alerte l'Arcep" platform in particular. These reports led Arcep to examine the issue of port blocking – as online services and applications are accessed through ports, and blocking them means blocking access to the service. Arcep thus passed users' issues along to the identified operators, one of which has already altered its existing mechanisms, while the other is exploring possible solutions to continue to provide equal treatment to all of the traffic on those ports.

In 2019, Arcep also focused its attention on Wi-Fi offers on trains. Offered to passengers, these Internet access plans, which are also considered to be publicly available, are subject to the provisions of the Open Internet Regulation. In their dialogue with the national railway company, SNCF, Arcep departments continued to examine on-board offers (technical discussions, conducting tests, etc.) over the past year. Arcep's departments are thus carrying through on the work that had already begun, and counting on future commitments from the SNCF to ensure compliance with the Open Internet Regulation.

Lastly, Arcep began updating its knowledge of how video on demand (VoD⁸) services work. The aim is to gain a deeper understanding of VoD services' operations and their technical constraints and eventually to analyse operators' practices in light of VoD's technological development. To this end, Arcep departments will begin a dialogue with all the ecosystem players who contribute to the VoD market in France, including telecoms operators, VoD content providers, web hosting companies that market video content storage solutions, and linear and catch-up video content providers. Arcep also invites any stakeholder interested in this issue to get in touch with the Authority's departments.

8. See Lexicon.

Open floor to



THOMAS SCHREIBER

Member of net neutrality team – RTR¹

PROVISION OF APPLICATIONS AND SERVICES: AUSTRIA'S REGULATOR ENFORCING THE RIGHT TO A PUBLIC IPv4 ADDRESS

The European Open Internet Regulation (Regulation [EU] 2015/2120) envisions a truly open internet: An internet, where not only a few content providers and many content consumers take part, but rather an internet, where every end-user can be both – content creator and consumer with very low access barriers.

This is enshrined in Art. 3(1) of the Open Internet Regulation, which grants end-users not only the *right to access information and content of their choice*, but also to *provide applications and services* for others to access. Such services range from smart home appliances for personal use (e.g. temperature monitoring), include filesharing with Network Attached Storage (NAS), to web servers operated by end users for third parties.

A key prerequisite for self-hosting of services is direct accessibility of the service operated by the end-user from the public internet. In technical terms, the end-user needs to be assigned a public IP address which can then be used to identify the servers hosting the service. In analogy to telephone networks, this would be comparable with the prerequisite for a telephone number in order for an end-user to be reached by others.

While a public IP address used to be assigned by default, today, in mobile networks in particular end-users are frequently assigned private IP addresses (using a technology called *Network Address Translation* [NAT]).

Apart from technical aspects, reasons for this include ISP's interest in keeping public addresses in reserve, since – as with IPv4 – these are becoming scarce. However, if multiple customers are required to share a single private IP address via NAT, this effectively prohibits any individual customer from providing services or content themselves. While some technologies, in particular IPv6, can solve some use-cases, e.g. allowing end-users to access own appliances via IPv6 addresses, solely providing a public IPv6 address is – at this point in time – not seen as sufficient, as large parts of the internet do not yet possess IPv6 connectivity. On the other hand virtually all of today's internet allows IPv4 connectivity.

Based on these aspects, Austria's regulatory authority interprets Art. 3(1) of the Open Internet Regulation as entitling end users to a free public, at least dynamic, IPv4 address, if the end-user requests such an address, for example because of wishing to offer services. The end-user can then utilize that address with dynamic DNS services to allow routing to their own services. Accordingly, any agreement concerning the levying of an additional fee represents a restriction to the rights of the end-user. In order to allow somewhat stable connections, ISPs are also banned to disconnect end-users daily, only allowing short disconnections at most once in 30 days.

A supervisory procedure against the Austrian incumbent regarding a product, that offered a public IPv4 upon request only at additional cost was already initiated in 2016. A formal decision was taken in late 2017, banning the ISP from charging an additional fee for a dynamic public IPv4 address and obligating it to pay back some of the fees already charged. In the same decision, the ISP also was instructed to disconnect end-users at most once every 30 days. While the ISP appealed the decision, a suspensory effect was denied by the petitioned administrative court, allowing the enforcement of the decision in 2018. In mid-2020, the administrative court (BVwG) then rejected the ISP's appeal and confirmed the decision of Austria's regulatory authority. The decision is not final yet.

Since 2018, Austria's regulatory authority is enforcing the right to a public, at least dynamic, IPv4 address with all Austrian ISPs, regardless of their size. As only some end-users request such a public IPv4 address, implementing this requirement, in our experience, was possible also for "new players" after informal talks and did not yet lead to any further formal decisions.

More information on this and other topics concerning Net Neutrality in Austria can be found on RTR's website: <https://www.rtr.at/nr>

1. Austrian Regulatory Authority for Broadcasting and Telecommunications.

PLATFORMS: INTERNET ACCESS GATEKEEPERS

What you need to know

There was a real shift in the focus of debates

in 2020:

the central question is no longer whether digital industry players are the root cause of certain problems, but rather how to solve those problems.

Around the world, a range of proposals were made for introducing *ex ante* economic regulation of Big Tech companies. In Europe, the European Commission published the Digital Markets Act

on 15 December 2020.

The Commission's proposal

marks a major step forward, but warrants being strengthened in several respects, notably with the addition of more proactive tools for the regulator.

The European Open Internet Regulation enshrines users' right to access and distribute information and content online. But it applies solely to ISPs, which are only one link in the internet access chain. Located at the end of this chain, devices (smartphones, voice assistants, connected cars...) and gatekeeper platforms' closed ecosystems have proven to be the weak links in achieving an open internet.

Arcep shared this conclusion in its 2018 report¹. The brief published in December 2019² extended this examination to the operators of the most powerful (aka gatekeeper) platforms, and marked an expansion of the Authority's scope of analysis. The brief reiterated the conclusion that a small number of companies had become the gatekeepers of citizens' and businesses' digital lives, by concentrating power over many of the services that have become an integral part of all of our daily lives. These players are now in a position to determine which content and services will be made available online, and the conditions under which users can access them. This concentrated control over a great many services has also involved the creation of closed ecosystems within which users have now become captive, automatically hampering their freedom of choice. Which is how these ecosystems have proven to be weak links in achieving an open internet.

While 2019 had been marked by a growing number of regulatory issues surrounding these ecosystems, 2020 saw a real sea-change in the debates: no longer wondering whether these players are causing problems, but rather how to solve those problems. One of the Commission's key conclusions is that the current regulatory framework does not allow it to do so: the Commission's enforcement of European Competition Law (Articles 101 and 102 of the TFEU) requires particularly lengthy procedures, which can give the undertakings in question time to lock in their market positions irrevocably³. In addition, the Commission's enforcement of antitrust rules can only take place *ex post* i.e. after a competition problem has emerged. As stated in a recent report from the European Court of Auditors⁴ (ECA), "*Particularly in the digital economy, this may be too late to tackle a competition problem*". The ECA report also stresses that "*outside merger control, the Commission has currently no tools in its hands that would allow it to intervene ex ante i.e. before competition problems would occur*". The European Commission thus seized the platform regulation issue by holding two public consultations, which resulted in two bills that were published on 15 December 2020. Through the Digital Services Act, the Commission is proposing to review the e-commerce Directive of 2000, and particularly the liability provisions governing hosted content, which apply to technical intermediaries.

1. https://en.arcep.fr/uploads/tx_gspublication/rapport-terminaux-fev2018-ENG.pdf

2. https://www.arcep.fr/uploads/tx_gspublication/plateformes-numeriques-structurantes-caracterisation_reflexion_dec2019.pdf

3. In its impact study, the Commission states: "*Moreover, – even when using interim measures (...) – competition law enforcement requires a detailed economic and legal analysis which, jointly with the procedural safeguards, bring the duration of the investigations to at least around two years and usually more than that. In markets characterised by powerful network effects and economies of scope, competition law interventions may mean not only delays in the interventions but also that irreparable effects such as tipping may no longer be reversible*".

4. European Court of Auditors, Special Report 24/2020: EU audit report: merger control and antitrust proceedings, 19 November 2020, paragraph 59.

This provision seeks to achieve broader guarantees of the best conditions for providing innovative digital services in the internal market, increase online security and safeguard fundamental rights. The Commission intends to use the Digital Markets Act (See inset below), to introduce *ex ante* economic regulation of Big Tech companies, aka the internet's gatekeepers⁵.

1 Developments observed in the marketplace

There was no shortage of headline news on this issue in 2020. A number of complaints filed against digital market players were also referred to regulatory authorities. The US Department of Justice's (DoJ) antitrust division, followed by a coalition of several US states, filed a lawsuit against Google in October 2020, alleging abuse of its dominant position in the search services market, notably through what were considered anticompetitive agreements signed with mobile handset makers, and mobile operators.

After having fined Google three times between 2017 and 2019, the European Commission also opened investigations into:

- Facebook and Google's data collection practices,
- Apple's app store policies,
- The terms and conditions of Apple's Apple Pay mobile wallet, and its limitation of access to the NFC chip,
- And the access conditions for Amazon's Buy Box⁶ for third-party marketplace vendors.
- Several similar investigations are underway in Australia, the UK and at the national level in several European countries (Germany, Italy, France).

App developers recently created a coalition called⁷ the "Coalition for App Fairness"⁸ to defend their grievances with Apple. They have highlighted three main Apple practices that they deem problematic: the 30% commission on sales on the App Store, the limits placed on users' freedom of choice, and the fact that the company gives preferential treatment to its own products and features in what is made available to users.

Lastly, an example of the impact of locking in users through a "network effect" was observed when users attempted to switch to Signal or Telegram after WhatsApp changed its terms of use⁹. A great many of them complained about being forced to keep a WhatsApp account to be able to continue to communicate with some of their contacts, or of being unable to recover their conversation history, notably due a lack of interoperability between messaging apps.



The Digital Markets Act

On 15 December 2020, the European Commission published a proposed regulation called the Digital Markets Act (DMA) whose aim is to introduce economic regulation of the largest technology companies. The DMA's stated objectives are to make digital markets open and fair, and to harmonise the legal framework across Europe.

The proposal seeks to designate companies that are qualified as gatekeepers, and list the obligations that apply to these undertakings. The Commission has concluded that it has become vital to apply asymmetric regulation to these gatekeepers, using mechanisms that it is working to make as "automatic" and efficient as possible, while including the ability to evolve over time. These mechanisms are chiefly made up of two types of obligation and prohibited practices, with which these gatekeepers must comply: a list that does not require any specification (e.g. they cannot link registrations to several services), and a list whose terms of implementation may be specified by the Commission if the terms offered by the gatekeeper are not satisfactory (e.g. the obligation to provide data portability).

To a large extent, these developments echo the recommendations that Arcep has set forth since 2018, particularly in the fact that they target the largest, most influential platforms, including operating systems, whose many limitations on users' freedom of choice have been documented¹. The Commission's proposal nevertheless warrants being strengthened in several areas (See dedicated section at the end of this chapter).

1. Arcep report, "Smartphones, tablets, voice assistants: devices, the weak link to achieving an Open Internet" (February 2018).

5. This notion is very similar to the concept used by the Authority of structural digital platform operators.

6. This is the "buy" button displayed for certain products on Amazon that allows shoppers to add products from certain sellers directly into their shopping carts. This feature is only enabled for certain vendors under certain conditions. For vendors, having this button on their products is crucial to their sales.

7. Spotify, Epic, and Tile, which had already made public statements criticising Apple's practices, are all members of the coalition.

8. <https://appfairness.org/>

9. <https://9to5mac.com/2021/01/06/whatsapp-share-your-data-with-facebook/>

2 Progress made in the Authority's work

Arcep continued its monitoring and communication work throughout 2020, in partnership with a wide range of stakeholders. The Authority updated its "J'alerte l'Arcep" reporting platform in November by opening it up to new groups of users, namely developers, and to new issues, such as device openness. App developers can now use a dedicated input box on "J'alerte l'Arcep", in the same way as local authorities, businesses and individuals. They can report any problems to Arcep that they have encountered with device manufacturers', operating systems' (OS), search engines' or app stores' tools or services. Arcep plans to draw on these reports, and developers' experience, to deepen its knowledge of this ecosystem. Developers' reports can pertain to a range of concrete incidents, such as:

- "The APIs I use change routinely for no apparent reason";
- "The app store refuses to carry my application";
- "The operating system does not inform me, or does not inform me with enough lead time of updates".

Naturally, these concrete cases are only sample categories provided by Arcep to make it easier to process the reports. App developers are free to report any other kind of issue to the Authority.

Arcep also contributed¹⁰ to the European Commission's public consultation on the Digital Services Act¹¹. The Authority called on the European Union to adopt *ex ante* regulation of gatekeeper platforms, and thereby make the internet once again an area of freedom of choice and freedom to innovate. Attached to this contribution was a memo on the remedies that could be used to regulate these platforms. This "toolbox" draws its inspiration from the approach that has been successfully applied to the telecoms sector for decades, notably thanks to tailored case-by-case remedies and dispute settlement measures.

3 Progress in the work being done in France

In France, national authorities set up the Digital regulation expertise hub/*Pôle d'expertise de la régulation numérique* (PEReN) that lends its expert assessment and technical assistance to federal government departments and authorities involved in regulating digital platforms. The group's purview is national in scope and, to this end, will include some 20 data scientists and IT and algorithm experts. Arcep and PEReN will meet on a regular basis, and have already identified several avenues of investigation for 2021. The Task Force created in March 2020¹², of which Arcep is a member, will continue to work on drafting French positions. This inter-ministerial Task Force¹³ provides investigative briefs to help in drafting arguments on the opportunity for and ways to regulate digital platforms.

4 Progress in the work being done in Europe

In Europe, several legislative proposals have been made alongside the Commission's. In December, the UK announced¹⁴ that it was implementing a new regulatory framework for a selection of digital industry players. A dedicated team was created to this end within the country's Competition and Markets Authority. The goals set by this new Digital Markets Unit include:

(i) to protect consumers' and citizens' interests, (ii) to be a centre of expertise on digital markets, (iii) to oversee digital firms with Strategic Market Status (SMS)¹⁵. In addition to the mechanism for designating these SMS companies, the regulatory framework will have three priority areas of focus:

- Codes of conduct: a set of clear principles designed to guarantee fairness for consumers and enterprises, and to protect competitors from practices that could undermine fair competition. The aim of these codes of conduct is to prevent and reduce the unwanted effects caused by significant market power.
- Pro-competitive interventions, such as personal data portability, interoperability, access to data that can foster more competition and innovation. The purpose of these interventions is to instil long-lasting change by altering the way the market is organised, and increase contestability from the roots on up.
- Specific rules for corporate mergers involving SMS companies, to enable stricter control over transactions.

10. <https://www.arcep.fr/actualites/les-communiqués-de-presse/detail/n/regulation-du-numerique-1.html>

11. The European Commission ultimately divided the Digital Services Act into two different texts. The section to which Arcep contributed is now included in the Digital Markets Act.

12. <https://www.entreprises.gouv.fr/fr/actualites/numerique/politique-numerique/la-regulation-des-plateformes-numeriques>

13. https://www.youtube.com/watch?v=XwvmLTf7m_w

14. <https://www.gov.uk/government/news/cma-advises-government-on-new-regulatory-regime-for-tech-giants>

15. This notion aligns largely with that of 'gatekeepers' used by the European Commission and what Arcep has referred to as structural digital platforms.

In early 2021, Germany also passed a law that allows the country's competition authority, the Bundeskartellamt, to designate a list of “*undertakings of paramount significance for competition across markets*”. These undertakings will be required to comply with a set of rules, including being prohibited from giving preferential treatment to their own services, or impeding interoperability with other services.

BEREC also published its opinion¹⁶ on the Digital Markets Act in March 2021, to which Arcep was an active contributor. BEREC strongly supports the European Commission's initiative to implement asymmetric *ex ante* regulation. The Body of European Regulators for Electronic Communications nevertheless believes the proposal is too backwards-looking, content with basing its work on a collection of competition authority decisions, and instead proposes adopting a more flexible framework by:

- Completing directly applicable obligations with additional remedies that could be tailored on a case-by-case basis to be fit for purpose.
- Strengthening cooperation with independent national authorities for the supervision and application of the DMA, and to reduce strong information asymmetries.

Another body that scrutinised the European Commission's proposal was the *Centre on Regulation in Europe* (CERRE). In November 2020, CERRE presented a compendium¹⁷ of all of its work on digital regulation. The institution warmly welcomed the European Commission proposal, and is continuing its own work on making concrete proposals, notably for improving application of the text. CERRE is of the opinion that the proposed regulation needs to be more flexible and dynamic, e.g. by creating the ability to have individually tailored remedies. The institution also proposes involving all of the stakeholders in the process of drafting and monitoring remedies, particularly third parties which are supposed to benefit from them.

5 Status of the work being done in the United States

In the United States, a report¹⁸ from the House of Representatives' Antitrust Subcommittee marked a turning point in debates over updating the country's antitrust policies, and a gradual change in the its Big Tech doctrine. While, up until then, the United States had adopted a “*laissez-faire*” policy, the growing number of antitrust lawsuits¹⁹ constituted an unprecedented offensive on digital sector giants, which could go as far as imposing (at least functional) separations of certain businesses.

16. https://berec.europa.eu/eng/document_register/subject_matter/berec/opinions/9879-berec-opinion-on-the-european-commissions-proposal-for-a-digital-markets-act

17. <https://cerre.eu/events/new-perspectives-on-digital-regulation-and-competition-policy/>

18. <https://www.reuters.com/article/us-usa-tech-antitrust-idUSKBN26R2V6>

19. Google, Apple and Facebook are among the targets of the ongoing lawsuits.

STRENGTHEN THE DMA TO ENSURE AN OPEN DIGITAL ECOSYSTEM THAT WILL BENEFIT EUROPE'S CITIZENS AND BUSINESSES

Arcep welcomes the proposed “Digital Markets Act” that focuses on the internet’s gatekeepers, and is open to being completed by proposals designed to make it more efficient, and better achieve its objective of an open digital ecosystem that benefits European citizens and businesses.

The internet developed as a common good. It was designed as an open network for everyone, such that no public or private institution could impede its evolution. This enabled the emergence of digital services that genuinely improved how the internet, and society in general operated. Despite which, it is now an accepted fact that a small handful of large and powerful platforms (including certain search engines, social networks and operating systems) **have become the internet’s gatekeepers, and now control and decide if and how users can access and share online content and services.** Under certain circumstances, even if they do continue to innovate, they have the power to hamper competition and innovation across the entire digital sector, and in turn restrict users’ freedom of choice and freedom of expression. This possible negative impact on citizens’ best interests, and consumers’ well-being, can no longer be ignored. It is thus crucial to **ensure that digital infrastructures develop as a common good, and to safeguard the internet’s original “generative”¹ dimension, in other words, the capacity for every user to contribute, unhindered, to enriching and helping it to thrive.** This capacity is guaranteed, notably by the internet’s decentralised architecture. Given this state of affairs, the proposed Digital Markets Act (DMA) **that seeks to ensuring digital markets’ contestability and fairness**, published by Commission on 15 December 2020, was a welcome milestone, and one that testifies to a digital Europe working to remain true to its values.

Arcep has been calling for the introduction of an agile and asymmetric *ex ante* regulatory framework for several years now. Here, the DMA, which targets **the most influential gatekeepers**, including operating systems², marks an important and commendable step forward. The Commission’s proposal will, however, only be effective and meet its objectives – in particular to **foster and unleash innovation** – if it is fortified in several respects, to consider the potential problems these undertakings pose from every angle, to be able to craft more targeted responses, and ensure they are genuinely effective.

As such, the regulator needs to be equipped with new dynamic tools that give it the ability to better anticipate issues, and to strengthen the resources it is allocated to ensure its *ex ante* intervention can be implemented effectively. This will include strengthening the process of **monitoring these gatekeepers to reduce information asymmetry and**, alongside the obligations set in advance and which apply to every player, to plan for **tailored remedies that are more suitable than a one size fits all solution.** These are among the key assets of *ex ante* regulation, which has proven its effectiveness.

Also, increased cooperation between the Commission and Member States could make the system more efficient, and provide critical resources and support mechanisms.

Lastly, it seems particularly necessary to better consider the ecosystemic dimension of certain undertakings who may be the root cause of market failures, with a view to improving competition conditions, including between platforms themselves. This would create the ability to take fuller account and foster the freedom of choice of end users who, today, can be captive to a centralised ecosystem, i.e. a set of products, services³ or computer hardware that interact with one another⁴, and end up locking in their users.

01. Certain complementary mechanisms and courses of action, drawing on twenty years of experience in opening up the telecoms sector to competition, would make the DMA more effective

The means put in place by the Commission will not be enough to guarantee its effectiveness. Although the proposal includes solutions to a number of problems that have been identified thus far, it puts the Commission in a position of playing catch-up with the gatekeepers, particularly as the DMA provides for only a single *a posteriori* rectification for a failure to apply the text, and the problems that will continue to arise: it leaves it up to the gatekeepers to

1. Jonathan L. Zittrain, *The Future of the Internet, And How to Stop It*, Yale University Press & Penguin UK, 2008, page 70: “Generativity is a system’s capacity to produce unanticipated change through unfiltered contributions from broad and varied audiences”.

2. Arcep report, “Smartphones, tablets, voice assistants: devices, the weak link to achieving an Open Internet” (February 2018).

3. E.g. applications, operating systems, online platforms...

4. Definition inspired from OECD (2019), *An Introduction to Online Platforms and Their Role in the Digital Transformation*, OECD Editions, Paris, page 22, <https://doi.org/10.1787/53e5f593-en>

decide first how to comply with the overall obligations to which they are subject. Added to which, undertakings that depend on or compete with those platforms have no way to voice their concerns if they encounter problems in their relationship with these gatekeepers.

To enable the regulator to take action in a timely and useful fashion, and to adapt to the practices of a sector in a state of constant flux, **the DMA should include tools, mechanisms and means of action needed to implement the asymmetric ex ante regulation they are drafting rapidly and efficiently**, and to achieve their stated objectives. The proposal does not provide enough flexibility or room to tackle situations on a case-by-case basis, which would allow the regulator to take disparities in situations and the different enterprises' business models into account. As it stands, the text also makes it impossible to compete with the resources of the undertakings to be regulated, whether in terms of the technicity of the issues being examined, exploitation of informational advantages (obtained from the large information asymmetries), or the creativity of possible attempts to circumvent regulatory restrictions. As a result, several familiar *ex ante* regulatory tools could be proposed.

- **First**, as an adjunct to the obligations set forth in Articles 5 and 6, the proposal should provide for a **tailored remediation mechanism**, to define remedies that are specific to each gatekeeper or type of service, following an in-depth analysis of the effects of the planned measures, to be able to tackle the unanticipated cases in the two lists of obligations in a proportionate fashion (e.g. non-discrimination obligations, targeted fair access, or a separation of certain services or data). The current mechanism is rigid and confining, so potentially easy to circumvent by developing new practices, particularly for certain measures, such as data portability, that have a highly technical dimension. By taking into account the particular features of the undertaking in question, tailored remedies allow the regulator to specify directly the way in which an obligation can be applied, thereby discouraging the regulated undertaking from any attempt at circumvention, and reducing the need for additional intervention and, ultimately, for over-regulation.
- **Second**, it seems vital to instil and maintain a **dialogue that includes all of the stakeholders**, and not just the gatekeepers as the text currently proposes. Consultation (formal, according to procedure, or informal for steady monitoring – cf. monitoring mechanisms below) with those undertakings that are supposed to benefit from the imposition of these obligations (gatekeeper platforms' competitors, business users and, in some cases, consumers and civil society...) will help ensure the creation of effective remedies, and the ability to anticipate nascent issues.
- **Third**, **monitoring** changes in the digital environment – for instance by asking the Commission to establish a list of indicators to be collected periodically from the undertakings – would allow the Commission to **gain technical-economic expertise and reduce the sizeable information asymmetry that exists between**

the regulator and the regulated. This monitoring could help fuel a data-driven regulation mechanism, which would itself also reduce the information asymmetry between platforms and their users, and help steer the market towards serving the greater good.

- **Fourth**, the introduction of a **dispute settlement** mechanism to complete the regulator's toolbox would allow an undertaking that is unable to reach an agreement with a gatekeeper, or that considers itself aggrieved by the obligations imposed by a gatekeeper, can appeal to the regulator to find an operational solution rapidly. This could cover a wide variety of issues (notably access to app stores, the operational implications of technical remedies such as portability) and to clarify the regulatory framework with respect to these practices, outside of any system of punitive measures.
- **Lastly**, the proposed regulatory framework should not scrimp on human or technical resources. The Commission proposes assigning 80 agents to the task. By way of comparison, authorities in the UK plan on having a staff of 300 assigned to an initiative similar to the Digital Markets Act.

Rooted in twenty years' experience in regulating the electronic communications sector, these proposed measures would help shore up the current proposal. While it would not make sense to merely transpose the current framework that governs electronic communications to the internet's gatekeepers, the Digital Market Act would gain from mining the elements and principles from that framework that give it its flexibility, its adaptability and its efficiency, through rapid, proportionate and justified intervention.

02. Strengthening the cooperation mechanism with Member States would foster greater proximity, especially with the smaller businesses that are the beneficiaries of the new provisions

Some of the provisions that seek to achieve more efficient application of the regulation would benefit from **stronger cooperation between the Commission and national regulatory authorities**, which would create a support system at the national level. As it stands, only a single mechanism includes cooperation, by having Member States be part of a Committee that issues advisory opinions prior to the Commission's adoption of implementing acts. This procedure gives Member States the ability to exercise a relative institutional countervailing power on the Commission's implementing acts. However, although it allows for this interaction, its goal is not to enshrine a true cooperation mechanism, and even less to create a system for providing feedback from the field.

If the regulated undertakings have an international dimension, a large percentage of the beneficiaries of the obligations will be small businesses or users who are active at the national level. It therefore seems that a role could be created at this scale to monitor the sector's evolution, to

verify the efficiency of the measures put into place, report back, settle certain disputes at the national level and, in more general fashion, serve as interlocutor for smaller undertakings who are in a highly asymmetric position compared to gatekeepers, and may be reticent to appeal directly to the Commission.

The DMA could provide for the creation of an independent group made up of independent National Authorities who would advise the European Commission, by bringing their technical expertise and knowledge of the situations, and so help render the regulation's application more effective, which would benefit businesses, consumers and society alike. This group could coordinate NRAs' future actions at the national level.

03. Scope of the proposal is relevant, but not sufficiently focused on opening up ecosystems for users' benefit

The Commission's choice of taking an asymmetric approach, which focuses on actions targeting the internet's gatekeepers, including operating systems and devices, is timely and warrants both praise and support. The proposal's scope of application seems relevant overall, barring certain services which, because they raise similar issues, warrant clarification on their inclusion, especially web browsers and voice assistants.

Although this marks a significant step forward, and the types of undertaking have been clearly identified, it could nevertheless be a more ambitious regulation, if the goal is to make digital markets truly fair and contestable, in a way that benefits everyone. The proposal is effectively focused chiefly on the relationships between the gatekeepers and the business users that depend on their services. It could be completed by **taking fuller account of the targeted undertakings' ecosystemic dimension, to:**

- Promote competition between the platforms themselves

The current proposal focuses on provisions that seek to guarantee that, when competitors are hosted by a vertically integrated platform, the downstream market will be driven by a state of fair competition. Although some obligations seek to reduce barriers to entry, and address lock-in effects, the proposal would be enhanced by containing more measures designed to challenge the centralised ecosystems

that have developed and are being maintained thanks to powerful economies of scale effects, network effects and leverage. The goal is to limit business users' dependence on gatekeepers by enabling the **emergence of alternative players**. For instance, if we welcome the introduction of a data portability obligation that is likely to solve some of the lock-in effects, the planned obligations do not challenge the de facto gains that are earned from capitalising on network effects, something that **true "horizontal" interoperability**⁵ would solve, under certain circumstances.

- Guarantee end users' interests

Fostering competition is naturally beneficial to consumers, but competition alone cannot ensure that all of end users' interests are being protected. The goals of guaranteeing European citizens' freedom of choice and an open internet⁶ could therefore be more fully incorporated by expanding the regulation's objectives beyond protecting only business users' interests, even if they do benefit end users indirectly. Some obligations that benefit end users directly⁷, notably transparency and interoperability, could therefore be added (in a targeted and proportionate fashion, *cf.* Part 2) and the scope of cases that justify the regulator's intervention⁸ could be expanded. For instance, services that have no or very few business customers, as defined by the proposal, would not be subject to the planned regulation. Some of them, however, undeniably constitute checkpoints in accessing and sharing online content and information for end users⁹. Finally, it seems vital to take fuller account of these players' and their business models' ecosystemic dimension – which leads to users being kept inside a closed environment – and of the effects they generate. This could be accomplished with the strengthening proposals explored in Part 2.

The Commission's proposal marks a major step towards achieving more open digital ecosystems in the European Union and beyond. To solidify its guarantees both more broadly and more effectively, Arcep invites European co-legislators to strengthen this proposal by giving it the flexibility it needs – making the proposed remedies more proportionate, effective and rapid, and more easily tailored to the variety of situations that arise, both today and tomorrow – and by capitalising on the support of Member States, especially so that they might better incorporate certain undertakings' ecosystemic characteristics, and give European citizens greater freedom of choice in their access to digital services.

5. Competing systems' (such as social networks) capacity to enable communication between their end users.

6. In addition to the network layer, which is already covered by the Open Internet regulation.

7. In particular by strengthening their ability to "multi-home" i.e. users' ability to use several competing platforms at once.

8. i.e. to mobilise already identified obligations to meet complementary objectives, notably when the Commission stipulates the conditions for implementing obligations via the mechanism provided for in Article 7.

9. E.g. cloud-based services and certain major instant messaging services whose clientele is made up largely of non-business customers.

Open floor to



IAN BROWN

Independent consultant

INTEROPERABILITY REQUIREMENTS COULD STIMULATE COMPETITION IN SOCIAL MEDIA AND INSTANT MESSAGING

Interoperability and interconnection are well-known telecommunications regulatory measures in the EU, to ensure operators can be required by national regulators to connect their networks with competitors. This ensures competition on the merits of their services, rather than the weight of network effects arising from large customer bases.

In its recent proposal for a Digital Markets Act, the European Commission has included similar but limited interoperability requirements with complementary services for the largest “gatekeeper” platforms, which provide core platform services such as social media and instant messaging. This follows calls from ARCEP and other European regulators for such powers,

which are already included in a recent amendment to German competition law. European small and medium-sized tech firms and civil society have called for these requirements to be broadened to cover core services of these gatekeepers.

Objections have been raised to this relating to the impact on innovation. However, competition is a key driver of innovation, and social media and messaging have now been mainstream services for two decades. At this level of maturity, competition economists have argued regulatory requirements for dominant platforms to make industry-standard features interoperable via open APIs or communications standards can maximise welfare.

Mechanisms for mandating technical standards are a key part of EU internal market law, and could be extended to enable regulators to mandate compliance with existing, well-developed standards from the World Wide Web Consortium and Internet Engineering Task Force. The European Commission could also provide R&D funding for infrastructure and new technology development, which was a key US policy mechanism behind the development of the ARPAnet/Internet. Specific protections for innovation could also be included in the Digital Markets Act, as they are in the European Electronic Communications Code.

Open floor to



HENRI VERDIER

Ambassador for Digital Affairs – Ministry for Europe and Foreign Affairs

OPEN TERMS ARCHIVE INITIATIVE

Today, Big Tech companies establish de facto standards through their Terms of Service (ToS). Understanding these terms is necessary:

- for every user, so they can identify what they have agreed to, the data they are sharing, the rights they have ceded to the services and those they have retained;
- for authorities, to verify that these contractual frameworks are compatible with national and supranational laws, particularly when changes are made;
- for regulators, to assess platforms' efforts and accountability.

To help keep these stakeholders informed, France's Ambassador for Digital Affairs launched the **Open Terms Archive¹ (OTA)** initiative. It is a free and open solution for tracking changes to and archiving the main online service providers' ToS, by:

- recording any updates to documents in real time;
- highlighting changes made to the documents;
- keeping a documentary record of their history.

OTA will continue to be enriched over time and become a Contributive Commons that can serve as a foundation, notably for building tools for comparative law research,

targeted alerts and linguistic analysis. A pioneering example of its use is in the coding of **Scripta Manent**, a service that creates the ability to measure any changes made to a set of 367 contracts between two given dates.

The choice to develop open and collaborative tools, committed to transparency, is entirely in tune with the two lines of force of French digital diplomacy: (i) embody **European digital sovereignty**, in other words real strategic autonomy rooted in a capacity to choose and take action; (ii) build **a digital regulatory framework based on multilateral and multi-stakeholder dialogue**.

1. A presentation of the Open Terms Archive can be found online, along with examples of the first trials and experiments, APIs, available datasets, as well as documentation on how it works and its terms and conditions.

PART 3

Tackling digital technology's environmental challenges

96

CHAPTER 6

Working to achieve digital sustainability

WORKING TO ACHIEVE DIGITAL SUSTAINABILITY

What you need to know

2020 was the year that Arcep launched its "Achieving digital sustainability" platform:

9 workshops,

127 participants,

42 written contributions

from stakeholders, which culminated in the publication of the report on "Achieving digital sustainability" on 15 December 2020.

The national Government roadmap

on the Environment and Digital Technology, published in February 2021, entrusts Arcep with several tasks, including the creation of a Green Barometer, analysing device sales and distribution practices and how they affect replacement patterns, and working in concert with ADEME to improve the assessment of the digital environmental footprint.

The bill on reducing the digital environmental footprint in France, and the bill on combating climate change and promoting biodiversity will be vital to the implementation of the proposals set forth in the reports published on this issue in 2020.

The impact that electronic communications networks, devices, datacentres and ICT use have on the environment is a source of growing concern, and one which an increasing number of stakeholders are gradually starting to address. The Citizens' Convention on Climate¹ also notes that while digital technology is a crucial lever of the green transition, and the battle against climate change, it must not itself be the source of increased emissions.

According to various studies conducted over the past two years², digital technology currently represents 3% to 4% of global greenhouse gas (GHG) emissions, and 2% of the carbon footprint in France³ (including the hardware production and usage stages). While the exact figures contained in these studies may vary, they all agree on the overall verdict.

If this percentage remains low compared to other sectors, the pace of the annual rise in digital consumption (data volume, number of devices, etc.) is cause for concern. According to the Senate Task Force on the digital environmental footprint, ICT's carbon footprint could increase substantially if nothing is done to curtail it (+60% by 2040 or 6.7% of the national GHG footprint). If such an increase were to materialise, it would seem contrary to the commitments made under the Paris Climate Agreement⁵ of 2015, which aims to contain the increase in global temperature to well below 2°C, and requires swift and massive efforts from every sector of the economy to reduce their own carbon footprint.

1. The Citizens' Convention on Climate (CCC) was formed in October 2019 from an engagement letter that the Prime Minister sent to the Economic, Social and Environmental Council. The CCC is made up of a group of 150 French citizens who are chosen by lot, and whose aim is to "take a social justice approach to defining structural measures that will reduce greenhouse gas emissions by at least 40% by 2030, compared to 1990". Its report was adopted on 21 June 2020, including proposal 150, to "Support digital development to make it more green". <https://www.vie-publique.fr/sites/default/files/rapport/pdf/274855.pdf>

2. See in particular The Shift Project, Lean ICT: Achieving digital sobriety, October 2018; GreenIT.fr, ICT's global environmental footprint, September 2019; Arcep, Future Networks - Digital Tech's Carbon Footprint, October 2019; CGE, Reducing digital technology's energy consumption December 2019 and Citizing, iCT's carbon footprint in France: are public policies enough to handle increasing usage?, June 2020.

3. At the national, GHG emissions are broken down between direct emissions (i.e. emissions tied directly to the production and use of a product or service) and indirect emissions (i.e. those, on a solely national level, tied to the consumption of energy that is an indirect source of GHG emissions or to other stages in the product or service's life-cycle, such as transport, recycling, etc.). These emissions do not factor in foreign energy sources, but only those located on national soil. The notion of footprint includes both the direct and indirect emissions produced on national soil and abroad. At the global level, then, direct and indirect emissions correspond to the footprint.

4. Senate, Information Report – Pour une transition numérique écologique/Achieving a Green Digital Transition, June 2020

5. The Paris Climate Agreement, adopted on 12 December 2015 in Paris, signed on 22 April 2016 at the United Nations headquarters in New York, and entered into effect on 4 November 2016 https://unfccc.int/files/essential_background/convention/application/pdf/english_paris_agreement.pdf

Arcep decided to devote itself fully to this issue, by building on the responsibility it was assigned by law in 2010⁶ following the Grenelle Environment Forum, to work in concert with the Government to align its actions with environmental protection imperatives.

Here, it is worth remembering that digital technology is a powerful engine of change in society, as much from an economic and social perspective, as in the daily lives of our fellow citizens and the development of public services. This, then, is the yardstick that Arcep uses to ensure that the users of digital networks and services maintain control over their choices, and are able to reap the benefits of ongoing technological developments. In other words, for the Authority, limiting digital technology's environmental impact is not necessarily synonymous with restricting uses or technologies. The challenge lies in combining the ongoing development of digital technology according to societal and economic needs, and satisfying new environmental imperatives.

Next, to better understand and tackle the issues surrounding the digital environmental footprint, and in keeping with how the regulator operates, Arcep decided to begin this new chapter in regulation by a dialogue with all of the stakeholders: through a series of meetings with experts in this area, but above all to decompartmentalise debates and gather input from as broad a spectrum of players as possible, by developing a space for dialogue, within the "Achieving digital sustainability" collaborative platform.

On 11 June 2020, Arcep launched a collaboration platform devoted to "Achieving digital sustainability" – calling on all interested associations, institutions, operators, digital industry businesses and experts to contribute through a series of workshops. The platform provided a forum for participants to examine (fixed and mobile) telecoms networks as a whole, but also devices and usage, which are key driving forces behind digital consumption and its environmental footprint. The inaugural meeting on 9 July 2020 provided an opportunity to set the themes for these workshops, culminating in the production of an initial report at the end of the year. Throughout the second half of 2020, a series of thematic workshops and two "big discussions", attended by 127 participants, were occasions for everyone to trade views, practices, tools and skills, and to help deepen the brainstorming process.

A progress report on the work done thus far, which includes 42 contributions authored by the participating players, was published on 15 December 2020.

1 The report's proposals

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. In these times of growing awareness, Arcep's proposals seek to propel this mobilisation, creating a momentum to drive it past the stage of good intentions and onto a concrete, ambitious path for reducing the environmental footprint. This means drafting environmentally-aware digital regulation, which covers not only telecoms operators but also device manufacturers, online content and application providers, datacentre operators... Consumers too can play a more active role, provided they have access to useful and relevant information, thanks to a data-driven approach to regulation.

Arcep's analysis highlights the need for more data, to be able to craft a more detailed definition of the digital environmental footprint, for all of the ecosystem's components, to move beyond the awareness stage and be in a position to take the appropriate measures.

The report underscores the "ecosystemic" dimension of digital technology, which encompasses a wide array of undertakings and so a variety of areas of expertise – such as network engineering, datacentres, devices, but also, for instance, the development of online applications and services, etc. – each of which requires a complex set of expertise from different backgrounds. Analysing the digital environmental footprint also requires close collaboration between environmental experts and digital experts, and this for the entire ecosystem and every stage in the lifecycle of the products in question (production, usage, end of life). This is why the Arcep report sets forth proposals for the entire digital ecosystem.

6. Act No. 2010-788 of 12 July 2010 on the National commitment to the environment.

THE "ACHIEVING DIGITAL SUSTAINABILITY" REPORT'S 11 PROPOSALS

Strand 1: Strengthen Public Policymakers' Capacity To Steer Digital Techn's Environmental Footprint

1. Entrust a public entity with the power to collect useful information from the entire digital ecosystem.
2. As part of its initiatives with ADEME, participate in the creation of a common frame of reference for measurement.

Strand 3: Increase incentives for economic stakeholders, private and public sector stakeholders and consumers

10. Work with interested stakeholders to draft Codes of conduct/charters to buttress green design, and which are capable of leading to the adoption of legally-binding commitments.
11. Increase users' accountability and their ability to take action through a data-driven approach to regulation, fostering the emergence of tools for aiding consumers to make informed choices ("Green Barometer").

Strand 2: Incorporate environmental issues into arcep's regulatory actions

For fixed access

3. Facilitate the transition from copper to fibre.
4. Encourage network optimisation (sharing schemes).
5. Encourage initiatives designed to implement automatic sleep mechanisms in operators' boxes.

For mobile access

6. Achieve more detailed analysis of the positive and negative impact of switching off 2G and 3G networks, to lift potential barriers
7. Examine network performance indicators in 2021, to incorporate environmental issues in consumer choice parameters.
8. Work with interested stakeholders to explore solutions for optimising mobile networks' medium and long-term environmental impact.
9. Develop more detailed monitoring of operators' handset subsidy practices and their effects.

99

2 Legislative and government work

Some of the report's proposals are echoed in the ongoing legislative work being done on the bill on reducing the digital environmental footprint in France⁷ and in the bill on combatting climate change and promoting biodiversity⁸.

In a parallel initiative, the "Digital and the Environment" roadmap published by the Government⁹ on 23 February 2021, carries forward several of Arcep's proposals¹⁰. Some of which concern Arcep directly, including:

- Collect environmental data from digital ecosystem players, and create a "Green Barometer"

The Government roadmap (action 3: "Create an environmental barometer"), entrusts Arcep, working in tandem with ADEME, with the task of performing an annual collection of environmental data from digital ecosystem undertakings, and of creating and maintaining an environmental barometer of digital ecosystem players.

Thus far, Arcep has expanded its information gathering decision regarding operators, and also collects information on networks' electric and energy consumption. The legislative work that is currently underway should result in expanding Arcep's powers to gather information on environmental issues for all digital industry undertakings (device manufacturers, online content and application providers, datacentre operators...).

7. The bill aimed at reducing the digital environmental footprint in France was introduced by Senator Patrick Chaize, and approved by the Senate on 13 January 2021. It was scheduled to be debated in the National Assembly in May 2021. <http://www.senat.fr/dossier-legislatif/pp120-027.html>

8. The bill on Climate Change and Biodiversity was introduced by the Government on 10 February 2021, as an attempt to respond to the Convention on Climate Change proposals. The very general text includes a few articles on digital technology. It was passed by the National Assembly on 4 May 2021, and will be debated in the Senate in June. https://www.assemblee-nationale.fr/dyn/15/dossiers/alt/lutte_contre_le_dereglement_climatique

9. <https://www.gouvernement.fr/numerique-et-environnement-la-feuille-de-route-du-gouvernement>

10. Notably 1. Entrust a public entity with the power to collect useful information from the entire digital ecosystem + 11. "Green Barometer" / 2. As part of its initiatives with ADEME, participate in the creation of a common frame of reference for measurement. / 9. Develop more detailed monitoring of operators' handset subsidy practices and their effects. / 10. Work with interested stakeholders to draft Codes of conduct/charters to buttress ecodesign.

- Establish a methodology for quantifying the digital environmental footprint

The Government roadmap, (action 1: “Establish a methodology for quantifying the digital environmental footprint”), confirmed the mission that Barbara Pompili, Minister for the Ecological Transition, Bruno Lemaire, Minister for the Economy, and Cédric O, Secretary of State in charge of the digital transition and electronic communications, entrusted jointly to Arcep and France’s Environment and Energy Management Agency (ADEME), to assess digital technology’s impact in France, one of whose goals is to obtain an objective measurement of fixed and mobile telecommunication networks’ environmental footprint, according to the applications they enable¹¹.

This collaboration between ADEME and Arcep extends beyond just this assignment, and creates the ability to develop a common approach to measurement, data collection and producing methodologies for measuring the environmental footprint of digital technology and its technical component parts. The two institutions have also initiated other workstreams and more regular interaction with experts on these subjects, to continue to deepen their understanding of the issues and challenges at hand.

- Produce a study on mobile phone sales and distribution models, and consumers’ replacement patterns for these devices

The Government roadmap, (action 6: “Extend the life of devices and combat software obsolescence”), tasks Arcep with producing a study of the different mobile phone sales and distribution practices, and their potential influence over device replacement rates, notably in comparison to other sales models. This analysis follows through on the request from the Citizens’ Convention on Climate, and is intended to help the Government take possible measures in this area. A letter of assignment dated 19 March 2021 sets out the details of the task and Arcep delivered its first analysis to Barbara Pompili and Cédric O in June 2021.

- Work on ways and means to take environmental issues into account in the criteria set for the next 26 GHz band frequency awards.

The Government roadmap (action 8: “Support digital industry undertakings in the adoption of ecodesign, digital sobriety and sustainable technology”) also sets Arcep the task of studying the ways and means for taking environmental issues into account in the criteria set for the next 26 GHz band frequency awards for 5G.

3 Ongoing work

As it has long been doing with consumer associations and with the internet community, Arcep is committed to continuing to nourish the process of dialogue, of listening and mutual enrichment that it has sought to build since launching its digital sustainability endeavour, in particular by providing the platform’s participants, and any other player wanting to join the effort, to **meet once again in summer 2021 to take stock of the progress made on its proposals, and on tackling the digital environmental footprint in general.**

11. This letter of assignment mission is mentioned with reference to the Government roadmap published in February 2021: <https://www.gouvernement.fr/numerique-et-environnement-la-feuille-de-route-du-gouvernement>

Open floor to



**BARBARA
POMPILI**

Minister of the Ecological Transition



CÉDRIC O

*Secretary of State
for the Digital Transition and
Electronic Communications*



CONTROLLING THE DIGITAL ENVIRONMENTAL FOOTPRINT, AND USING DIGITAL TECH TO SPEARHEAD THE GREEN TRANSITION

The Government firmly believes that the digital and ecological transitions are now inextricably linked. Far from being a passing fad, reconciling them is imperative. Both of these two sweeping transitions that are shaping, challenging and sometimes shaking up our daily lives have escalated, especially during the current crisis. If digital has become a pillar of our society, ecology is the lifeblood of our and of nature's survival.

To arm ourselves with every possible practical means of action, on 23 February of this year we began to implement our "Digital and the Environment" roadmap. Broken down into three priorities and 15 concrete actions, its overarching aim is to control the digital environmental footprint, first by working to extend the lifespan of products whose manufacturing accounts for the vast majority of the sector's carbon footprint.

Combatting planned obsolescence, supporting the development of reuse and repair, ensuring the widespread adoption of ecodesign for hardware and services: these are the priorities we have set for ourselves, and

which are coming to fruition through the Recovery plan, from public procurement that leads by example, new regulatory mechanisms (availability of spare parts, environmental imperatives for datacentres) and future codes of conduct with digital industry players.

What this roadmap ultimately aims to do, and this is a deeply held belief, is to see digital technology as a chance, as a spearhead of the ecological transition. This transition cannot happen without digital tech, very high calibre networks, strong ties between players and heavy use of artificial intelligence. We are already seeing a number of very interesting advancements in the field: better management of farming resources, optimised logistics, reduced water consumption, and better waste management. We are strong supporters of initiatives from SMEs and startups, which includes contributing more than 300M€ to support Greentech.

To turn these priorities into concrete results, the roadmap is also committed to meeting the need for accurate, clear, objective and widely accepted data, on digital's true impact on the

environment, to be able to build knowledge and inform decisions and collective actions.

It was with this goal in mind that the Government tasked Arcep with several key assignments: deliver a study on the environmental impact of digital infrastructures and services, in concert with ADEME, analyse the environmental impact of mobile telephone plans, notably service bundles, examine the paths and means for taking environmental issues more thoroughly into account during the possible upcoming award of 5G frequencies in the 26 GHz band.

Arcep is a key partner in delivering a clear objective view, but also in working to control this footprint. The annual publication of a very detailed account of the state of the internet in France, along with the report last December on "Achieving digital sustainability" testify to how exemplary the regulator's work continues to be.

Achieving a convergence of the digital and green transitions is a collective challenge. We need to tackle it together.

Open floor to



PATRICK CHAIZE

Senator of Ain, Chair of the Digital Task Force, President of Avicca



GUARANTEEING THE DEVELOPMENT OF A SOBER, RESPONSIBLE AND ECO-FRIENDLY DIGITAL ENVIRONMENT

The environmental issues we are facing today are bringing all of us to examine our tools, behaviours and organisational systems, to make them more sustainable. And digital networks and uses are no exception.

The Covid-19 crisis underscored the essential role that digital tools play. If their widespread availability is a positive thing for society, it also automatically increases their environmental impact. It requires stakeholders to reconsider their actions, to tip the balance between the benefits of having digital help drive the green transition, and the environmental footprint generated by the construction, operation and replacement of networks, servers and other devices.

It was with this in mind that I introduced a bill co-signed by more than 130 Senators that seeks to reduce the digital environmental footprint in France. The aim is to shepherd all digital players' behaviour, to guaranteeing the development of a sober, responsible and eco-friendly digital environment.

Adopted at first reading by the Senate in January 2021 and by the National Assembly in June 2021, whose main guidelines of this bill were echoed in the report from the High Council on Climate (HCC), this bill is set to be included in the Senate's upcoming agenda for second reading.

The work carried out by Avicca follows this same path. It ensures the promotion and dissemination of local authorities' best practices, whose responsibilities and projects make them central to the convergence of the economic, ecological and digital transitions. It was also decided that the digital environmental impact would be a new central area of focus.

Avicca is fully committed to the task, working in concert with Arcep, supporting its key actions designed to make all of the players along the chain more accountable and adopt more eco-responsible practices.



ARNAUD LEROY

President - ADEME

ADEME-ARCEP, YEAR TWO OF OUR COLLABORATION

Among other things, 2020 offered a reminder of how heavily we rely on digital services and networks to be able to continue to live, work, communicate, teach our children, study, be entertained... While also reminding us of the need to understand and control the impact of these services, which is far more tangible and real than the ideas they convey.

France's Environment and Energy Management Agency, ADEME, began a close and fruitful collaboration with Arcep to achieve a detailed understanding of the environmental impact of digital technology. This work will enable us to deliver an objective view of this impact in France, and to propose a forward-looking vision up to

2050. Our goal is to be able to propose possible courses of government action and levers. This investigative work will also be a way to contribute collectively to the Government's "Digital Tech and the Environment" roadmap, and to give people in France the means to understand the issues, and consume more responsibly.

Our collaboration also extends to establishing methodologies for developing a technical foundation, to be shared and used by all of the players who are committed measuring the environmental impact of their digital products and services.

In addition to increasing our knowledge of these environmental

effects, work also needs to be done on reducing them, notably by developing ecodesign, and this for every one of digital services' building blocks, be they software or hardware. Digital industry heavyweights, including telecom operators, and content and service providers, are beginning to commit to the issue and to blaze a trail to greener tech. But the pace of change needs to accelerate. The implementation of the national Recovery Plan provides an unprecedented opportunity to support businesses heading down the path to what needs to be more frugal innovation, while also meeting the needs of our society.

Open floor to



MICHEL COMBOT

Managing Director – French Telecoms Federation



DIGITAL INFRASTRUCTURES AND THE ENVIRONMENT

The public health and economic crises that our country has been enduring since the start of 2020 have proven how vital digital infrastructures are to maintaining France's economic and societal activity. Digital networks were able to absorb a significant surge in traffic: up to 30% on the internet, reaching a peak during the first lockdown in March 2020.

Which is why it is crucial that everyone, businesses and individuals alike, be able to access these infrastructures. In addition to which the development of digital networks and usage helps to decrease overall greenhouse gas (GHG) emissions, due to the impact on industrial sectors as a whole and on citizens' daily lives, whether by

reducing travelling or automating industrial processes.

For instance, according to a study that Arthur D. Little produced for the Federation, one gram of CO₂ emitted through remote working led to a 100 g savings in CO₂ emissions.

It is also worth noting that, even if digital networks represent only 5% of digital's greenhouse gas emissions in France – according to a June 2020 study by Citizing KPMG – compared to 81% for devices and 14% for datacentres, the digital infrastructures sector has been investing steadily in optimising its energy consumption. Fibre consumes three times less energy than copper networks, and

each new generation of mobile network has created the ability to reduce the power needed to transmit a gigabyte by a factor of ten, compared to the previous generation. Which will also be the case with 5G.

It is thus critical to foster public awareness of environmental issues: whether by incentivising them to recycle their mobile phones – FFT operators have collected 5.5 million phones since 2016 – or by providing them with information on the GHG emissions generated by their use of digital technology. Operators will begin providing this information in the coming months, in particular thanks to work done in concert with ADEME.



LEXICON

Afnic (Association française pour le nommage internet en coopération):

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

Android: mobile operating system developed by Google.

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.

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

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

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

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

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

Crowdsourcing: crowdsourcing tools refer to 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.

DNSSEC: Domain Name System Security Extensions

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 fibre is pulled right into the customer's premises.

GDPR (General Data Protection Regulation):

European Union (EU) regulation No. 2016/679 on data protection and privacy.

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

HTTP (Hypertext Transfer Protocol):

client-server communication protocol developed for the World Wide Web.

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

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

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

IoT (Internet of Things): network of objects outfitted with sensors and software that gives them the ability to connect to other devices and online systems, and exchange data with them.

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.

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

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

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

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

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

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

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.

PoP: an operator's physical point of presence.

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

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

Speed: 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.

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

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 non-wireline networks. SVoD = subscription VoD services.

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

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

Virginie Mathot, Advisor to the Chair
Cécile Dubarry, Director-general

DIRECTORATE FOR INTERNET, PRINT MEDIA, POSTAL AND USERS

Loïc Duflot, *director*

“Open Internet” unit

Aurore Tual, *head of unit*

Samih Souissi, *deputy head of unit*

Vivien Guéant and Emmanuel Leroux, *advisors*

“Data-driven regulation” unit

Pierre Dubreuil, *head of unit*

DIRECTORATE FOR ECONOMY, MARKETS AND DIGITAL AFFAIRS

Anne Yvrande-Billon, *director*

Laurent Toustou, *advisor to the director*

“Economic analysis and digital intelligence” unit

Anaïs Le Gouguec, *head of unit*

Anaïs Aubert, *deputy head of unit*

Arthur Dozias, *advisor*

Estelle Patat, *intern*

DIRECTORATE FOR MOBILE AND INNOVATION

Anne Laurent, *director*

Maxime Forest, *deputy director*

“Mobile coverage and investments” unit

Guillaume Decorzent, *head of unit*

DIRECTORATE FOR COMMUNICATIONS AND PARTNERSHIPS

Clémentine Beaumont, *director*

Anne-Lise Lucas and Charlotte Victoria, *advisors*

DIRECTORATE FOR LEGAL AFFAIRS

Elisabeth Suel, *director*

“Infrastructures and open networks” unit

Agate Rossetti, *head of unit*

Paul Pastor, *advisor*

Thank you...

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



This content is provided under the terms of:

Creative Commons Attribution-ShareAlike 4.0 International Public License

Publication

Arcep

14, rue Gerty d'Archimède - 75012 Paris

Directorate for communications
and partnerships: com@arcep.fr

Design

Agence Luciole

Translation

Gail Armstrong

Photos' credits

Pages 6, 7, 8 and 9: Adobe Stock

Page 39: DC3

Illustrations

Pages 73, 74 and 75: Simon Giraudot

July 2021



NETWORKS AS A COMMON GOOD ARCEP MANIFESTO

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

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

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

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

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

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