CHAPTER 1

Supervising data interconnection and relations between internet service providers and content providers

THE BOTTOM LINE

- Inbound traffic to the main ISPs in France was estimated at **50.8 Tb/s at the end of 2024**, which marks a 9.2% increase YoY.
- Around **47% of inbound traffic for the top four internet service providers comes from five companies:** Netflix, Akamai, Facebook, Google, and Amazon (including traffic from Twitch).
- BEREC collected data from across the EU on the **IP interconnection** market and published an overview of the European market between 2017 and 2022. It concluded that market competition is satisfactory overall but recommended that monitoring continues and increased attention be given to safeguarding an open internet.

1. DATA INTERCONNECTION, AT THE HEART OF ARCEP'S EFFORTS TO SAFEGUARD AN OPEN INTERNET

The internet is a "network of networks", in other words networks that are interconnected in a way that enables information to take a multitude of possible paths. "Interconnection" refers to the **technical and economic relationship established between different parties to connect to one another over the internet and exchange traffic.** It takes the form of a physical link between networks, creating a global mesh, and enabling end users to communicate with one another.

Data interconnection is thus at the heart of how the internet, this network of networks, functions, since it is through these links that the internet's many players exchange traffic, thereby creating a global network to which end users connect via their internet Service Provider (ISP). ISPs, meanwhile, interconnect with content and application providers (CAP) and other players along the internet ecosystem, to relay content and ensure good quality service to their subscribers. The more direct the links, the better the quality of service.

The internet can only run smoothly if these interconnections are sound. Negotiation difficulties between two interconnected parties may, for instance, result in a lower quality of service or a loss of interconnection which, in turn, will make it partially or fully impossible for users to access, use, or distribute the services and applications of their choice. Interconnection could also be used for the purpose of anti-competitive discrimination against the source, the recipient, the destination, or the content of the traffic being relayed.

When an interconnection issue arises, **Arcep can exercise the powers assigned to it by the legislator,** either through an *ex ante* regulatory decision or a dispute-settlement decision at the request of one of the parties.

To ensure continuous monitoring of the market, and particularly the relationships between content providers, technical intermediaries, and operators, **Arcep has been collecting data on interconnection and data transport on a biennial basis since 2012.** The aggregated findings of these data collection campaigns are published in the Barometer of Data Interconnection.[1] Key figures for the 2025 edition of this Barometer, pertaining to 2024, are included in this chapter.

The Authority is also involved in the work of BEREC which, in 2024, published a report on IP interconnection in Europe (See Chap.1.3.).

1 The Barometer of Data Interconnection is updated annually on the Arcep website.

THE MAIN PLAYERS INVOLVED IN INTERCONNECTION AND THE INTERNET

A range of major stakeholders interconnect within the internet ecosystem. These include:

- **Content and application providers** (CAPs): the owners of the content who rely on multiple intermediaries to relay their content to end users;
- **Web hosting companies:** the owners of the servers that host the content managed by third parties (CAPs or individuals);
- **Transit providers:** international network managers that act as intermediaries between CAPs and ISPs to relay traffic;
- **Internet Exchange Point (IXP) managers:** third parties operating an exchange point that enables the different players to interconnect directly through that IXP, rather than going through one or several transit providers;
- **Content Delivery Network (CDN) operators:** these technical intermediaries specialise in delivering large volumes of traffic to multiple ISPs, in different geographical areas, using cache servers located close to end users, to optimise routing while improving performances and reducing costs;
- **Internet Service Providers (ISPs):** network operators who are responsible for relaying traffic to end users.

2. THE STATE OF INTERCONNECTION IN FRANCE IN 2024

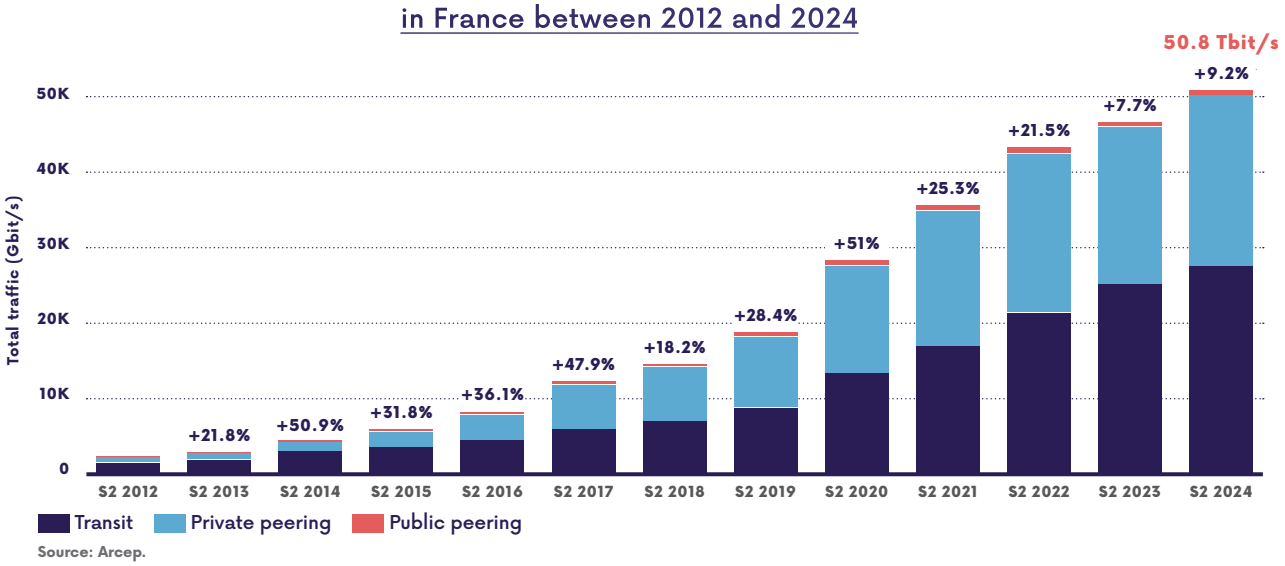
Arcep therefore has technical and financial data on interconnection from the first half of 2012 to the second half of 2024. For confidentiality reasons, the published findings[2] only cover the **aggregated results from the four main electronic communications operators in France.**

2.1. Inbound traffic

Inbound interconnection traffic to the networks of the four largest ISPs in France rose from 46.5 Tb/s at the end of 2023 to **50.8 Tb/s at the end of 2024, which marks a 9.2% increase YoY.**

This progression is comparable to the 7.7% increase in 2023, and well below the rates of increase in previous years. By means of comparison, the annual rise in inbound traffic in 2022 was estimated at 2.5%.

Progression of inbound traffic to the main ISPs in France between 2012 and 2024



Source: Arcep.

2 Results obtained from ISPs' responses to information gathering on the technical and financial conditions of data interconnection and routing, the scope of which is detailed in Arcep Decision 2017-1492-RDPI.

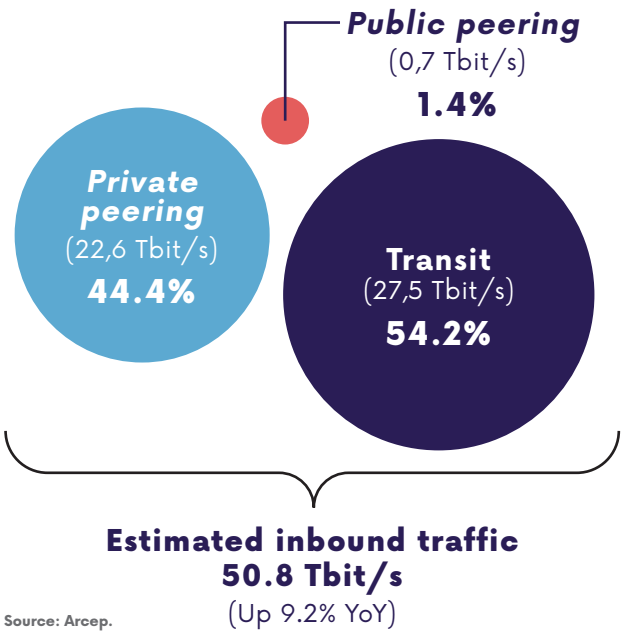
This increase in bandwidth consumption is consistent with the progression in mobile data traffic that Arcep documented in its Observatory of the Electronic Communications Markets in France, which revealed a slight decline in mobile data traffic since 2023[3] that can be attributed to:

- first, a change in demand: for instance, the 2024 Digital Market Barometer published in March 2025[4] underscored a levelling off of the penetration rate for video on demand (VoD) services – at 56%, identical to the previous year – after several years of steady increase;
- second, some content providers' efforts in terms of compression and traffic optimisation, including the use of on-net CDNs.

In the second half of 2024, inbound traffic to ISPs' networks was split chiefly between transit (around 54.2%) and private peering (around 44.4%), with a fraction being handled by public peering, i.e. at Internet Exchange Points or IXPs (1.4%). Transit thus accounts for the majority of this traffic once again in 2024, with very little change in the overall balance compared to 2023, when it stood at 54.1% for transit, 44.7% for private peering, and 1.2% for public peering.

The high proportion of transit can be explained in large part by the transit traffic between Open Transit International (OTI), a Tier 1 operator owned by Orange, and Orange's internet backbone and backhaul network *(Réseau de Backbone et de Collecte internet d'Orange,* RBCI), for relaying traffic to the ISP's end customers. This rate of transit is much lower for other ISPs that do not have their own transit business and so rely far more heavily on peering.

Distribution of inbound interconnection traffic in 2024



Source: Arcep.

2.2. Asymmetry between outbound and inbound traffic

At the end of 2024, outbound traffic from the networks of France's four largest ISPs climbed to around 5.1 Tb/s, which marks a 17.5% increase from the end of 2023. This traffic virtually tripled between the end of 2019 and the end of 2024.

The volume of outbound traffic therefore continues to be smaller than inbound traffic, due to an asymmetry in how the internet is used, with end users receiving more data than they send.

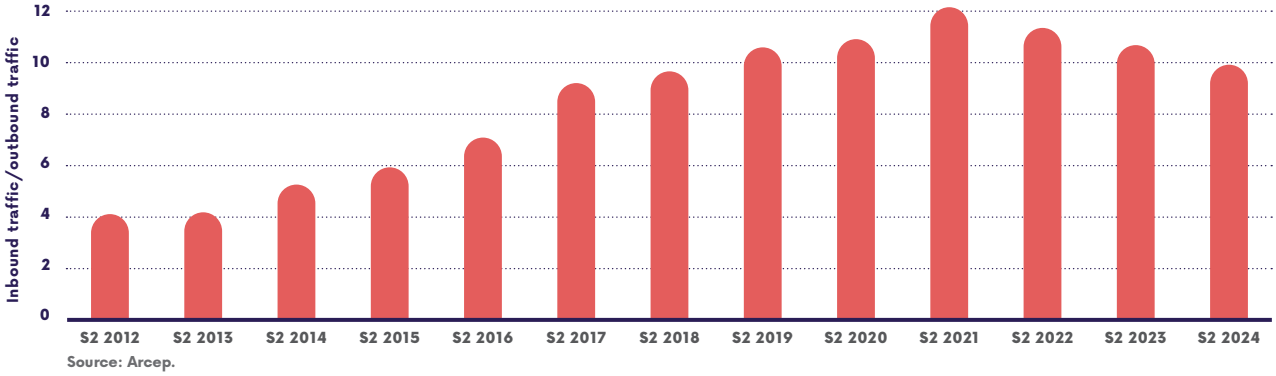
The asymmetry ratio between inbound and outbound traffic on the main ISPs' networks has, nevertheless, been narrowing steadily since 2022. In 2024, for 1 Gb/s of outbound traffic there were 9.9 Gb/s of inbound traffic, compared to a ratio of 1 to 10.6 Gb/s in 2023 (see the chart titled 'Change in the asymmetry ratio between 2012 and 2024').

Several assumptions can be made to explain this increase in outbound traffic that is altering the asymmetry ratio. **The main assumption is the rise in video uploads to social media sites.** End users are uploading more videos online, which is increasing ISP networks' outbound traffic. Unsurprisingly, the 2024 Olympic Games in Paris saw a dramatic uptick in mobile network traffic[5]. Streaming videos over smartphones appears to have become commonplace, which may well be affecting outbound traffic.

Although some players expect to see an increase in the percentage of traffic dedicated to artificial intelligence (AI)[6], **it is not yet possible to draw any definite conclusions about how generative AI will affect traffic.** There is, indeed, little reliable data available on the use of these applications and their impact on traffic. In its latest report, Telegeography[7] explains that the impact of generative AI on international traffic capacity is "not entirely clear". The report nevertheless puts forward the hypothesis of a possible increase in ISPs' traffic over time, resulting from the use of services such as GPU-as-a-service, which enable remote model training.

3 See the figures from Arcep's Observatory of Electronic Communications Markets in France for Q1 2024.
4 Arcep, Arcom, CGE, ANCT, 2025 Digital Market Barometer.
5 Florian Dèbes October 2024. "Electronic communications: how the 2024 Paris Olympics and Taylor Swift shaped the future of mobile networks", Les Echos (in French).
6 By way of example, the article in Frontier Economics, "The impact of artificial intelligence on the telecoms sector", published in 2023, mentions the Omdia assumption estimating that AI could represent two-thirds of ISPs' traffic by 2030.
7 Telegeography, 2025. State of the network.

Change in the asymmetry ratio between 2012 and 2024



Source: Arcep.

2.3. On-net CDNs' share of traffic towards end users

Seamlessly transmitting content, and video content in particular, is becoming vital for CAPs who are striving to move closer and closer to end users. This has led to the advent of a new interconnection method: on-net (or proprietary) CDNs. **CDNs are systems that make it possible to optimise the transmission of content to end users, thanks to a network of cache servers that store content temporarily, located close to users where demand exists.** This approach helps to reduce latency (content is loaded more rapidly) and to distribute the traffic load (requests are distributed between the different cache servers) when demand is high. To this end, CAPs create partnerships with ISPs to have their content hosted on cache servers on each ISP's network. These on-net CDNs can belong to the ISP that hosts them or to third parties.

By way of example, the service providers that account for a large percentage of ISPs' inbound traffic, such as Netflix, Google, Amazon, and Meta, can install their own servers on certain ISPs' networks. Arcep has been collecting data on on-net CDN since 2016.

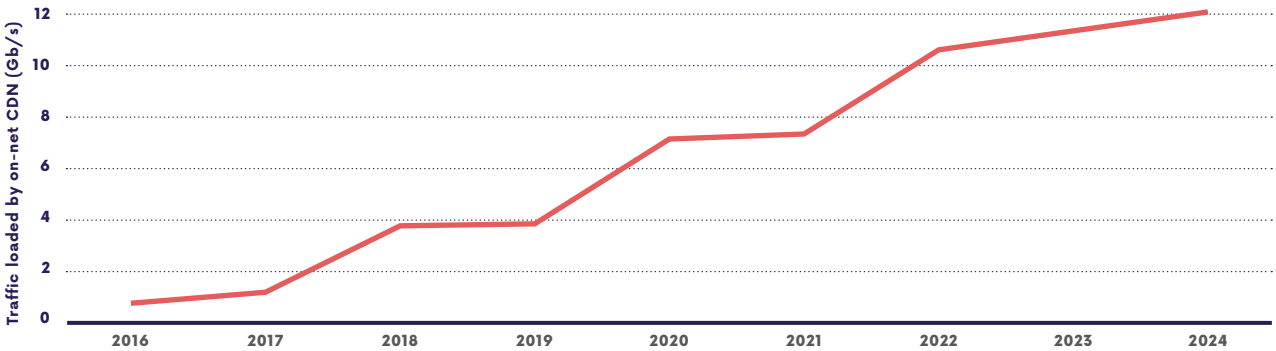
Between the end of 2023 and the end of 2024, traffic from on-net CDNs to the customers of France's largest ISPs increased slightly, rising from close to 11.4 Tb/s to around 12.1 Tb/s.

Since their first appearance, on-net CDNs have become firmly established. Because they are an efficient way to distribute content, they minimise inbound interconnection traffic and the volume of traffic being relayed over the internet. The ratio between interconnection traffic to the on-net CDN cache and outbound traffic from the on-net CDN to end users varies between 1:10 and 1:19 depending on the ISP, with an average ratio of 1:14. In other words, **the data made available via on-net CDNs are viewed an average of 14 times** (see the chart 'Interconnection point traffic, and the role of on-net CDNs'). This ratio, which stood at between 1:7 and 1:15 in 2023, has increased, proving that demand is highest for content that is hosted on on-net CDNs.

Using on-net CDNs helps to reduce interconnection point traffic, hence provisioning of the links. At identical end-user consumption levels, inbound interconnection traffic would increase by 24% in the absence of an on-net CDN.

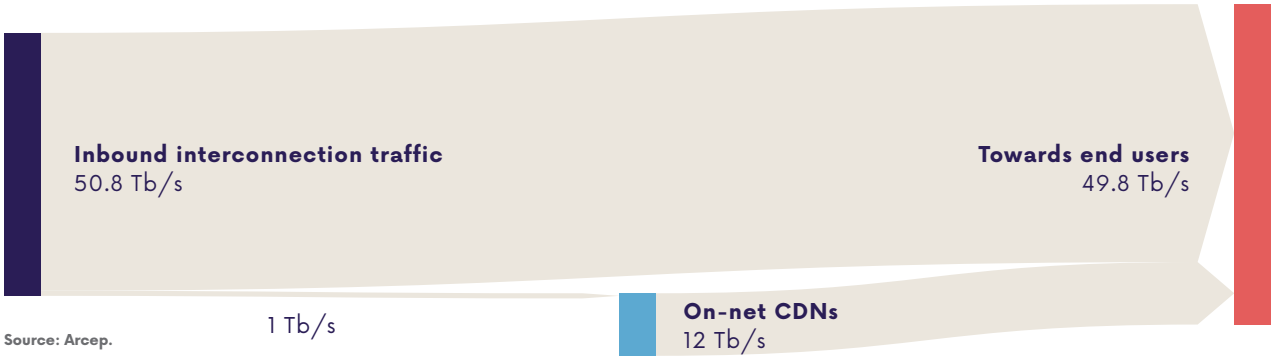
In 2024, the percentage of traffic coming from on-net CDNs represented around 19% of traffic to ISPs' customers. This is relatively unchanged compared to 2023, although it does vary between 12% and 29% depending on the ISP.

Progression of on-net CDN traffic



Source: Arcep.

Interconnection point traffic, and the role of on-net CDNs



Source: Arcep.

2.4. Breakdown of traffic by origin

Based on data collected from ISPs[8], Arcep can estimate the proportion of traffic coming from certain CAPs and content delivery companies (notably third-party CDNs), when they are identifiable, as a percentage of total interconnection traffic.

It should be noted that **the interconnection data analysed here pertain to direct relationships between internet companies' network infrastructures,** identified by their Autonomous Systems (or AS) number. This means that content hosted or transported by a third-party, which does not therefore involve a direct interconnection with an ISP reported to the Authority, is not identified in the graphic below.[9]

Despite being very popular with users, some service providers are not represented as their traffic is relayed by intermediaries (CDNs, transit providers, etc.) up to the ISP's interconnection point. For example, broadcasters – such as TF1, M6, France TV, and VoD platforms like Disney Plus[10] – relay all or a portion of their traffic via CDNs or other technical intermediaries, which explains why such a small percentage of traffic is attributed to them in the graph below. Content providers represented in the graph may also relay a portion of their traffic via technical intermediaries and thus be associated with a percentage of traffic that is proportionately smaller than the actual amount of their content consumed on user devices.

WHAT IS THE LINK BETWEEN USERS' DIGITAL PRACTICES AND INTERCONNECTION TRAFFIC IN FRANCE?

Traffic measured by ISPs at the interconnection point is influenced by users' digital habits in France but is not an exact representation.

The interconnection point is where traffic is exchanged with all ISPs' partners. It can, therefore, be seen as representing the border between ISPs' networks. It is a border in a technical but not a territorial sense: although the traffic being exchanged could come from France, Europe, or anywhere else in the world, its origin cannot be accurately determined.

Here, Arcep is presenting the aggregated results of the speeds measured at the interconnection point. These measurements are not taken on end-user devices.

The traffic, which is measured upon its arrival into the ISP's network, does not enter solely to meet the needs of end users. A minority of the data exchanged may be relayed over an ISP's network to reach another destination, such as another ISP's network.

In addition to the information from the Barometer of Data Interconnection, Arcep collects and publishes other data that can help provide a more detailed understanding of how the internet is used, and particularly mobile data traffic, as part of the Observatory of Electronic Communications Markets in France. The annual Digital Market Barometer, which is produced in partnership with Arcom, CGE, and ANCT, delivers a more qualitative snapshot of digital practices in France.

8 Here again, aggregated data are only from France's top four commercial ISPs.

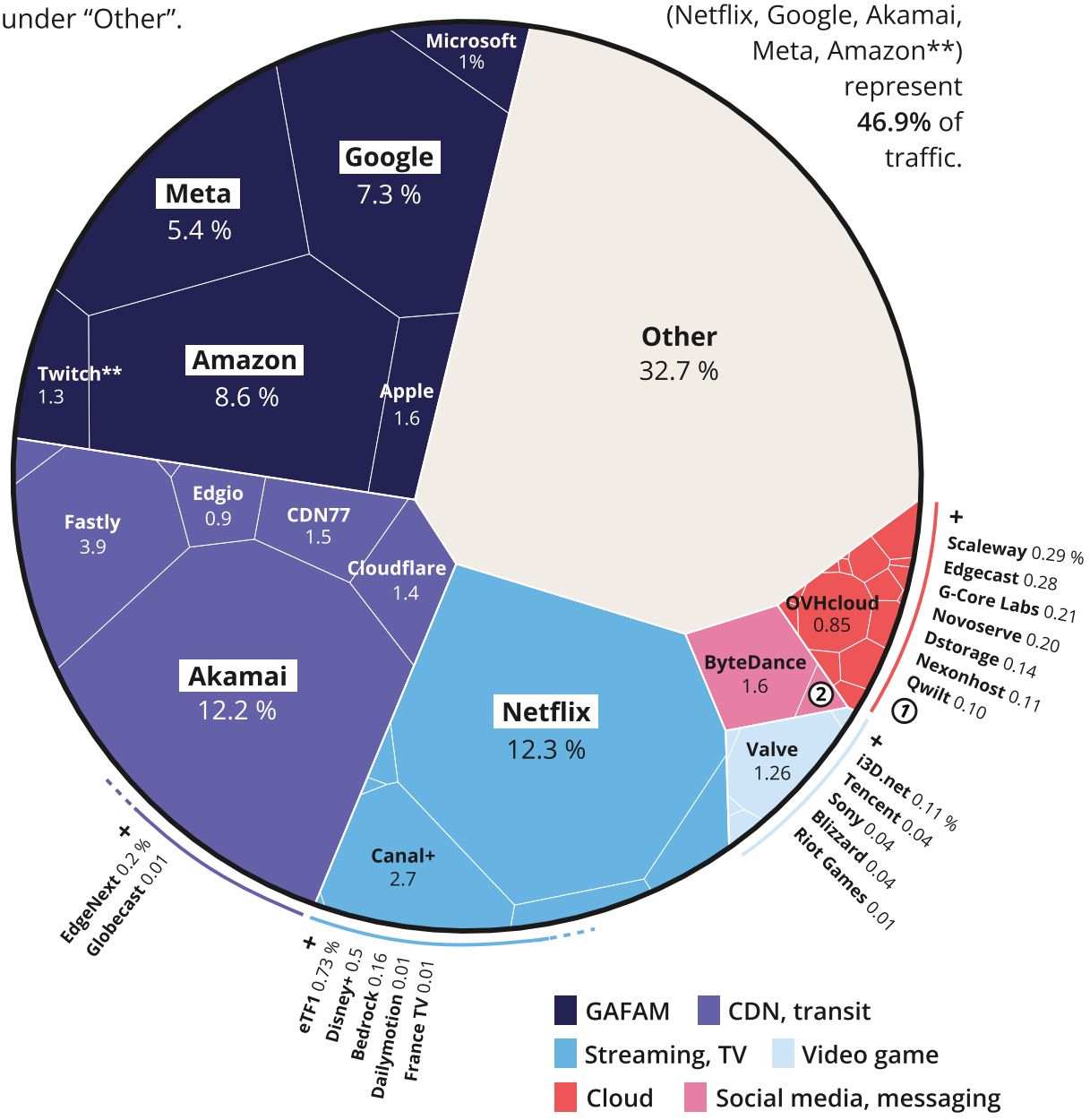
9 The graph does not, for instance, distinguish between traffic tied to the Facebook, Instagram and WhatsApp apps within the Meta group, since these services are interconnected with ISPs via Meta's common network infrastructure. This is also the case with other applications and services provided by the top five Big Tech companies ("GAFAM"). The only exception is traffic from Twitch which still has a separate infrastructure and a dedicated AS number. For the sake of clarity, however, this is included under Amazon.

10 See "Disney+ compte près de 130 million d'abonnés, nettement plus qu'attendu" (in French), Le Parisien, 10 February 2022.

Estimated breakdown of traffic by origin in 2024

Percentage of inbound traffic at the interconnection point from 44 transport or content production companies, as reported by the main ISPs at the end of 2024. The remaining traffic is shown under "Other".

Top 5 companies (Netflix, Google, Akamai, Meta, Amazon**) represent **46.9%** of traffic.



Source: Arcep.

* Bouygues, Free, Orange, SFR. ** includingTwitch, property of Amazon.

① **M247** 0.06 % ; **Alibaba Cloud** 0.06 ; **Dropbox** 0.03 ; **Zscaler** 0.03 ; **Worldstream** 0.03 ; **Leaseweb** 0.02 ; **Zenlayer** 0.01 ; **Mediactive** <0.01. ② **Telegram** 0.2 %.

The graphic p.21 illustrates an aggregation of traffic to the top four ISPs, distributed based on the partners with which they are interconnected. The different types of interconnected players have been categorised to make the graph more legible, and only those involved in distributing or transporting content are listed.

Regarding the "TV streaming" category that includes VoD services and TV channels, Netflix remains the company that generated the largest volume, estimated at 12.3% of total traffic. This share has nevertheless been shrinking since 2022 (it stood at 15.3% in 2023). The relatively small share of the other players in this category (e.g. 2.7% for Canal Plus and 0.5% for Disney Plus) needs to be qualified: some VoD services and TV channels relay a portion of their traffic via CDNs rather than their own infrastructure, which can result in a relative underestimation of their share as depicted in the graph.

Regarding CDN providers, the percentage generated by Akamai held steady in 2024 at 12.2% (compared to 12.3% in 2023[11]) and is comparable to Netflix's share this year. Meanwhile Fastly's share has increased dramatically, rising from 1.9% of traffic in 2023 to 3.9% in 2024.

Traffic from the Big 5 tech companies, i.e. Google, Apple, Meta, Amazon and Microsoft, which provide a very wide range of products and services,[12] reached 25.1%. Amazon represents 8.5% of traffic, a significant increase on 2023 (up 2.1 points). Including Twitch,[13] Amazon accounts for 9.7% of traffic, followed by Google (7.2%) and Meta (5.3%). Traffic from Microsoft increased slightly, from 0.8% in 2023 to 1% in 2024, as did that from Apple, whose share rose from 1.2% to 1.6%.

Close to 19% of traffic comes from global Tier 1 transit providers whose solutions act as the link between the different internet players (content providers, ISPs).

In the social media category, traffic generated by **TikTok parent company, ByteDance, accounted for 1.6% of total aggregated traffic in 2024,** a slight (0.5 point) increase over 2023.

Lastly, traffic generated by the "other" category, whose share stands at 32.7%, comes from ISP-to-ISP interconnection, or from companies whose main business is not content distribution or hosting.

PUBLIC RESEARCH AND HIGHER EDUCATION NETWORKS: THE FRONTRUNNERS OF THE INTERNET

When students connect to the internet on their university campus, there is a very high likelihood that their internet service provider is not a retail market ISP, but rather a national research and education network (REN), such as Renater in France.

Little known to the general public, these national research and education networks are now specialised operators serving research labs and universities. In Europe, they are grouped together within Géant[1], which enables interconnections between laboratories and research facilities.

RENs mainly provide connectivity and play an important role in knowledge sharing and the transmission of critical data for scientific experiments, e.g. for the Large Hadron Collider (LHC) at CERN.[2]

It is worth noting that these networks have made a significant contribution to the history of the internet, both nationally and internationally. In France, the dissemination of Renater relied on groundbreaking work carried out around the Cyclades[3] computer network, which is considered one of the precursors of the internet. This networking of higher education and research establishments actually predates the public internet. Another example took place in 1995, when the Renater public interest group took part in the creation of SFINX, one of the first IXPs in Europe.[4]

1 Géant, 2023 *Compendium.*
2 Renater, *LHCONE*.
3 SCHAFER, Valérie and TUY, Bernard, 2013. *Dans les coulisses de l'Internet : RENATER, 20 ans de Technologie, d'Enseignement et de Recherche.* Paris : Armand Colin. « Le sens de la recherche », p.240. DOI : 10.3917/arco.schaf.2013.01 (in French).
4 SCHAFER, Valérie, 2012. *« De Cyclades à Renater : Des réseaux de données pour la recherche et l'enseignement (années 1970-1990) ».* Histoire de la recherche contemporaine. La revue du Comité pour l'histoire du CNRS, 11 octobre 2022. (in French).

11 This on the heels of a very sizeable increase between 2021 and 2022, attributed to a rise in the consumption of content hosted by this company, and to changes in the CDN market where players switched from an other CDN provider to Akamai, which also explains why Akamai's market share stopped growing.
12 The "GAFAM" category includes traffic from networks owned by Google, Amazon, Meta, Apple, and Microsoft. As it is impossible to distinguish the interconnection traffic of these different companies' services, it is also impossible to break down the different services according to the categories listed in the graph. This is why, for instance, Instagram is not classified in "social media" or YouTube in "video and streaming".
13 Twitch was still using a separate AS number in 2024 but displayed as "Amazon IVS". While listed separately, Twitch is included in Amazon's share since the two belong to the same group. Moreover, Twitch's decreasing share may be explained by traffic being switched over from the old AS to Amazon's main AS.

3. STATE OF INTERCONNECTION IN EUROPE IN 2024

Published in December 2024, the BEREC report on IP interconnection in Europe[14] provides a state of the art on interconnection in Europe since 2017. **For the first time, it draws upon a data collection campaign carried out across Europe in autumn 2023, in a coordinated fashion with each national regulatory authority** (NRA). It focused on European ISPs' interconnection agreements, drawing on 174 contributions.

The report analyses overall changes in interconnection traffic from 2017 to 2023, along with cost and pricing trends. The data and stakeholder feedback suggest that traffic growth is levelling off, while costs and prices are decreasing steadily. The report also details the market's competition dynamics, and the power relations between players. The growing prominence of CDNs and direct peering is, for instance, putting competitive pressure on transit providers, and especially on the price of transit services.

Although many of the points corroborate the analyses conducted by Arcep (notably the growing entrenchment of CDNs in the interconnection landscape since 2017, which is equally evident across Europe), the report's findings also reveal the specificities of the French market, particularly the role of paid peering, which tends to be minor at the European level.

From this analysis, the report deduces that competition in the IP interconnection market is satisfactory, which aligns with BEREC's earlier conclusions on this subject. In addition to continuing to monitor the market, BEREC suggests that a more in-depth investigation may be warranted into this market segment's compliance with the open internet principle, and the applicability of solutions resulting from the Electronic Communications Code and Open Internet Regulation.

EUROPEAN WORK ON THE TOP CONTENT AND APPLICATION PROVIDERS (CAPS) AND THEIR RELATIONSHIPS WITH ELECTRONIC COMMUNICATIONS OPERATORS

In addition to IP interconnection, Arcep and BEREC have been actively working on the various technical and commercial relationships between content providers, infrastructure operators, and electronic communications networks, to inform current European discussions on this topic. In particular, Arcep co-chaired BEREC's work on the entry of large CAPs into the markets for electronic communications networks and services.[1]

The report, which includes stakeholders' feedback to the public consultation, aims to identify those parts of the internet in which gatekeeper platforms are investing, and to analyse their strategies for moving up the value chain, their business models, and their relationships with traditional ENC/ECS providers in terms of competition, cooperation, and interdependence. The report thus provides an overview of the impact that these Big Tech companies are having on networks and certain electronic communications services in Europe.

Relations between large CAPs and electronic communications operators are multifaceted. Both players can form partnerships to provide joint or complementary services (e.g. ISPs provide broadband internet access services, and CAPs provide content and applications; home routeurs deliver both internet access and access to Over-The-Top or voice assistant services). ISPs and CAPs can also compete directly, notably when it comes to calling and messaging services, the supply of cloud services, CDNs, submarine cables, etc.

In its report, BEREC analyses these different dynamics through three case studies on CDNs, on submarine cables, and on internet relay services that are akin to virtual private networks (VPNs). The analysis reveals how gatekeeper platforms have deployed their own physical infrastructures (e.g. CDNs, data centres etc.) and network infrastructure (submarine cables), and are now operating a large portion of the services internally, that they had previously contracted from electronic communications operators (e.g. international transit).

The report also details some of the restrictions imposed by operating system (OS) providers that affect, or could affect, the ability of electronic communications operators to provide internet access or access to certain services.

For further details on Arcep's work on digital technology, see Volume 1 of the 2025 Annual report

1 https://www.berec.europa.eu/en/document-categories/berec/reports/draft-berec-report-on-the-entry-of-large-content-and-application-providers-into-the-markets-for-electronic-communications-networks-and-services

14 BEREC, 2024, Report on the IP Interconnection ecosystem.

Giving the floor to

ALENA MURAVSKA

Programme Manager on the Community & Engagement at RIP NCC

The RIPE NCC: At the Heart of a Stable and Open Internet

The RIPE NCC (Réseaux IP Européens Network Coordination Centre) is one of the five Regional Internet Registries (RIRs) in the world. As a not-for-profit membership organisation, the RIPE NCC is responsible for the allocation and management of Internet number resources in Europe, the Middle East, and Central Asia. These resources include IPv4 and IPv6 addresses, as well as Autonomous System Numbers (ASNs). But beyond its technical mission, the RIPE NCC also plays a key role in supporting the global interconnection ecosystem and the open Internet.

Infrastructure for a Stable Internet

One of the RIPE NCC's main objectives is to ensure that the Internet remains open, stable, and accessible to all. By ensuring the accurate registration of Internet number resources, the RIPE NCC enables networks around the world to connect with one another. Every Internet service provider, network operator, hosting company, or enterprise needs these resources to be identified and to route Internet traffic properly.

Without careful and fair management of these resources, the Internet would be chaotic, unstable and vulnerable to abuse. The RIPE NCC applies policies that have been developed by the RIPE community itself, through an open, transparent, and bottom-up process to ensure a fair and transparent distribution of resources. This collaborative governance model is one of the cornerstones of our open Internet.

Building Consensus

In its role as secretariat to the RIPE community, the RIPE NCC organises two RIPE Meetings each year, in addition to other regional events. RIPE meetings bring together a broad community: Internet service providers, researchers, policymakers, network engineers, representatives from governmental and non-governmental organisations, and many others. Here people share best practices, discuss technical developments, debate resource management policies, and strengthen human relationships in what is often a highly technical field.

While much is discussed at RIPE Meetings, the actual policy-making process occurs on public mailing lists, which are open to anyone and form the backbone of the RIPE Policy Development Process (PDP). These mailing lists are where consensus is built, objections are addressed, and proposals are refined. The RIPE NCC also facilitates this process as the community's secretariat.

Supporting Research and Network Resilience

The RIPE NCC also provides tools and technical services for monitoring and understanding the Internet. For example, RIPE Atlas, a global network of distributed probes, allows real-time measurement of Internet connectivity. RIPEstat, another key service, provides a complete and freely accessible overview of the state of IP resources, routing, and global connectivity. The Internet community can also publish ideas, data tools and analyses on RIPE Labs, which is managed by RIPE NCC and also includes a podcast covering a range of topics relating to Internet infrastructure and governance.

These services support not only academic research and innovation but also the operational resilience of networks. In the event of an incident, they enable a faster response and better coordination between operators, thus contributing to the overall stability of the Internet.

Promoting Education and Cooperation

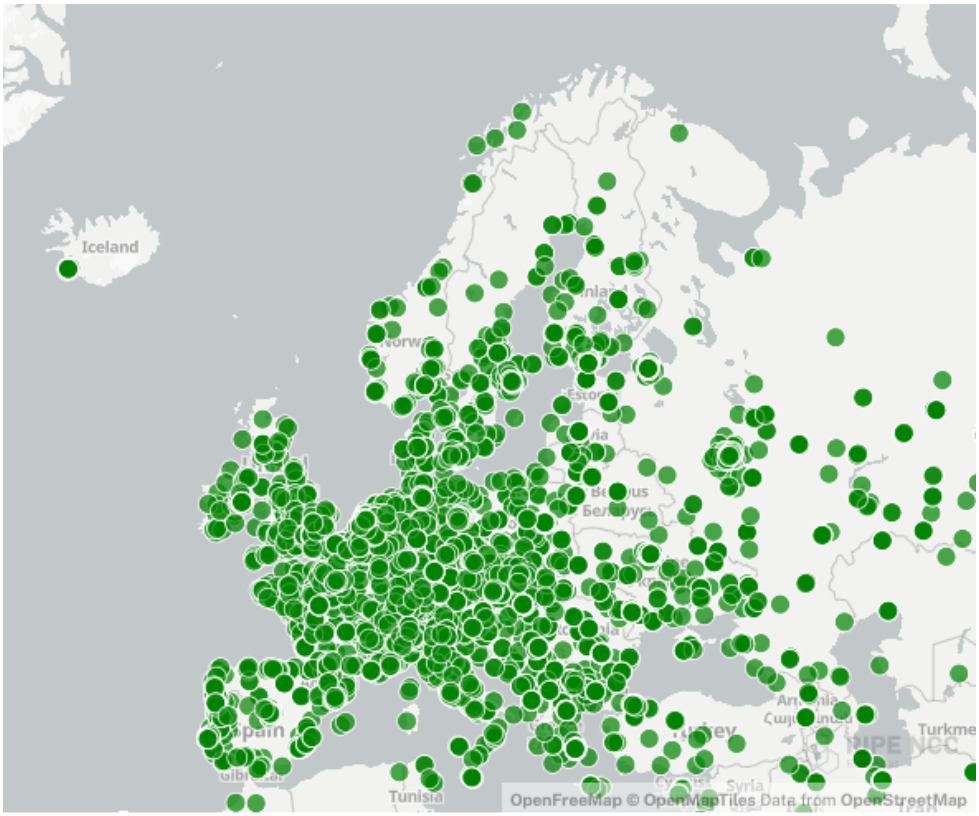
The RIPE NCC regularly organises training sessions, webinars, and certification programmes to help network professionals develop their skills. This includes face-to-face training across its service region, a free online academy and, for those who want to go further, a certification programme that validates these competencies.

The RIPE NCC also participates in key multistakeholder forums such as the Internet Governance Forum (IGF), the ITU, and other regional platforms, where it works to ensure that decisions about the Internet's future are inclusive, transparent, and evidence-based. It also supports capacity building and informed participation among its community members, helping them engage in policy dialogues and contribute to shaping Internet governance from the bottom up.

The organisation also plays a key role in raising awareness about critical issues such as Internet security, IPv6 adoption, and Internet governance, particularly among audiences less familiar with the technical landscape, such as government representatives and the general public.

A Voice for an Open Internet

In a global context where geopolitical tensions, national regulations, and commercial interests can threaten the neutrality of the network, the RIPE NCC remains a trusted steward of the open, inclusive, collaborative Internet model. By staying true to its mission, the RIPE NCC retains the trust of its members and its community, a mission it is determined to uphold in support of a single, stable and resilient Internet.



Altas probes coverage map.

Source: https://atlas.ripe.net/statistics/coverage

Lexicon

3GPP

The 3rd Generation Partnership Project is an umbrella organisation for cooperation between standard development organisations to establish technical specifications for mobile networks.

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.

Afnic (Association française pour le nommage internet en coopération)

The French domain name registry. A non-profit organisation (under the French 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).

API (Application Programming Interface)

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 program provides services to other software programs.

Autonomous Systems (AS)

A collection of networks managed by the same administrative entity, with relatively homogeneous routing protocols.

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.

CAP

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

CDN (Content Delivery Network)

Internet content delivery network.

Codec

A device or computer program that encodes or decodes a digital data stream, for transmission or storage purposes.

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 modem/router. Cross-traffic decreases the bandwidth available for the test.

DNS (Domain Name System)

Mechanism for translating internet domain names into IP addresses.

Dual stack

Assigning both an IPv4 address and an IPv6 address to a device on the network.

FttH (Fibre-to-the-Home) network

Ultrafast electronic communications network, where fibre is pulled right into the customer's residential or business premises.

HTTP (Hypertext Transfer Protocol)

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

HTTPS

HTTP Secured through the use of SSL (secure socket layer) or TLS (transport layer security) protocols.

iOS

Mobile operating system developed by Apple for its mobile devices.

IP (Internet Protocol)

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

IPv6-enabled

Device or connection that actually transmits and receives traffic using IPv6 routing, either through 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.

ISP

Internet Service Provider.

IXP (Internet Exchange Point) or GIX (Global Internet Exchange)

Physical infrastructure enabling the ISPs and CAPs connected to it to exchange internet traffic between their networks through public peering agreements.

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.

NRA (National Regulatory Authority)

A body mandated by a BEREC Member State to regulate electronic communications.

On-net CDN

Content delivery network (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.

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.

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.

RIPE NCC (Regional Internet Registry for Europe, the Middle East, and Central Asia, Network Coordination Centre)

An organisation that is distinct from RIPE (Réseaux IP Européens), it is an open forum of internet companies, but provides administrative and logistical support for RIPE. RIPE NCC is also responsible for distributing IP address resources between the ISPs requesting them. Every network is assigned an AS, which then serves to identify that network for routing and interconnection purposes.

Specialised service

Electronic communication service(s) that is distinct from internet access services, and which requires specific quality of service levels.

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: Mb/s, Gb/s, Tb/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.

Tier 1

Network capable of reaching every other internet network through peering without requiring a transit provider. Wikipedia lists 14 Tier 1 networks in 2025:

- Arelion (formerly Telia Carrier);
- AT&T;
- Deutsche Telekom AG;
- Global Telecom & Technology (GTT Communications);
- Liberty Global;
- Lumen (formerly CenturyLink then Level 3);
- NTT Communications;
- Orange;
- PCCW Global;
- Tata Communications;
- Telecom Italia Sparkle;
- Telxius/Telefónica;
- Verizon Enterprise Solutions;
- Zayo Group.

Depending on the criteria, some operators, such as Cogent, may not be considered to be Tier 1.

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, providing access to the entire internet as part of paid, contractual 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.

VoIP (Voice over IP)

Technology for relaying voice calls over IP-compatible networks via the internet.

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.

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 application without the traffic being counted against their data allowance.

ARCEP, NETWORKS AS A COMMON GOOD

The internet, fixed and mobile electronic communication networks, data centres, as well as postal and press distribution networks constitute “infrastructures of freedom”. Freedom of expression, freedom to communicate, freedom to access knowledge and to share it, but also freedom of enterprise and innovation, all of which are key to the country’s economic development and cohesion within Europe.

Because it is essential 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 the highest standards in terms of accessibility, universality, performance, neutrality, trustworthiness and sustainability.

The genesis of the Regulatory Authority for Electronic Communications, Postal Affairs and Press Distribution (Arcep) was the acknowledgement that independent state oversight was needed to ensure that no power, be it economic or political, is in a position to control or hinder citizens’, businesses’, associations’, publishers’ or innovators’ ability to communicate or trade. A neutral and expert arbitrator with the status of independent administrative authority, Arcep is the **architect and guardian** of communication networks’ status as common goods in France.

As network architect, Arcep creates the conditions for an open and decentralised network organisation. It works to safeguard the competitiveness of the sectors it is responsible for regulating, by promoting pro-investment competition. It provides the framework for the networks’ interoperability so that, despite their diversity, they remain easy to access and seamlessly interconnected. It coordinates effective interaction between public and private sector stakeholders, particularly when local authorities are involved. It provides the trustworthiness needed for data intermediation between different enterprises. It also creates the conditions for open and competitive access to cloud computing solutions for businesses.

As network guardian, Arcep enforces the principles that are essential to safeguarding all users’ current and future ability to communicate and trade. It oversees the provision of the Universal Service and assists public authorities in guaranteeing the most extensive access possible to high-quality and resilient networks nationwide. It ensures users’ access to clear and accurate information, their freedom of choice, and protects against possible neutrality violations on both the internet and in the press. More generally, Arcep combats any type of impediment that could threaten the freedom to communicate and trade on the networks or the free movement of data and, to this end, pays close attention to the intermediaries that are devices and the internet’s gatekeeper platforms. For the sake of generations to come, the Authority is dedicated to future-proofing digital technology and its uses, measuring the progression of its environmental footprint, and making sustainability a core tenet of its regulatory actions.

MANIFESTO

arcep