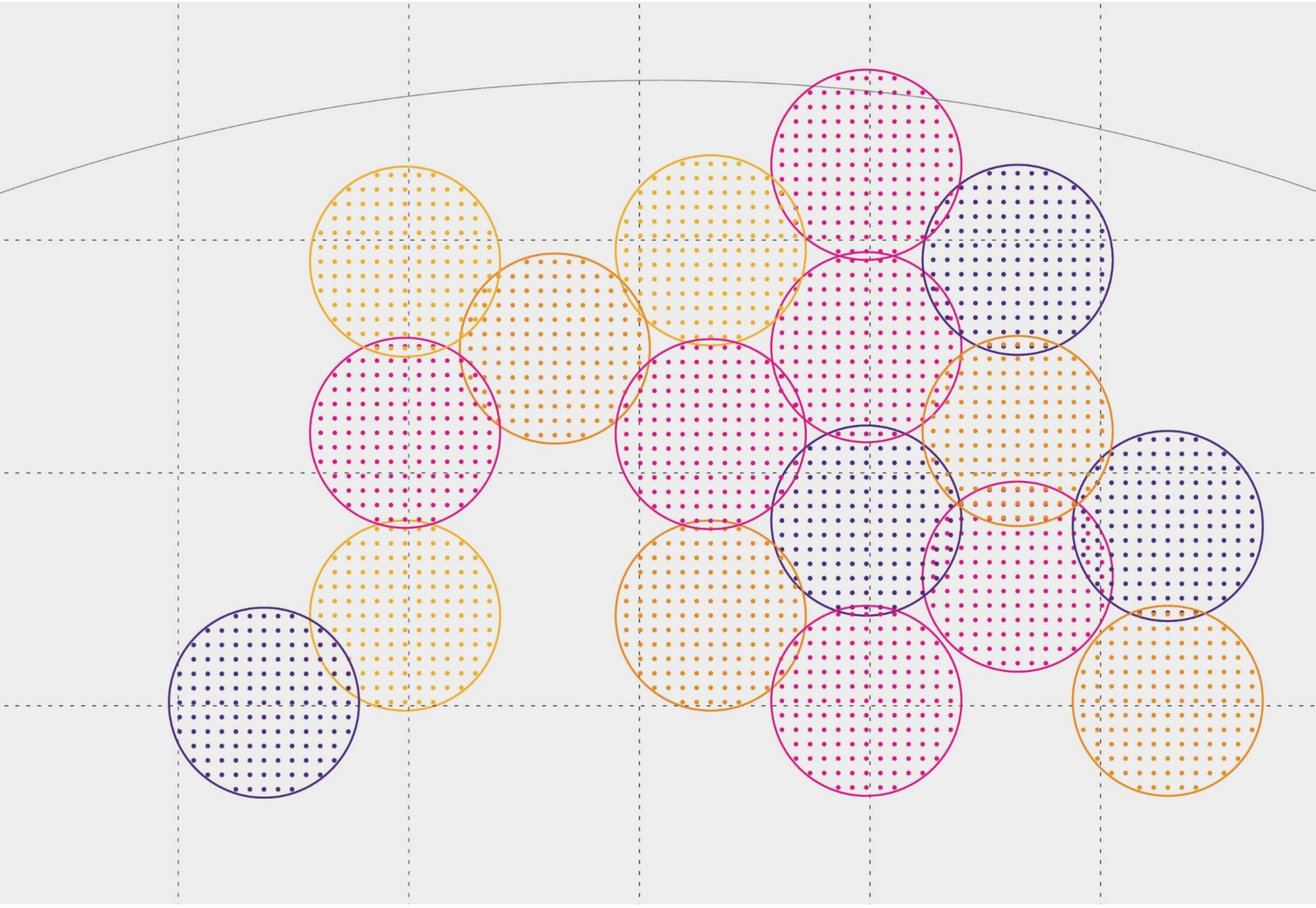
How the Internet Works and How it is Paid For (Part 2: The Structure and Economics of the Internet)

12 July 2022

Mark McFadden, Aude Schoentgen, Karim Bensassi-Nour



plumconsulting.co.uk

About Plum

Plum offers strategy, policy and regulatory advice on telecoms, spectrum, online and audio-visual media issues. We draw on economics and engineering, our knowledge of the sector and our clients' understanding and perspective to shape and respond to convergence.

About this study

This is a report for Google in addressing the topic: *How the Internet works (and is paid for) – a 2020s refresh* (to inform policymaking).

This is the second of three parts of the study: concentrating on how the Internet works and how its infrastructure is paid for.

Plum Consulting
10 Fitzroy Square
London
W1T 5HP

T +44 20 7047 1919
E info@plumconsulting.co.uk

Contents

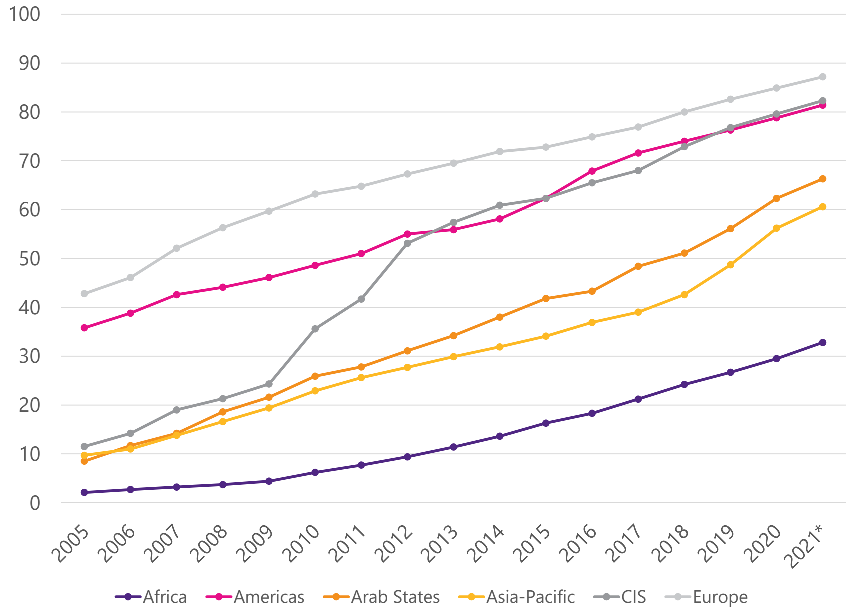
1 A market overview of today's Internet

1.1 Global Internet penetration

The Internet has been one of the most life-changing and fast-growing technologies in the world. According to the latest ITU estimates, 4.9 billion[1] individuals around the globe are using the Internet, which is 4.8 times more than in 2005. The average global Internet user spends around 7 hours per day online, and in 2021 alone, more than 293.3 billion dollars have been spent on digital media and online subscriptions.

Although the Internet adoption and usage have grown at an incredible rate, around half the world's population is still offline. Figure 1.1 below shows the percentage of individuals using the Internet by region. The top three regions with the highest number of Internet users are Europe, the Americas regions, and the Commonwealth of Independent States (CIS) region. In the APAC region, where more than half of the world's Internet users are located, only 66.3% of individuals are using the Internet. Africa is the continent with the lowest usage rate despite having the highest growth of Internet users in the 2005-2021 period.

Figure 1.1: Percentage of individuals using the Internet by region[2] (2005-2021)



Besides the disparities between regions, there is also a persistent digital divide within regions and countries based on urbanization level.

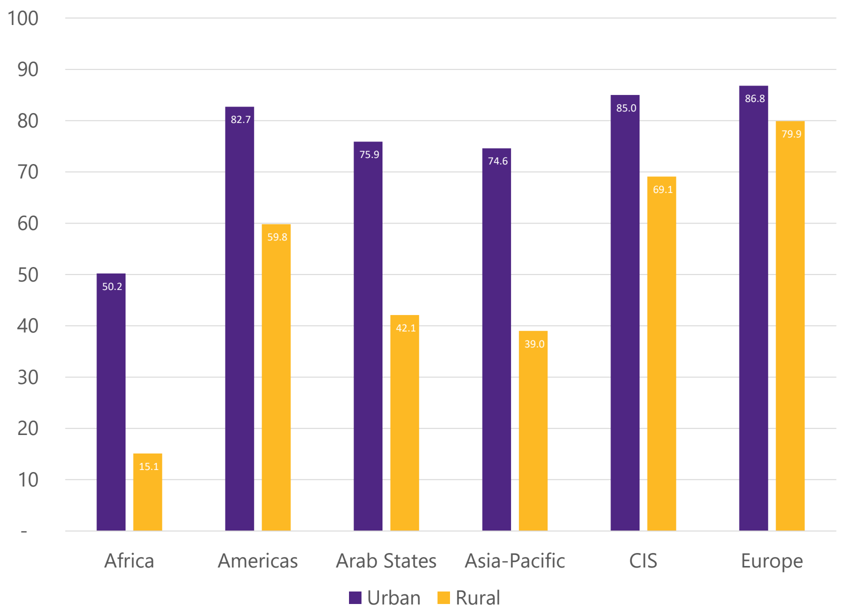
Internet penetration has indeed been more successful in urban areas where Internet users' percentage is significantly higher than in rural areas with the largest rural-urban gap in Africa (Figure 1.2). On average, only 38.8% of the world's rural population uses the Internet, compared to 75.6% of the urban population[3].

[1] ITU Statistics 2021. https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[2] ITU Statistics 2021. https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[3] ITU Statistics 2020. https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

Figure 1.2: Percentage of individuals using the Internet by region and rural/urban areas[4] (2020)



1.2 International bandwidth and data traffic

The strong growth in Internet traffic recorded in the past years is mainly due to the emergence of new Internet-enabled devices, the growing broadband penetration in developing economies, higher access rates and more bandwidth-intensive applications such as streaming platforms and online video games.

During the COVID-19 pandemic, we have seen network-wide and individual-user increases in data consumption and it is reported that Internet traffic growth has significantly outpaced pre-COVID-19 forecasts: average traffic in 2020 grew by 48 per cent while global peak traffic grew by 47 per cent, compared to forecasts of average annual growth between 2016 and 2020 of 30 per cent[5]. In the US and Europe in particular, traffic on broadband networks increased 51 per cent because of the COVID-19 pandemic, and average per-subscriber (or household) usage increased from 344 GB per subscriber in Q4 of 2019 to 482.6 GB per month in Q4 of 2020, an increase of 40 per cent[6]. Working from home requirements represent the main driver of this additional volume as usage has significantly increased during the day, whereas networks were previously less busy. However, networks are designed based on peak consumption and not volume, and while volume has exceptionally grown during this period peak traffic has not systematically increased to the same extent[7] - another reason Internet infrastructure was able to manage the rapid changes in demand due to the pandemic.

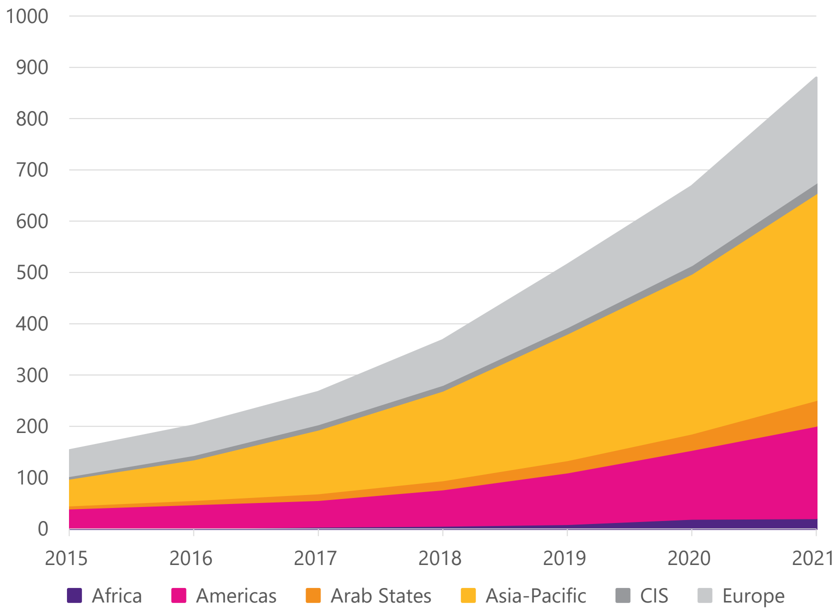
[4] ITU statistics 2020. https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[5] Telegeography. 2020."Internet Traffic and Capacity in Covid-Adjusted Terms" see: https://blog.telegeography.com/Internet-traffic-and-capacity-in-covid-adjusted-terms

[6] OpenVault. 2021. "OpenVault Broadband Insights Report". See: https://schutz-vor-strahlung.ch/site/wp-content/uploads/2021/04/OpenVault-OVBI-Q420-Broadband-Insights-Report.pdf

[7] Peak traffic has increased in some markets mostly because of increasing SVOD and gaming downloads while this has not been the case in other ones. See for example: https://newsroom.bt.com/the-facts-about-our-network-and-coronavirus/ and https://blog.telegeography.com/Internet-traffic-and-capacity-in-covid-adjusted-terms

Figure 1.3: International bandwidth in Tbit/s[8] (2015-2021)



1.3 Technological progress

Accessing the Internet before the advent of broadband and Wi-Fi was a slow and frustrating experience. One had to sit in front of a large computer physically connected to a modem while no one else at home could use the phone as the phone line was used to establish a connection to the Internet. This was known as the Dial-up Internet.

Since the era of dial-up Internet, the world has witnessed a technological advancement (see Figure 1.4) that reshaped the Internet user's experience. Not only have computers and smartphones become more sophisticated, but access technologies have evolved to allow faster data rates, higher throughputs, and a new frontier of usage.

Wi-Fi for example, made the Internet accessible beyond the office desk if you had a laptop, or a tablet. It took off in the early 2000's with the launch of the iBook by Apple, although the earliest versions were implemented in the mid-90s.

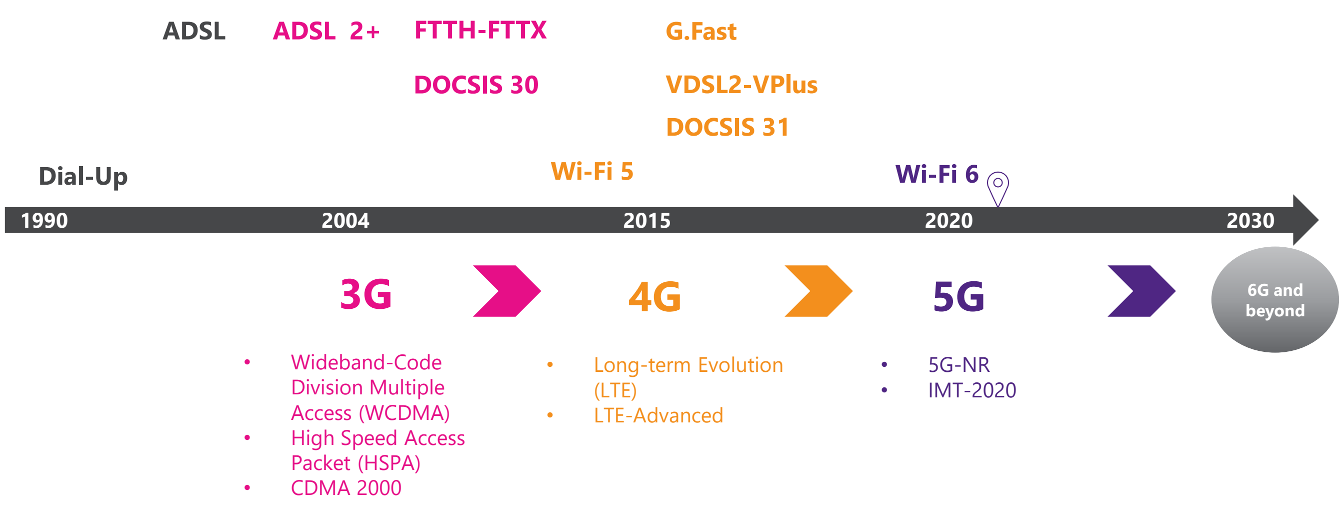
Early versions of the mobile Internet, such as the WAP (Wireless Application Protocol), resembled the dial-up fixed access: only elementary web pages could be accessed, at a very slow rate. Then radio technology allowed for more than calls and texts to be sent, and the first mobile data standard known as 3G began to be developed. At the same time the iPhone 3G model was introduced, and the world saw the rise of a mobile app industry that grew quickly with the launch of 4G in the early 2010's. Compared with 3G, 4G offered a big step up in terms of a user's experience -- enabling services such as interactive TV, video blogging, online gaming and professional services.

With the gradual introduction of 5G, (Figure 1.4) there is no doubt that user experience of the Internet will continue to change and patterns of usage will keep evolving. As of January 2022, the GSA (the Global Mobile

[8] ITU statistics 2020. https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

Suppliers Association[9]) has identified 87 operators in 145 countries and territories that have either launched, acquired spectrum licences, have demonstrated, or are testing 5G networks.

Figure 1.4: Mobile and fixed technology evolution



Source: Plum

1.4 It's not just people...

As the Internet has transformed social, political, and economic life since its emergence in the public sphere in the 1990's, there is a common assumption that this is simply a tool to connect people together in webs of common interest.

However, the Internet's impact on political and economic life means that the community of stakeholders is far broader than individual users. The stakeholder community also includes businesses, academic institutions, governments, non-governmental organizations and almost any organization on the planet that works, communicates, or plays with other organizations and people.

Enterprises

While it's common to think of the Internet as a tool that connects people, it is crucial to understand the importance of the Internet to enterprises. According to Cisco, the number of devices connected by businesses to the Internet represents 26 percent of all devices. The business share is growing faster (12.0 percent Compound Annual Growth) than the consumer share (9.1 percent CAG)[10].

Things and devices

The Internet of Things (IoT) is a buzzword that refers to the billions of connected devices on the Internet. With extremely inexpensive computers and network connections, it is possible to connect things as small as a temperature sensor to something as big as a plane to the Internet. In many cases, these devices connect to the Internet and perform a simple function without having a human being intervene. It seems simple, but the

[9] See http://www.gsacom.com
[10] Cisco Annual Internet Report

implications for the Internet are enormous. First of all, there are billions of things connected to the Internet already – many more things than people. Second, the things collectively assemble mountains of data that can then be combined into huge collections of data that can be analysed for trends and changes. Finally, some of the objects connected to the Internet can provide real-time warnings that make the world safer for humans. The Internet of Things can make the world a little smarter, safer, and more responsive to our needs.

The idea of adding sensors and intelligence to objects in the human environment has been around for a long time. But the size and expense of computers, the cost of network connections, and the size and capabilities of batteries limited early experiments. Computer chips that were cheap and frugal enough to be essentially disposable were needed before things could be connected to networks in great numbers.

Today, with the advent of tiny, inexpensive computers, the IoT is already upon us. The tech analyst Gartner predicts that the enterprise and automotive industry alone will account for more than 5.8 billion devices in the current pandemic year. Even larger will be the utilities sector with the ongoing global rollout of smart energy meters.

However, the incredible number of connected devices puts pressure on the Internet. That pressure comes not just from the added traffic and connections required by such a vast number of devices but from the risks that emerge when so many devices are connected. Security vulnerabilities of the devices make them susceptible to attack or misuse. Because these machines are so limited in their capabilities, they are generally unable to run antivirus or malicious software detection programs to protect against abuse. The marketplace is evolving to protect against these vulnerabilities in new ways.

In addition, the sheer number of devices being connected means that new strategies for identifying those devices needs to be provided. In many cases this means transitioning to a new version of the Internet Protocol (IPv6) which has an enormous address space available.

Things and devices represent an almost unseen change to the Internet. It's not uncommon to have cars, refrigerators or televisions connected to the Internet. That the Internet of yesterday has adapted to meet the new challenge of the Internet of Things is an example of the Internet's successful open, permissionless model of technology adoption

Webscale platforms and services

Webscale platforms and services make it possible to use the Internet to build highly distributed, highly reliable applications and services for use around the world. The word "webscale" describes a set of architectural principles. For instance, the tolerance of failure is essential in a highly distributed system so that availability of a service or application is not affected by local, temporary outages. Large companies like Facebook and Google have designed this idea into their networks for years. The major difference is that now the same technology that allowed those companies to scale to massive computing and network environments is being introduced into mainstream businesses.

These highly reliable, global systems have been built on an ever-evolving Internet: capable of growing and expanding in function while remaining compatible with older technologies.

2 Key features of today's Internet

2.1 Protocols

Protocols are rules for communication. When devices on the Internet want to talk to each other, they need a common language each understands. There are many different protocols in use with many different purposes. In every case, the protocol establishes a set of rules that define how information is exchanged, what happens when there are errors and details about what can and cannot be sent.

One essential protocol is the Internet Protocol (or simply IP). The Internet Protocol describes how information is transmitted in packets. Like an envelope, an IP packet has a destination address and a source address. Every device on the Internet gets an IP address that allows that device to communicate with other nodes on the network. Whether it is a mobile phone, laptop, router, refrigerator or tablet, every device gets an IP address and uses it to communicate with all the other devices that follow the rules of the Internet Protocol.

2.2 Packets

The Internet is different from traditional telecommunications because devices on the Internet organize information into packets. In general, packets have addressing information (where the packet came from and where the packet is destined to go to) and content. When two devices need to communicate on the Internet – exchanging email, video conferences or pictures – they do so by grouping data into packets and then sending them toward their destination using addresses.

Almost all messages are made up of multiple packets. The sender breaks up large objects like a video or picture into groups of packets and then the receiver reconstructs the multiple packets into the original object.

This is very different from traditional telecommunications where the communications between end devices must be set up before they can communicate, and the network resources in between reserved for the duration of the communication. In the case of a traditional telephone network, the "circuit" is dedicated to the two nodes it connects for the duration of that connection.

Unlike the traditional telephony network the Internet's packet-based network does not have a dedicated linear connection between the two nodes. Instead, it formats the packets based on the rules for the Internet Protocol and then sends those packets through the networks independently of each other. The packets may get lost, arrive out of order or arrive at different times. As a result, instead of a dedicated communications channel, the Internet provides a "best-effort" service that can be used by a variety of hosts to communicate at the same time.

Packets on the Internet are made up entirely of 0's and 1's – called binary data because the information is encoded as a sequence of just two possible numbers.

2.3 The end-to-end principle

One of the fundamental design features of the Internet is called the "end-to-end principle." Simply put, the end-to-end principle asserts that packets sent into the Internet should reach their destination without modification or interference. The binary data that is sent should flow through the Internet's connected networks and reach their destination without change. The network should act like a pipe.

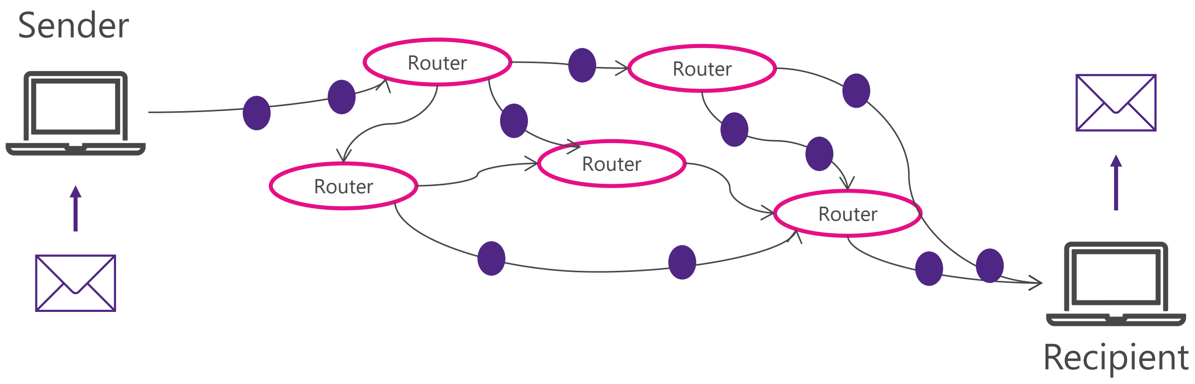
For example, if you request a web page from your local newspaper, the two endpoints might be your computer and the web server operated by the newspaper. The end-to-end principle requires that the Internet shouldn't modify the packets that return from the newspaper back to your browser. It guarantees that the web page you receive is exactly the same as the newspaper sent.

This puts a responsibility on the endpoints in the network. For instance, the endpoints become responsible for security. If an attacker sends you malware, it is up to your endpoint to detect and deal with the packets that make up the malware. The end-to-end principle means that the Internet is only responsible for delivering the packets.

That's very different from a phone network. If I call a friend, I dial a phone number that is in my friend's hometown. If she is away from home, the network knows that they need to re-route the call to the place where my friend is. This part of setting up the call requires significant intelligence and activity by the network. Once connected, the network takes my voice and converts it into a stream of packets over the established connection. In this case, the telecommunications network does a tremendous amount of work on our behalf.

One of the advantages of the end-to-end principle is permissionless innovation. If someone wants to improve and create new services on the Internet, they only need to change the device or application at the endpoints and not the entire network. New services that abide by the Internet's standardized protocols, can evolve and be deployed without having to make any changes to the underlying network.

Figure 2.1: Illustration of how packets travel over the Internet



Step1:
The IP Protocol breaks data into packets

Step 2:
The packets travel from router to router over the internet

Step 3:
The packets are reassembled into the original whole

Source: Plum

3 Internet before vs Internet today

3.1 Why old descriptions of how the Internet works are no longer accurate

Later in this paper we will see that the way we gain access to the Internet has changed dramatically in recent years. The emergence of fibre to the home, 5G home Internet services, low-earth orbit satellite access, and advanced Wi-Fi services make access to the Internet faster, more reliable, and more resilient than it has ever. The importance of mobile access to the Internet and the Internet of Things cannot be understated.

In addition to access to the Internet, a new set of services is being used to change the end-to-end principle. Many ISPs have experimented with providing access to the Internet that blocks out spam, filters out viruses, and removes objectionable content. While some customers valued these services, ISPs also found that there were customers who wanted their services unfiltered.

Other customers discovered that legitimate e-mail was accidentally being removed along with the spam and advertisements.

At the infrastructure layer, the Internet is more complex because of changes in the way performance is optimized and costs are lowered. Optimizations such as Content Delivery Networks enable content to be delivered more efficiently to the end user while still allowing the content to be controlled by the creator/publisher of the content.

3.2 How is the Internet model different from traditional telecommunications?

3.2.1 Technical model

The Internet contrasts sharply with traditional telecommunications models because of three fundamental principles:

- Connectivity is open to anyone and any organization that abides by standard protocols,
- There is no centralized control of the network, and
- The core protocols that make up the Internet are reasonably simple to understand and implement.

The Internet is open in a variety of ways, but most importantly, anyone can connect as long as they use the established protocols that govern connectivity and applications. These standard protocols are open and available for use by all – without the need to pay royalties or fees per use. Networks can connect by establishing business relationships for transit without having to acquire permission from any organization or individual. The public availability of the Internet's standards has a long history and tradition – perhaps most famously with the World Wide Web and Tim Berners-Lee[11] who deliberately created standards that were open, shared and to be extended by others.

The open model of the Internet allows for permissionless innovation: innovation can be brought to the networks without having to get the permission of any centralized authority. There is no central authority or organization that owns or runs the Internet. This means that there is no unintended overhead related to administering the network and no restrictions imposed by any central organization. This influences connectivity as well: there is no need to seek permission to have a new network connect to the Internet. Routing, as we have seen in later

[11] Sir Tim Berners-Lee is an English computer scientist best known for the invention of the World Wide Web.

sections, also works in a decentralized way, allowing networks to become available to others without having to register or pass tests.

The Internet's core protocols are built up from relatively simple building blocks that can be assembled to solve more complex application or networking problems. Using a building block approach means that each building block is independent and can be updated without affecting other modules in the stack. A modular approach may not provide the optimal solution in every use case, but it provides a general-purpose approach that meets a broader number of needs. In contrast, the telephone network offers an optimized approach to telephone calls with lower overhead and better service characteristics. However, that optimization does not extend to other applications, and the result is that the Internet successfully acts as a transport for a vast range of applications – including voice and video.

3.2.2 Economic model

As we have seen elsewhere, the Internet evolved with a much simpler model than telecommunications networks. The Internet evolved with just two models for the economics of connection. In the first, one provider positioned itself as a provider of services to another. This established a customer/provider model, and the customer paid the provider for the service. The other model had the two providers positioning themselves as near-equals and able to exchange traffic on the Internet at no cost to each other. We refer to the first model as the "transit" model and the second, "peering." Transit and peering are discussed in more detail in section 4.3.

This pair of economic models resulted in an arrangement of providers into groupings called "tiers." In general, the providers who are in the same tier had peering arrangements for interconnection and those that crossed tiers resulted in the lower tier network being the customer and the higher tier network being the provider. The tiers are not formally defined by any external agency or organization, and there is no guarantee about which ISPs would be in which tiers. Still, the result was that each ISP is primarily categorised into a tier based on the community of ISPs with whom they peer.

At the top of this classification were the backbone providers of the Internet that provided transit services for a very large part of the network.

An important part of this model is that the further the end-user is from the content they desire, the higher the cost of transit and the slower the delivery of that content. In today's Internet, the solution to this problem is to move the content closer to the consumer. Rather than pay to transit traffic to remote servers and data centres, large content providers are moving copies of their content closer to the user.

This is a dramatic difference from the economic model for traditional telecommunications which has no similar provision.

3.2.3 Regulatory model and public policy model

Unlike traditional telecommunications, the Internet is entirely decentralized: connecting networks together across the globe without concern for jurisdictional boundaries. A lack of centralized control means that explicit regulatory control by an individual government can sometimes be circumvented. If a website is removed in one country, it can be back in operation nearly instantly in another. If a document is removed from a website, it can be reposted on many more almost trivially.

The result is that many public policy and regulatory issues on the Internet often cannot be handled by traditional territorial, national institutions. The regulatory and public policy model for the Internet is usually not top-down but characterized by transnational cooperation between many stakeholders, including protocol engineers, ISPs, network operators, users, governments, and international organizations. National policies play an important part in shaping the Internet, but the Internet has also evolved new institutions and governance arrangements that respond to the unique needs of the network.

Internet governance happens at the global, regional, national, and local levels. As a basic rule, infrastructure and the technical layer of the Internet have a global approach to governance. Protocols, cables, and routers are maintained collaboratively by multi-stakeholder organizations that support the Internet as a cross-border and international technical structure. In contrast, applications and content are more susceptible to national or local governance mechanisms. As an example, regulating content that is allowed to be published or viewed online means that Internet users are subject to their countries' laws and regulations when going online.

In fact, there are varying aspects of regulation for Internet content, going from strict end (China) to less restrictive and this is enforced in various ways. For instance, it is still possible for many governments to block access to the Internet and this is done often with the cooperation of licensed ISPs.

Returning to the Internet and Internetworking (peering and transit), many countries have some form of licensing framework that defines who can provide transit services in the country. However, the underlying technical resources like IP and ASN numbers that are used to provide transit services (or peering) are not provided by the government. Instead, they are managed by transnational, multistakeholder organizations.

One of the most crucial aspects of Internet governance is a question of regulatory power: Who should have how much influence and control over the Internet's protocol layers and decision-making processes? This debate has two camps. On one hand, the United States, many Western countries, as well as private companies favour the multistakeholder approach where all stakeholders affected by the Internet should also be allowed to participate in its governance. The advocates of this view believe that the very nature of the Internet as a decentralized, global, and open system makes it too complex to be governed by governments alone and, as such, giving states too much control would pose the danger of restricted civil rights and liberties. On the other hand, governments such as China and Russia demand an increasing role for governments in Internet governance, particularly with regards to fighting (cyber) terrorism and controlling data: they contend that governments have more legitimacy than non-governmental organizations or the private sector in governing something as crucial as the Internet

3.2.4 Geographic and geopolitical differentiation

Another important trend is that local requirements are met through customizations in access, intermediaries, and content delivery. This has been detailed in Section 4.2.6 (Geolocation access control services).

For example, intellectual property requirements may mean that certain pieces of content (a TV show, a movie, for example) may only be shown to a certain group of users. Geolocation tools have emerged that attempt to identify the location of an end-device so that policy decisions can be made about delivering the content. If the customer is not allowed to have access to the content, it is blocked from being delivered.

Another example is the detection of content that must be blocked for regulatory reasons. In some jurisdictions, ISPs are required by regulation or law to ensure that certain classes of content cannot be delivered to an end-device.

The practical result of meeting these local requirements is that the Internet "looks different" depending upon your vantage point. In some situations, the differences result from contractual, intellectual property or other commercial arrangements. In other cases, the difference results from local or national regulatory action.

Some national governments are motivated to express public policy through regulatory approaches that include licensing of ISPs, transit providers and content providers. Other governments take a hands-off approach and allow market forces and public and private-sector enterprises to build industry-led best practices.

Very large content platforms face an all but impossible challenge: generating standards for acceptable speech that transcend borders and apply universally. From online child protection to hate speech and violent material, these larger platforms have tried to establish rules and implement content-moderation regimes that apply around the world. That these approaches have struggled to meet their goals is no surprise: the global speech standards suggested by online platforms are not the first time that tech innovators have tried to write global rules for speech. The problem for the large platforms is local, linguistic, and cultural. Today's Internet reflects a diversity that makes global standards for content nearly impossible.

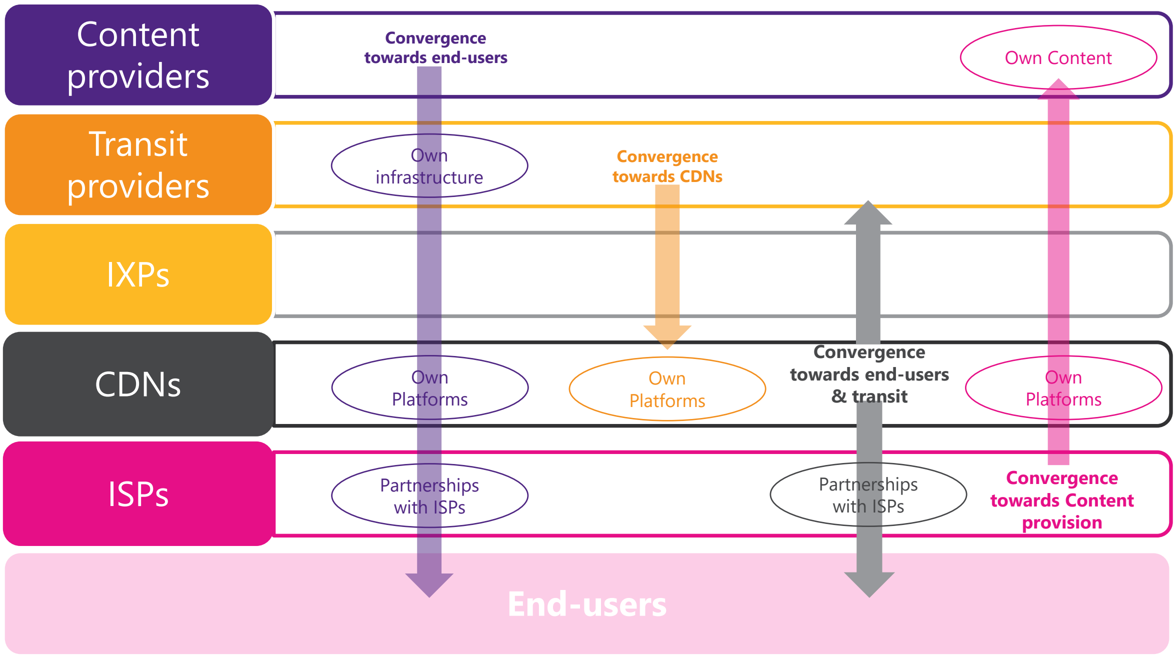
3.2.5 Stakeholders' roles

The Internet works by giving people and things access, providing peering and transit for packets across the Internet, allowing intermediaries to provide services on behalf of endpoints and by delivering content, services and applications.

Very large companies on the Internet play more than one role in this model. Hyperscale platforms, in particular, are also major providers of transit and intermediary resources. These platforms benefit by delivering the content and services of their platform as close to the user as possible. It is also true that large companies who provide access are also providers of transit.

In any case, the Internet's stakeholders can play many roles at the same time. In the private sector, this can be because a business model demands it or because playing more than one role provides the opportunity to deliver better content or services. Figure 3.1 below shows the stakeholder convergence trend that has been growing in the past years.

Figure 3.1: Internet stakeholders' convergence



Source: Arcep, Plum

Table 3.1: Internet stakeholders' convergence: the case of Orange

Internet stakeholders' convergence: the case of Orange

Orange, formerly France Télécom, is a leading French telecommunications multinational company. It has evolved from being a French publicly owned telecom incumbent to a global digital services provider with a presence alongside the Internet value chain through its numerous entities.

Besides mobile and fixed telephony, Orange provides mobile and fixed Internet access for both individual and enterprise customers in 26 countries. The company is also active at the international wholesale level under the Orange International Carriers (OIC) brand which operates a global connectivity network of 40 submarine cables stretching over 450,000 km as well as a wide system of PoPs, CDNs and terrestrial links. OIC is also a solution-provider for services in roaming, messaging, voice, bandwidth, IP and security to business customers that include ISPs, content providers and wholesalers[12].

The Orange group is also active as an intermediary service provider under the Orange Business Services brand (OBS). It operates 70 datacentres across the globe and offers a diverse portfolio of services including cloud infrastructure solutions, cloud applications management, business VPN services, Artificial Intelligence, and analytics services. The B2B entity also supports its customers with on-demand networks, including software-defined networking and network functions virtualization. Additionally, security is embedded in OBS solutions through the Orange Cyber Defence entity[13] which is the expert cybersecurity business unit of the Orange Group, providing managed security, managed threat detection & response services to organizations around the globe.

At the same time the multinational is also present at the content level through its own movie streaming platform OCS and is own production company Orange studios.

More recently Orange has also launched digital financial services including Orange Bank and Orange Money in various operating countries.

Categories	Content	Intermediaries				Interconnection	Local Access	
Elements		CDNs	IXPs	Managed Security	Cloud services	Transit services Peering	Internet access	VPNs
Orange presence	√	√		√	√	√	√	√
Orange entity	• OCS • Orange Studio	• Orange International Carriers		• Orange Cyber Defence	• OBS	• Orange International Carriers	• Orange • Sosh (MVNO)	• OBS

[12] https://internationalcarriers.orange.com/en/know-us-better.html
[13] https://orangecyberdefense.com/uk/about/

3.3 Permissionless innovation

Permissionless innovation on the Internet is reflected in many parts of the Internet's infrastructure. The lack of centralized control on the Internet means that individuals and organizations are free to take whatever approach they want in four key areas: infrastructure, equipment, services, and applications.

Infrastructure is the invisible category. The organizations that provide the backbone of the Internet, Content Delivery Networks, IXPs, transit and peering providers innovate to deal with change, develop services that are competitive and create brand new offerings that help connect networks, content, and stakeholders. Innovations in connectivity, routing, and the equipment that makes the Internet's infrastructure work come from large network operators, ISPs, CDNs and other content companies. Once again, that innovation comes to the public Internet without the intervention of any central authority and allows the infrastructure of the Internet to thrive and adapt to new circumstances.

Equipment is one of the most visible of the categories. Innovations in equipment have led to the dominance of mobile and personal connections to the Internet. The latest tablet or smartphone can connect to the Internet by simply following the rules of the protocols that rule the Internet and establishing a connection with a network provider. Innovations in laptops, tablets and smartphones are a visible part of this innovation. Less visible, but equally dramatic are the innovations that make smart cities, the Internet of Things or eHealth possible. The companies that build and sell equipment for use on the Internet constantly innovate to keep their devices interesting and useful to consumers.

Services are no longer the exclusive domain of large telecommunications companies. Instead, anyone with an idea and the energy to bring it to life can start providing a new service – without having to check with, pay royalties to or get approval from any other organization. Innovation in this space means that services are provided by an enormous range of private entities, start-ups, public authorities, and large corporations.

Finally, the rise of the application for the mobile Internet has made an entirely new set of tools available for individuals and enterprises. The emergence of app stores has allowed nearly anyone to develop applications and make them available to a wider audience than was ever possible before. Once again, the ability to develop and distribute apps, without intervention by a central organization, has allowed innovation on the Internet to prosper in ways that it could not on other networks.

Permissionless innovation is not anarchy. The Internet is possible because everyone who connects to it adheres to the fundamental Internet protocols. The protocols cannot be developed through anarchy – instead, they require collaborations, cooperation, and consultation. Those consultations are well-organized and developed in forums such as the IETF (Internet Engineering Task Force), ICANN (Internet Corporation for Assigned Names and Numbers), the Regional Internet Registries and the W3C (World Wide Web Consortium). These forums are available to anyone who wants to participate and get involved. The stakeholders include users, companies, vendors and even governments. All of these stakeholders participate on an equal footing.

3.4 Advantages of the Internet model

The Internet's permissionless innovation is a key advantage over other networking models. However, the Internet's design has four other key features that give it an advantage over other networking technologies.

The simplicity of the Internet Protocol means that it can run on top of almost any physical network. This gives the Internet the advantage of tremendous flexibility. The Internet runs over a huge variety of physical carriers including simple copper pairs, coaxial TV networks, cellular mobile systems, satellite systems and a wide variety of wireless networks. The advantage for the Internet model is that there can be improvements in the physical capacity of the underlying network without the need to change anything from the Internet Protocol to the application. In fact, it is this flexibility that results in the Internet Protocol dominating as the preferred method to transport most kinds of traffic, including traditional voice, video and other data.

Simplicity alone is not the only advantage: the Internet has scaled faster and more dramatically than any other network technology in history. Not only has the number of people and devices grown exponentially in the last twenty years, but the amount of traffic has increased dramatically. Once again, scaling the Internet is related to the independence of the layers that make up protocols on the Internet. Both the networks, and the applications that use them, can be changed or replaced without impacting the other.

If we use the common characteristic of the Internet as a 'network of networks" the growth rate would be in evidence by counting the number of distinct networks connected together. In 1986 there were 80 Autonomous Systems (AS) attached to the Internet, by 2000 the number had increased to about 10,000 and today the number is nearly 100,000.[14] This expansion combines growth in the number of users with an expanded geographic reach. In addition, to the number of networks, the Internet has also scaled up in capacity in the global backbone. Transoceanic cable capacity is primarily driven by growth in content and Internet applications and content providers are investing in the supply of that part of the backbone – those companies now account for about two-thirds of the total capacity of subsea cables.[15]

The Internet also has an advantage in adapting to new needs and requirements. Before the mid-1990's, information publication and sharing was difficult. The emergence of a new technology, the World Wide Web, meant that nearly anyone could publish on the Internet and that publishing application was available to anyone on the globe. The Web emerged as a dominant technology – so much so, that many users think the World Wide Web is the Internet. The Internet has the advantage of becoming the primary tool for distributing services. Traditional services, such as health care, travel reservations, schooling, watching movies or banking have moved from being associated with a specific location to being available anywhere. Support for diverse applications directly results from the permissionless innovation design principle.

Recently, not only has the Internet's scaling advantage been obvious, but so is its resilience in the face of unexpected changes or events. The pandemic has been the most dramatic unexpected event: traffic rates in some regions of the world increased by 50percent over the previous, pre-pandemic year. Working from home, home schooling and home entertainment all combined to create a sudden explosion of traffic. Developers of applications worked to change their applications to work in the face of increased volume. Operators of networks also increased network capacity in the face of the increase in traffic. Studies have shown that the deployment of increased capacity allowed end-users to maintain download speeds without implementing service guarantees or class of service rules. One reason for this resilience is that the Internet is decentralized, and the networks that make up the Internet are autonomous and able to respond to local changes in demand independently of other parts of the network. Another is that the Internet's topology contains no single, central point of control. There are multiple routes to most content on the Internet, and if one of those routes fails, other routes can provide needed content without other changes to the network.

Many interconnection agreements are informal and flexible on the Internet. This allows the Internet to be resilient in the face of unexpected events such as COVID, cable outages, and changes to the character of Internet use patterns. ISPs, online service providers, CDNs are able to flexibly negotiate means to deliver and receive traffic in the face of sudden changes by cooperating amongst each other. This resilience comes from decentralization as well as from flexibility in commercial arrangements between stakeholders – a situation different from that in traditional telecommunications networks.

[14] See "What will Happen When the Routing Table Hits 1024K?," Geoff Huston, https://blog.apnic.net/2021/03/03/what-will-happen-when-the-routing-table-hits-1024k/

[15] ibid

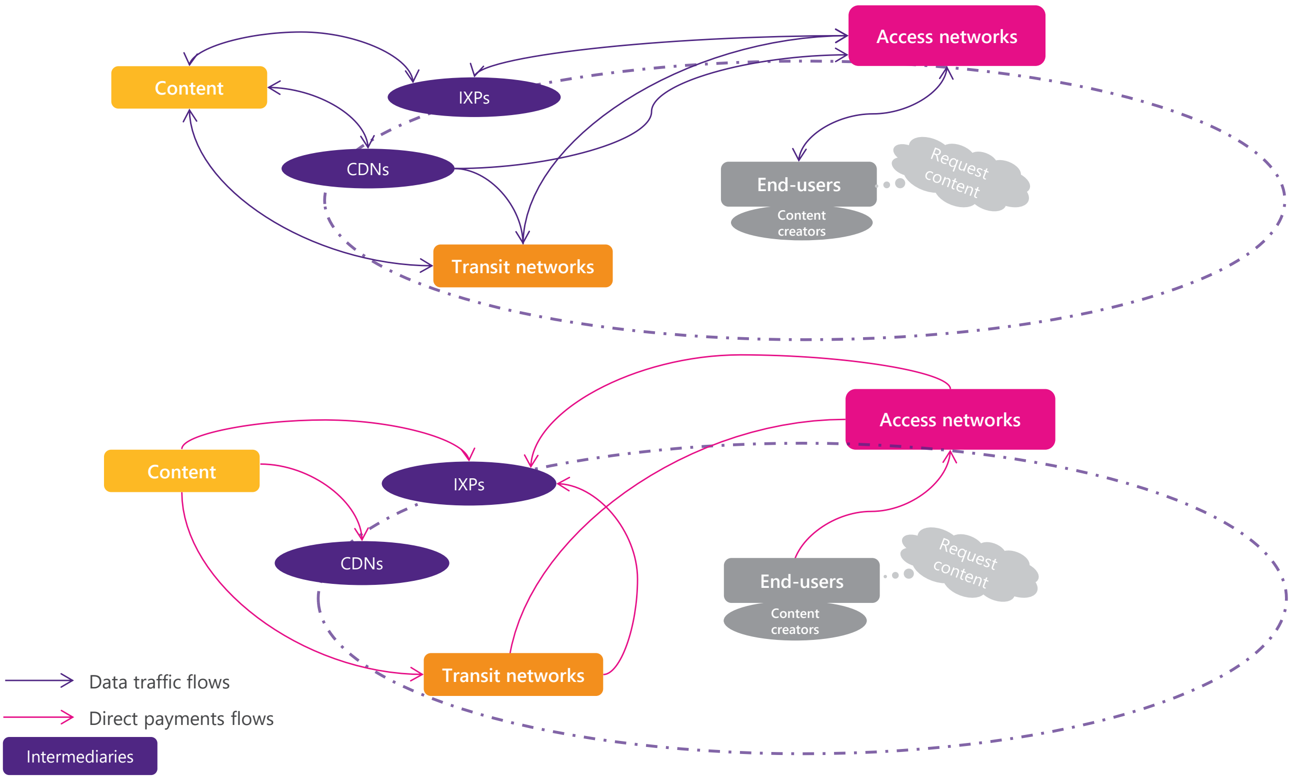
4 Four essential categories of Internet infrastructure

As described in the previous section, the modern Internet is very different from what it used to be thirty years ago. This evolution is not only a feature from the user's perspective (what can I do with the Internet), but it is also reflected in the new the Internet infrastructure that has seen the emergence of new services and new players (what is the Internet). In order to provide a simple yet comprehensive description of how the modern Internet works and how it is paid for, we have developed a taxonomy that reflects the variety of stakeholders that are involved in this complex ecosystem as well as the traffic-related and financial interactions between them (See Figure 4.1). Based on this taxonomy, the global Internet infrastructure is broken up in four essential categories of services:

- Access
- Interconnection
- Intermediaries
- Content

Among these four categories, it is important to highlight the role of network intermediaries: While the early Internet functioned without intermediaries, it is impossible to imagine the contemporary Internet without them.

Figure 4.1: Data traffic flows and payments flows in the Internet infrastructure.



Source: Plum

These categories of services can be viewed as the Internet value chain within which data traffic is moving to reach end-users. Each of these categories encompasses various elements and involves several stakeholders that can also be active in other categories as shown in Figure 4.2.

Figure 4.2: Break down of the Internet value chain.

	Content	Intermediaries				Interconnection	Local Access	
Elements		CDNs	IXPs	Network Security	Cloud services	Transit services & Peering*	Internet access	VPNs
Types of players	- ISPs - Media - Tech platforms - Applications	- ISPs - Tech platforms	- IXPs colocation - Shared data centres	- Firewalls - Filters - Content moderation	- IAAS - PAAS - SAAS	- Large ISPs - CDN providers - Tech platforms	- ISPs - MNOs - MVNOs - Satellite operators - Cable operators	- ISPs - Pure players
Examples	- AT&T - Netflix - YouTube - Sony - Spotify - Zoom	- Cloudflare - Akamai - Level 3 - Google - Netflix	- Extreme IX (India) - KINX (S.Korea) - DE-CIX - LINX - MICE	- Cisco - BlueVoyant - Symantec - IBM - NTT	- AWS - AZURE - Gmail - Salesforce	- Level 3 - Cogent - Telia Carrier	- Vodafone - Orange - AT&T - Jio	- NordVPN - Orange

*All elements described in this table participate in peering

The four categories are discussed in more detail in the following sections.

4.1 Access

The access category includes not only Internet access services provided by Internet Service Providers (ISPs) but also the VPN services that provide a secure and private network connecting one or more locations, local networks, or intranets together.

4.1.1 Internet access service

4.1.1.1 Service description

The local access level, often referred to as the connectivity last mile, is a localized transport service that connects end-users -- whether they are individuals or businesses -- to the main Internet backbone. In other terms, this is the portion of service between a customer premises and the ISP’s designated Point-of-Presence. ISPs own or resell facilities that bring Internet access to residential and business end-users who both consume and generate Internet traffic.

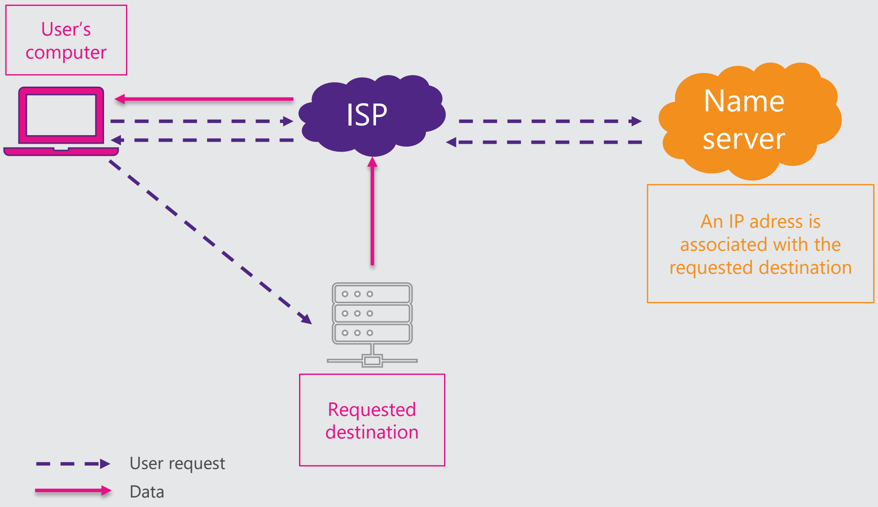
Local access links may use various underlying technologies that can be wire-based (fixed) or wireless (mobile) -- providing consumers with various modalities of access. Internet access can be categorised by data rates[16] (I.e., the speed at which data can be downloaded): Basic broadband with download speeds of more than 2 Mbit/s, standard broadband (SBB) with speeds of 10 Mbit/s or more, superfast broadband (SFBB) with speeds of 30Mbits or more. SFBB is also referred to as "Next Generation" services.

Table 4.1: Illustrative example of what happens when a single user wants to access a website

What happens when a single user wants to access a website?

Accessing an online website is equivalent to requesting information. It triggers a number of near-instantaneous actions by various stakeholders to move data online. Here is a simplified explanation of the mechanics involved when a single user wants to access a website.

To access the Internet, an individual user uses a web-enabled device, such as a computer or a smartphone. He has access to an Internet Service Provider (ISP) providing wireline or wireless access. The ISP takes the user's request to a nameserver. The nameserver translates a Uniform Resource Locator (URL)[17] into an IP address to be used in formatting the Internet Protocol packet Thus informed, the user's browser directs the query to the webserver with that IP address. The requested server responds by returning the requested data in packets, which are formatted to comply with a specific protocol used to interconnect devices on the World Wide Web. That data travels to the user's ISP, which delivers it to the user's device, where it is rendered by the device into a form the user can view.



[16] https://assets.publishing.service.gov.uk/media/56992242ed915d4747000026/BT_EE_final_report.pdf
[17] For instance, http://www.sony.com or mailto://someone@mailserver.net

4.1.1.2 Market Overview

Demand-side

At the local access level, Internet access is purchased by either enterprises or individual consumers. These two categories have different requirements as they have a different need for their Internet connection. Enterprise customers, for instance, usually require services with lower latency, higher reliability, and stronger resilience than individual customers. The modalities for access, including the underlying technologies and the pricing are therefore different for these two categories.

a Individual consumers

Individual consumers make up the largest slice of the Internet Access market. To access the Internet, individual users usually require an Internet-enabled device (a computer, a mobile or a tablet) and an access service from an Internet service provider (ISP). Access to the Internet can be through wireline (fixed) or wireless (mobile) technologies.

In the early stages of the Internet era, most users accessed the Internet over dial-up services, whereas today broadband Internet access has become more and more common, especially in more developed countries, enabling consumers to enjoy higher data rates and enhanced user experience. In addition, almost every mobile device is now provided with default Internet access services. Residential Internet access is faster, more reliable and has more options than even four years ago.

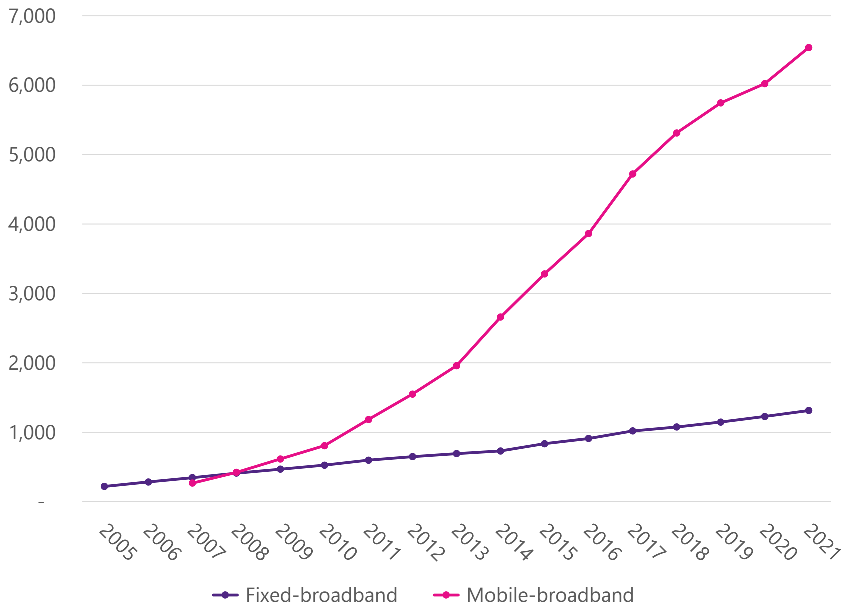
Broadband Internet has emerged as cable television companies have begun to offer cable modems and many local exchange telephone companies started offering various types of digital subscriber line (DSL) services. More recently, FTTx technologies and fibre networks have been at the centre of national connectivity strategies, particularly in Europe, where the number of subscribers is expected to reach 135 million by 2026[18].

b Demand is growing

The residential demand for Internet access has grown at an incredible pace and is driven by the range of online services to which consumers have access. These services have evolved over time and have changed the nature of activities that are possible online. The most notable changes are due to the rise of Web 2.0 businesses, social media platforms, the emergence of short and long form video, streaming, as well as online video games. Nevertheless, the demand for Internet access is heterogeneous. Individual usage and technical abilities vary from consumer to consumer, and this translates to a difference in terms of preferences toward access modalities and in terms of willingness to pay for Internet access services.

[18] https://www.ftthcouncil.eu/knowledge-centre/all-publications-and-assets/246/ftth-forecast-for-europe-market-forecasts-2021-2026

Figure 4.3: Fixed and mobile broadband subscriptions in the world, in millions (2005-2021)[19]

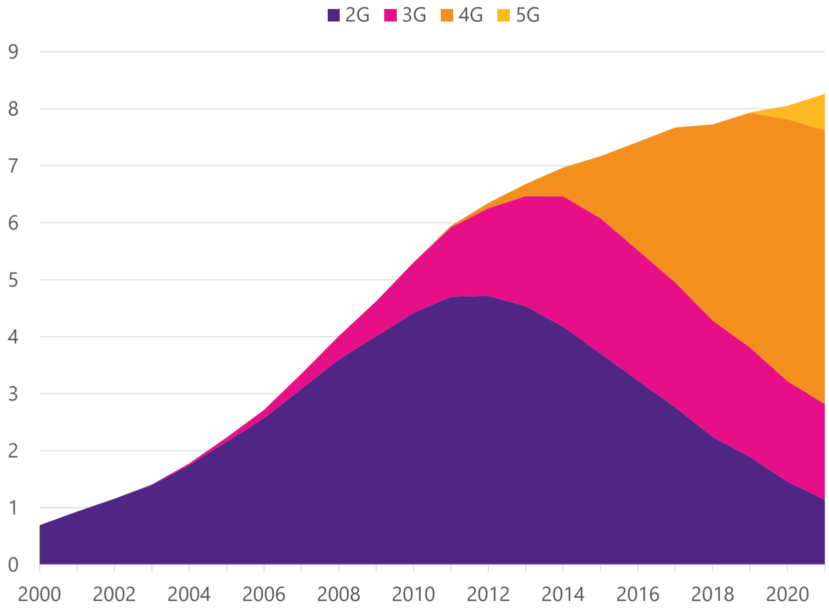


c Mobile is dominating.

Currently, at the global level, individual access is dominated by mobile, and this has been the case since the early 2000s, as shown in Figure 4.3. Fixed-broadband subscriptions have grown steadily while mobile-broadband subscriptions have significantly increased, driven by multiple factors such as the mass-market deployment of smartphones and tablets, the introduction of 3G/4G, and now 5G. Total mobile broadband connections by technology is shown in Figure 4.4. The ITU estimates that in 2021 there were around 1.3 billion active fixed-broadband subscriptions in the world, while the number of active mobile-broadband subscriptions was five times higher (6.5 billion).

[19] Source: ITU. 2021 figures are estimates

Figure 4.4: Total mobile broadband connections in the world by technology (200-2021)[20]



d Fixed and mobile substitution and complementarity.

There has been a significant amount of research on the level of substitutability and complementarity between fixed and mobile Internet access. There is no clear-cut answer: it depends on access capabilities and usage and varies by location of the user. When there is a tolerance for delays (electronic mail, passive or static browsing) fixed and mobile access can substitute for each other. This is not necessarily the case in data-intensive applications such as streaming or gaming, where delays can hamper user experience. There can also be complementarity such as when tweeting is encouraged during an online gaming event or streaming of content. However, it should be noted that there are a significant number of households that can rely only on a wireless smart phone or satellite Internet access. In any case, the extent of substitution and complementarity between fixed and mobile services is an important open topic of research[21].

e Enterprise consumers

Enterprises make up the next largest part of the Internet access market. Businesses use the Internet as a means to communicate with employees, customers and associates. The pandemic has had a role in the rise of telecommuting and making it possible for employees to work from home. This put significant pressure on access ISPs and the transit and peering networks that serve them. Businesses also have used the Internet to market to wider areas than would be possible with traditional marketing. The Internet has also made it possible for companies to enter into collaborations and research that would not have been possible previously.

Businesses generally have access to the Internet through two types of networks: shared and dedicated networks. The former type is the most common and is usually used by small businesses, or as a backup connectivity for larger organisations. Bandwidth of a common network connection is shared with other commercial users in the area.

Dedicated Internet access has emerged as the dominant solution for enterprises that require a reliable and permanent Internet connection. It is suitable for organizations that use the Internet to access mission-critical

[20] Source: GSMA Intelligence
[21] Greenstein (2020)

applications and business communication. The main benefit of using dedicated Internet access is Service Level Agreements between the ISP and the business that provides assurances of speed and reliability. Dedicated Internet access can also scale to meet a wide range of connectivity requirements with bandwidth from 1.5 mbps to 100 Gbps.

Supply-side

f Players

The supply-side of the local access market is characterized by the presence of a variety of network operators offering fixed and/or wireless connectivity services to end-users based on different access technologies. These players are:

- Fixed Internet Service Providers (ISPs), offering DSL or fibre connections
- Cable operators, offering Cable modem connections
- Mobile Internet service providers, also called Mobile network operators (MNOs) offering mobile data connections
- Mobile Virtual Network Operators (MVNOs)
- Satellite operators, offering Internet access through a satellite connection
- Fixed wireless services supporting direct connections between two entities over a wireless link

g Different modalities of access

Initially, Internet access was offered by ISPs or telephone companies through dial-up connections by using the underlying telephone network. Modems were deployed through central offices to convert analogue voice connections to Internet protocol data packets before routing those packets across the Internet. Dial-up access, also referred to as narrow-band, provided very limited data speeds and required the customer to initiate a phone call when willing to connect. Today Internet access is dominated by broadband services. The offers on the market vary greatly in speed and other characteristics. ISPs offer a range of speeds at different price points, and some are not available to all customers. Figure 4.5 below provides a description of the different Internet access modalities that are available today, as well as their advantages and disadvantages.

Figure 4.5: Internet access technologies

Access Technology	Advantages	Disadvantages
DSL Digital Subscriber Line (DSL) is a family of related services that are used to provide access to the Internet over telephone lines that were originally intended for traditional analogue service.	Easy to deploy because it uses standard telephone lines. Widely available.	Access speed is dependent on the distance between the customer and the access point as well as the quality of the telephone line itself. As a result, DSL is often slow or unavailable in rural areas.

Access Technology	Advantages	Disadvantages
Cable Internet access via cable users the coaxial cables that were originally intended to deliver analogue video to television sets. Cable-based ISPs use a standard called DOCSIS, which is an international protocol that allows for the same cable to provide high-speed data transfer on top of the existing video services.	Very widely deployed in urban and suburban areas and can achieve high bandwidth over existing cabling.	A technology in transition to fibre-based access. Cable providers find that DOCSIS has much slower upload speeds than download speeds.
Cellular and Mobile Internet Cellular services provide the last link in the service delivered by radio. It is called cellular because the area of radio service is divided into cells in a pattern based on terrain and reception characteristics. The technologies for Internet access have evolved in generations of wireless services given family names of 2G, 3G, 4G and 5G.	Radio towers cover wide geographic areas supporting mobility and use cases that wired connections cannot support. The current evolution to 5G is providing significantly higher Internet access speeds. 5G is also an access option for residential and, in some cases, residential networks.	Many mobile Internet services have "data caps" – limits of how much bandwidth you can use over the connection. In rural areas, mobile Internet services can be less reliable and slower because of the deployment of less radio infrastructure.
Fibre Optic Fibre-based Internet access services are currently the fastest way to deliver access to homes and businesses. Fibre is the key technology for the Internet's backbone and its use as an access technology means that there are no bottlenecks between the end-user and the backbone of the Internet.	The fastest access technology available and possibly a means to future-proof access strategy.	Requires significant investment to put new cable in the ground or on utility poles. Currently an expensive option for Internet access.
Satellite Internet access via satellite is provided by communications providers who own or lease capacity on satellites in Earth orbit. Those satellites in geosynchronous orbit require about a half a second for each pack to transit to the satellite and back to Earth.	Makes Internet access available anywhere on Earth. Some companies are experimenting with using satellites in lower Earth orbit to lower the latency between senders and receivers of Internet packets.	Expensive access technology that requires a "line of sight" between the user and the satellite. Existing technology has relatively long delays between sender and receiver and lower data limits for the access subscriber.
Fixed Wireless Unlike cellular technologies, fixed wireless uses wireless technologies to directly connect pairs of fixed locations (such as between an office and a radio tower). There are many technologies that support the connection of enterprises and users to the Internet using wireless.	A well-understood approach to Internet access, fixed wireless can be easier to deploy than putting cables in the ground or on utility poles. Fixed wireless works especially well in areas where there is an uninterrupted line of sight between the two endpoints.	Speeds for fixed wireless Internet access are often slower than wired services. Deployment of services requires initial capital expense and upgrades are also expensive.

4.1.1.3 Economic dynamics and relationships

a Market structures

Historically, and in most countries, the local access market was controlled by a monopoly telephone operator. Markets have since evolved to see the entry of competition and new players. Today, in most economies, the local access markets are moderately competitive, with competitive differentiation mainly based on price and speeds. Urban, high-density locations have experienced higher competition levels, and most consumers have access to two, three, or more Internet service providers.

One of the key aspects of the modern local access markets is the convergence of fixed and mobile: Operators tend to respond to demand for both fixed and wireless connectivity. For instance, a single stakeholder can act as an ISP offering fixed connectivity, while operating a mobile network, and also having an MVNO sub-brand at the same time. This convergence trend is illustrated by the growth of commercial offers based on bundles (triple play, quadruple play etc.).

Fixed and mobile networks differ in many aspects, which means there are different economic and business considerations for the operators. However, at the local access level, there are some common economic characteristics and dynamics for all the players in the market, and this will be the focus here.

Table 4.2: The local access market in Japan

The local access market in Japan

In Japan, for example, KDDI, NTT and Softbank are the three large Internet service providers[22] in the country holding 65% of the market share in terms of traffic, and the country has about 200 other ISPs of various sizes in the market. The three companies are also known as established mobile network operators and provide consumer and business services, as well as other digital and media businesses. In 2014, Rakuten Group, an e-commerce and online services player, entered the local Internet access market as an MVNO, offering low-cost voice and data services, and launched as a full MNO in April 2020. It relied on KDDI capacity to offer national coverage to support rollout of its own 4G network[23].

Additionally, there are more than 80 MVNOs[24], including 10 MNO sub-brands[25]. These MVNOs are supported by the three established MNOs and UQ Communications, a company specialising in the provision of WiMAX services. As of 2021 Q1, there were 26.12 million MVNO subscribers, which accounted for approximately 13.4percent share of the mobile market[26].

b Revenues and costs

First, in terms of revenue, the operators get paid by end-users for Internet access provision. End-users are generally charged on an unmetered basis through "flat rates" or on a usage basis. The flat rate for Internet

[22] The WIDE project in Japan surveyed a variety of residential, non-residential, exchange point and international providers and concluded that the Japanese marketplace is quite varied. Some of the reporting from the WIDE project is available at: http://www.hongo.wide.ad.jp/InternetTraffic/data/

[23] Telegeography, 8 April 2020, Rakuten Mobile launches low-cost mobile plans in Japan. Available at: https://www.commsupdate.com/articles/2020/04/08/rakuten-mobile-launches-low-cost-mobile-plans-in-japan/

[24] Source: GSMA Intelligence 2021

[25] This includes three KDDI sub-brand MVNOs, four NTT sub-brands, two SoftBank, and mineo. Source: GSMAi, 2021.

[26] MIC, March 2021, "Publication of quarterly data on number of telecommunications service contracts and market share." Available (in Japanese) at: https://www.soumu.go.jp/menu_news/s-news/01kiban04_02000187.html

access includes the Internet connection itself and the transfer of an unlimited volume of data[27]. In the early days, prior to the advent of broadband, most customers' monthly Internet access spending had two components: an Internet service subscription fee, and a metered fee related to the amount of time a customer was connected to the Internet[28].

In terms of costs, operators generally face very high fixed costs[29]. To reach end-users, operators need to either build their own last-mile infrastructure or rent/lease that infrastructure from another operator. For fixed networks, the physical environment and population density are important cost drivers. This means network deployment is more expensive in some areas than others. In the case of fibre, the more homes a single fibre loop passes, the less expensive it will cost to serve each one. The example of an apartment building is useful to understand the importance of population density: hundreds of homes can be served by bringing one fibre connection into the building. This is one reason why Japan and Korea, which have a high portion of their population in a few urban areas dominated by apartment buildings, have such high fibre penetration relative compared to the rest of the OECD[30].

The delivery of a single unit of incremental traffic for operators is a function of multiple variables. This cost is different from one operator to another, and it is not unusual that operators themselves don't fully understand it. Network dimensioning is usually based on peak-hour capacity requirements.

c End-user price variation

In terms of end-user prices for Internet access, there is great variation across different regions of the world. These disparities can be explained by the differences in terms of regulatory regimes, competition levels, infrastructure development and consumer bases. Figure 4.3 shows the median prices by Internet access type for ITU country groupings.

Figure 4.6: 2020 median prices for various Internet access type for ITU country groupings, in USD[31]

Basket	Africa	Arab States	Asia & Pacific	CIS countries	Europe countries	The Americas	World
Fixed broadband	$ 22.30	$ 19.73	$ 20.26	$ 5.61	$ 22.39	$ 28.40	$ 22.79
Mobile broadband data-only	$ 6.15	$ 13.00	$ 7.18	$ 3.71	$ 11.90	$ 11.30	$ 8.72
Mobile data and voice high usage	$ 13.81	$ 17.18	$ 13.41	$ 4.39	$ 18.08	$ 26.29	$ 16.48
Mobile data and voice low usage	$ 8.45	$ 11.53	$ 9.66	$ 3.53	$ 15.42	$ 19.66	$ 11.95

Note: The fixed broadband basket is based on the cheapest fixed-broadband subscription offered in a country with a minimum of 5GB monthly usage and an advertised download speed of at least 256 Kbit/s

[27] Some operators protect themselves against intensive use by reducing the maximum speed of data transfer for the remainder of the month once a certain monthly data volume has been exceeded.

[28] https://www.cisco.com/c/dam/en_us/about/ac79/docs/sp/Rethinking-Flat-Rate-Pricing-for-Broadband.pdf

[29] When operators build their own infrastructure, variable costs are then low. Another possible model for operators is to lease infrastructure from another operator, in this case there are no fixed costs and ongoing Opex.

[30] https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/CISP(2013)8/FINAL&docLanguage=En

[31] https://www.itu.int/en/ITU-D/Statistics/Pages/ICTprices/2019default.aspx

4.2 Intermediaries

Intermediaries are network resources in the path of end-to-end communications that provide services to either or both endpoints.

Two examples of intermediators are the Content Delivery Networks discussed in section 4.2.3 above. The goal of CDNs is to provide faster, less expensive, and more reliable access to popular content and applications. CDNs are deployed around the globe by commercial and private operators. CDNs often connect at Internet eXchange Points (IXPs) where ISP are linked together for the purpose of exchanging traffic between networks. Having a connection to these high speed and highly interconnected locations, a CDN operator is able to reduce costs and transit times for the delivery of popular content.

A second example is security services provided by the network rather than deployed at an end node. Many companies now offer tools that provide security services for a network as a whole rather than for individual endpoints. The benefits to the network of using this type of intermediary can be reductions in operational costs, expansion of security capabilities, improvements in detection and response to threats and, where needed, compliance with regulatory rules.

Examples of this second type of intermediary are services that attempt to filter objectionable content or malware before it is delivered to an end-user. Typical implementations use a combination of fingerprinting, traffic pattern analysis and machine learning to identify malicious content/traffic while it is passing over a connection between endpoints. The challenge of this example of intermediary is to provide service in the end-to-end communications channel while minimizing the impact on the end-user.

As we said before, while the early Internet functioned without intermediaries, it is now impossible to imagine today's Internet without them.

4.2.1 Who are the stakeholders?

4.2.1.1 End-users as stakeholders for intermediaries

In the case of an intermediary such as a Content Delivery Network, end-users get the benefit of better performance for the following reasons:

- The network distance between where the content is stored and where it needs to be delivered is smaller
- Files sizes can be reduced to increase the speed at which content is loaded
- Server infrastructure can be optimized to respond to user requests more quickly.

In each case, the user benefits from faster speed, lower cost and higher reliability because the intermediary can deliver the content rather than have it traverse the entire distance between source and requestor.

End-users also benefit from higher reliability. CDNs balance the load of commonly and frequently used content. When some servers go down, the replicated content in the CDN means that the content can be served from another source.

In the case of managed security services, end-users profit by having predictive security protection, updated protection against threats and access to security intelligence that would be otherwise unavailable at the endpoint. An ISP that provides filters and access control is more likely to have the resources to keep those protections current and effective against emerging threats.

Managed security services also provide the end-user with some (but not absolute) certainty that illegal content will be filtered before reaching them. When ISPs use managed security services, they are able to make policy decisions about the content that may be of value and interest to the consumer. Those same policy decisions may result from the ISP complying with regulation that makes network access safer or potentially less abusive.

Intermediaries can also serve as a resource for privacy for the end-user. An intermediary can relay requests for content through a third party and have the content for those requests delivered without the server or application provider knowing who had requested the content. Some Internet intermediaries perform an important privacy service on behalf of end-users – sometimes without the explicit knowledge or intervention of the end-user

4.2.1.2 Enterprises as stakeholders for intermediaries

When enterprises connect to the Internet, they have different requirements than end-users. As a result, the services they get from Internet intermediaries are different.

Importantly, enterprises use intermediaries to outsource the running of enterprise services and applications. Cloud services providers, essential to large-scale enterprises, provide shared, distributed compute, storage and applications services outside the enterprise's own network. This trend, called virtualization, makes it possible to run a "virtual" service in a shared network environment on the Internet. The motivations for the enterprise are scalability, reliability and better services to employees and customers.

It is also very common for enterprises to use managed security services provided by an intermediary. Such services have access to potentially better and more up-to-date tools than the typical individual enterprise. The intermediary also may have access to predictive information that will help avoid attacks on both shared network services and the enterprise's own network.

By using cloud services as intermediaries, enterprises can also deliver applications to end-users without exposing the enterprise network to risk. Some intermediaries can separate traffic intended for a particular service or application from all the rest of the enterprise's Internet traffic – resulting in less risk to the enterprise and to the application itself.

Smaller enterprises use special-purpose computing platforms to perform specific tasks (for instance, identifying malware or spam on incoming email messages). These "appliances" generally are difficult to scale as the enterprise grows. Larger enterprises use managed security services to replace the cost and complexity of adding the appliances directly into the enterprise network.

4.2.1.3 Access providers as stakeholders for intermediaries

Access providers get many of the same benefits from intermediaries that end-users do. Performance and reliability improvements mean that the quality of access service is improved for the customer – lowering support costs for the access service.

In addition to those benefits, access providers also cost savings from not requiring as much bandwidth needed for transit. Since many ISPs have to pay for some of their transit, any use of a CDN means less traffic over paid transit connections. In this way, use of the CDN lowers the overall costs of transit for the ISP.

CDNs are also especially well-suited to defending from DDoS attacks. When an attacker sends huge amounts of data at a target website, an individual website is easier to overwhelm than a network of servers, each providing replicated content.

Access providers are also stakeholders for intermediaries that support regulatory requirements related to filtering of content

4.2.2 What are their motivations?

The enterprises that support intermediaries see business opportunities in a variety of areas.

In addition to traditional CDNs, many companies that support intermediaries also support direct-to-consumer services such as video conferencing or replacements for conventional telecommunications (OTT). Direct-to-consumer solutions help spread the workload for general-purpose services and tune the delivery of special-purpose services. Once again, the intermediary is providing a service that, if not available, would be difficult to provide from a single point on the network.

Video distribution has become especially important in the pandemic. The volume of video being consumed has skyrocketed in the last two years. Intermediaries provide virtual platforms for video distribution, including cloud-based video distribution and video-on-demand from delivery networks. Supporting video distribution in an end-to-end model without intermediaries, would be nearly impossible because of bandwidth and service requirements. In addition, virtualized services allow for updating important software (for instance, codecs) that make video delivery more efficient.

From the user perspective, the critical motivations for intermediaries are speed of accessing content and applications, reliability of access to that content, and reduced cost of access. Elsewhere in this report we have documented that, if the content is closer to the user (from the point of view of the network), then the user quality of experience is typically higher, which may include faster delivery, lower latency or reduced packet loss. This also results in benefits for content not using CDN platforms - there is now more capacity on long-haul and international links for the long tail of content that is not using CDN platforms.

Users are likely unaware that optimising delivery between the user and the application or service can make Internet access less expensive. By delivering content or applications more locally than typical, the traffic doesn't have to traverse long network distances over, potentially, expensive transit connections. Eliminating or reducing the dependence on expensive transit connections results in immediate savings to the ISP. The ISP can then be more competitive in the marketplace by reducing the cost of access to the consumer.

Content providers also benefit from some of these same characteristics: higher quality access to applications, service and content. Using intermediaries also means that content providers who used to have mainly local reach, can now extend their local content toward a global audience. By taking advantage of existing shared network services, the content provider is spared the expense of having to build out network resources of their own – concentrating instead on the core competency of the organization: provision of the content, application or service.

4.2.3 Content Delivery Networks

4.2.3.1 Service description

Content Delivery Networks (CDNs) have become a major stakeholder of the value chain of the Internet by contributing to a more regionalised Internet interconnect that relies less on international transit. The increasing volume of content going through the world Internet in the past few years has entailed two main issues:

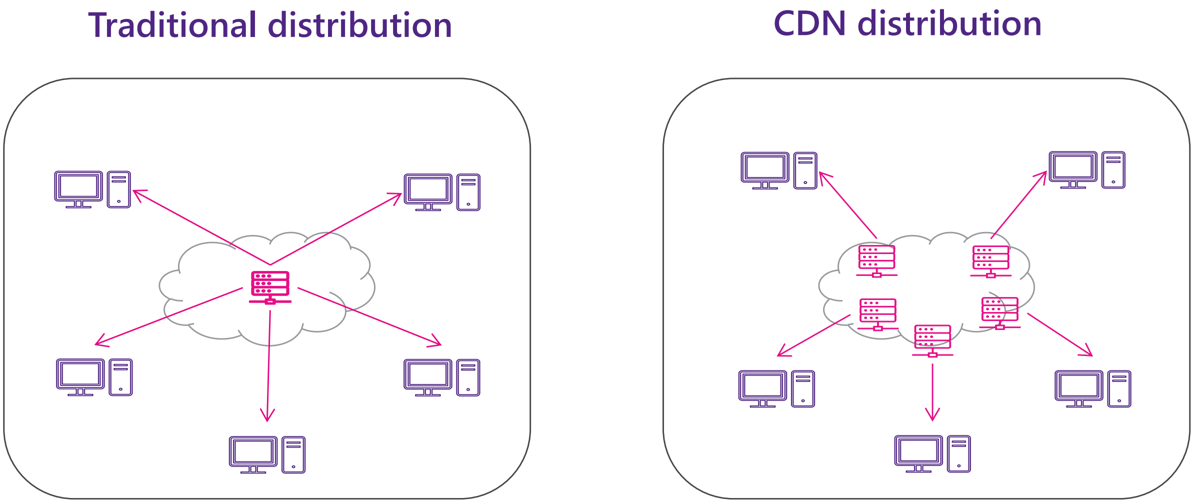
- One technical: the latency of content delivered has increased, resulting in a lower quality of service to the user
- One economic: the cost of content delivery has increased.

In this context, CDN services have emerged to move the content "closer" to the final user for improved delivery. CDN is a network of servers (called edge servers) that has been deployed in different geographical locations that cooperate in providing content/data to their users (Figure 4.8), by handling traffic loads and reducing time of content delivery, through a process of replication. The CDN determines the shortest possible route between the user and the web server (located at the edge of the Internet) based on indicators like proximity, speed, or latency.

Consider the two broad types of content:

- Static content (e.g. audio recordings, YouTube videos) can be stored in multiple places. Caching is the mechanism of storing static content (after the first request for the resource is served to the end-user) in a location for serving future requests for the same source. In a caching server, the client does not have to fetch the static content the second time. Instead, it provides the data from a copy located in its memory (or, cache).
- Dynamic content (e.g. video calls, media streaming, online gaming) can't be stored. To deliver dynamic content, CDNs' Points of Presence (PoP) are used to optimise the route traffic takes between the two endpoints of an application, through localised peering between networks including ISPs.

Figure 4.7: Comparison between traditional distribution and CDN distribution[32]



Source : Kanoha — Travail personnel, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=7868809, Plum

[32] Another model to note is the peer-to-peer CDN, where the content is hosted in the user's computer (e.g. Emule, BitTorrent), but this is not particularly popular anymore.

CDN services are value-added services, as they enable optimisation of web delivery through bandwidth cost reduction and improvement of user experience (for services sensitive to delays and bandwidth stability). They also appear to be a "mandatory" service to use for large scale content providers if they want to be competitive.

CDNs provide benefits to end-users (by enabling lower latency and thus better quality of service), to content providers (through better service reliability), and to ISPs (by lowering traffic cost). For instance, CDN's benefits are essential for the gaming industry to provide quick and responsive downloads to gamers.

4.2.3.2 Market overview

Gourdin et al.[33] underlines that a number of CDN are now part of the biggest contributors to Internet traffic globally, while this ranking only included ISPs a few years ago.

Initially, CDN were independent companies managing the service for third-party businesses.[34] More recently, the market has been rapidly evolving: It has grown from USD 1.81 Billion in 2016 to USD 6.23 Billion by 2021, at a Compound Annual Growth Rate (CAGR) of 28.0 percent[35], with North America as being the largest market and Asia Pacific having the highest market growth[36]).

The CDN market development is due to different drivers[37]:

- On the demand side, the ubiquitous use of mobile devices to produce and use content, and the continuous growth of content consumption[38], and

- On the supply side, content and service providers are looking for new revenue streams and to compete with hyperscale providers.

4.2.3.3 Supply-side: The CDN's market stakeholders

The number of CDN companies has recently been estimated at around 170 globally[39]. Some CDN companies leverage the infrastructure of already established CDN companies to propose their services. Other companies have developed self-owned, self-managed private CDNs. Four types of market players have been identified as operating in CDN services:

- "Pure play" CDN market players (e.g. OVH, Cloudflare, Fastly, Akamai Technologies, Level 3, Limelight Networks) develop, deploy and operate CDNs as their primary businesses, relying on a great understanding of content delivery issues. The market has then shifted towards vertical integration of CDN activity with new entrants including telco CDNs, hyperscale companies and large content providers.

- "Telco CDNs" have been developed by telecom operators and equipment vendors: e.g. Ericsson, SFR Business (France), Orange Business Services through a partnership with Akamai. Telcos rely on their wired and wireless networks, their backhaul networks and their numerous self-owned points of presence, within a fast-growing mobile industry.

[33] Eric Gourdin, Patrick Maillé, Gwendal Simon, Bruno Tuffin. The Economics of CDNs and Their Impact on Service Fairness. IEEE Transactions on Network and Service Management, IEEE, 2017, 14 (1), pp.22-33. 10.1109/TNSM.2017.2649045. hal-01398923v2

[34] More recently, hyperscale companies have developed their own CDNs for delivering their own content and in some cases to supply third-party companies with CDN services.

[35] Markets and Markets (https://www.marketsandmarkets.com/Market-Reports/cloud-content-delivery-network-cdn-market-208477558.html)

[36] *For more detail see here: https://www.mordorintelligence.com/industry-reports/cloud-cdn-market*

[37] http://www2.onapp.com/rs/017-CKO-601/images/CDN_whitepaper-$15bn_opportunity_for_service_providers_OnApp.pdf

[38] Large mobile operators are huge users of cached content and of their own CDNs.

[39] December 2021, Source : https://tracxn.com/d/trending-themes/Startups-in-Content-Delivery-Network-(CDN)

- Hyperscale companies have developed their own CDNs: e.g. Google Cloud CDN, Baidu AI Cloud CDN, Amazon CloudFront, Azure CDN (Microsoft). These companies rely on their networks of very large data centres. In recent years, they have developed extensive private peering partnerships with individual ISPs, as well as connecting to IXPs, and rely less on international transit. This is a way for them to deliver content closer to the end-user.

- Large content providers (or Over-The-Top streaming services) operate their own CDNs -e.g. Netflix (through Open Connect) - while sometimes keeping using "traditional" CDN services.

The way CDN services are marketed depends on both business and technical decisions, as well as security and reliability issues. Some service providers have developed a CDN for their exclusive use (e.g. Netflix), others will share their infrastructure with third parties. Some companies use the CDN infrastructure of an existing company, develop their own CDN offer, and market it as a separate service. This is called virtual CDN services. In China, mobile operators allow their infrastructure to be used by third parties who then market their own virtual CDNs.

4.2.3.4 Demand-side: CDN's users

Quality and volume of data are the main drivers of CDN demand. CDNs are used extensively by companies like ISPs, social networks, media and entertainment websites, online broadcasters, e-commerce websites, or educational institutions to serve content quickly to users in different locations.

As a CDN services user, different strategies can be considered to avoid outages and disruption when peak traffic and content consumption are high[40]:

- With a managed CDN strategy (outsourced service), the content provider relies on one or more CDN service provider(s) to manage the end-to-end service (third-party pre-packaged service offering This strategy has the benefit of providing good performance while leaving the provision and control of the CDN infrastructure to an outside entity. In a multi-CDN strategy, the important decision on how to distribute flows between the different CDN companies is done by software, either through internal or external expertise.

- Having its own CDN strategy (insourced service) requires expertise and CAPEX investment to build a distributed infrastructure, while offering greater control over infrastructure and content. For companies with already a distributed network, like telcos, deploying CDN services can bring value, first to provide the service for potential clients and monetize the service, second to use their CDN for their own purposes and thus reduce costs. This has been a choice made by some major content providers like Netflix.

- Some users have a hybrid approach and use a mix of multi-CDN and own CDN strategies.

[40] https://www.medianova.com/en-blog/multi-cdn-vs-managed-cdn-vs-diy-cdn-what-to-choose/ and http://www2.onapp.com/rs/017-CKO-601/images/CDN_whitepaper-$15bn_opportunity_for_service_providers_OnApp.pdf

Table 4.3: Case of a CDN use by a media company

Case of a CDN use by a media company: The example of TV5MONDE and Orange Media Delivery Boost[41]

TV5MONDE is an international French-language TV channel which offers, among other services, access to a large catalogue of videos on its mobile app across several African countries.

In order to enhance user experience on its application, the media company uses Orange Media Delivery Boost service, which uses the Orange CDN to optimise web content delivery. Benefits include a low latency within the MEA region, a single contract to use any Orange Content Points of Presence and bundling opportunities with Orange retail offers. With Orange being committed to contributing to content delivery improvement in Africa, the company has committed to provide new content PoPs and support the development of TV5MONDE

On the demand side, it is also important to note that CDNs have played an essential role in dealing with the enormous traffic increase during the COVID-19 pandemic that the world has faced in the past couple of years. By serving up local content, ISPs and network providers don't have to gather more bandwidth for all the traffic generated by people at home (people working from home, movies and TV shows watched during lockdowns). There would have been no way to put infrastructure in the ground rapidly enough to meet that demand in such short periods of time. Instead, much of that demand was met with cloud services and CDNs.

4.2.3.5 Economic dynamics and relationships

The economic dynamics of CDN market, the complex relationships between stakeholders and their motivations have not yet been analysed with rigorous methodologies - despite the growing role of CDNs and the fact that technical performance of CDNs have been extensively studied[42,43].

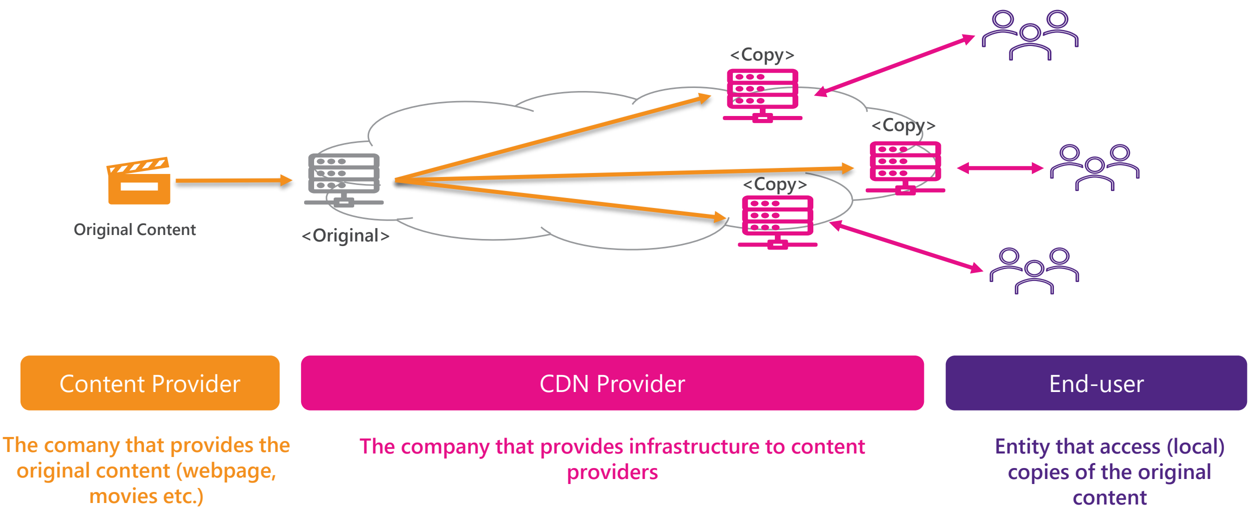
The figure below shows a simplified scheme between the content provider, the CDN service provider, the Internet access network provider, and the end-user. CDNs are placed within regional data centres for content to be delivered from a point that is topologically closer to the user, which raises the crucial role of data centres.

[41] https://www.orange.com/en/newsroom/press-releases/2019/tv5monde-chooses-orange-media-delivery-boost-optimise-end-user-mobile

[42] Eric Gourdin, Patrick Maillé, Gwendal Simon, Bruno Tuffin. The Economics of CDNs and Their Impact on Service Fairness. IEEE Transactions on Network and Service Management, IEEE, 2017, 14 (1), pp.22-33. 10.1109/TNSM.2017.2649045. hal-01398923v2

[43] Behrouz Zolfaghari, Gautam Srivastava, Swapnoneel Roy, Hamid R. Nemati, Fatemeh Afghah, Takeshi Koshiba, Abolfazl Razi, Khodakhast Bibak, Pinaki Mitra, and Brijesh Kumar Rai. 2020. Content Delivery Networks: State of the Art, Trends, and Future Roadmap. <i>ACM Comput. Surv.</i> 53, 2, Article 34 (March 2021), 34 pages. DOI: https://doi.org/10.1145/3380613

Figure 4.8: Simplified scheme between the CDN and other players


Original Content
<Original>
<Copy>
<Copy>
<Copy>
Content Provider
CDN Provider
End-user
The comany that provides the original content (webpage, movies etc.)
The company that provides infrastructure to content providers
Entity that access (local) copies of the original content

Source: Plum, Ofcom[44]

From a regulatory point of view, Gourdin et al.[45] underline that CDN have an ambiguous role in net neutrality: Because its purpose is to maximize its profit, the CDN will be inclined to go to the most paying content provider, which can have an impact on the quality of experience of the end user. The authors call for including CDNs in the debate on net neutrality.[46] However, others consider[47] CDNs as an essential optimization that has allowed the Internet to scale efficiently. Traffic served from CDNs reduces load on core and international network links, leaving more space for services that are not using CDN platforms.

Business models

From a general point of view, the following elements can be noted:

- The content provider will need to find a trade-off between investing in bandwidth and investing in regional storage capacity (whether through a third-party CDN or an insourced CDN).
- As CDN enables to improve quality of service (bandwidth stability and low latency) for the final user, it brings a potential revenue increase for the content provider (e.g. media sites, social media, e-commerce) through improved customer acquisition and retention.
- For the Internet access provider, CDN saves a significant amount of money because using international transit for each content user request is not necessary anymore.

This section explains two main CDN business models.

a The "buy" model

[44] Based on OFCOM (https://berec.europa.eu/files/news/ofcom_ipic.pdf)

[45] Eric Gourdin, Patrick Maillé, Gwendal Simon, Bruno Tuffin. The Economics of CDNs and Their Impact on Service Fairness. IEEE Transactions on Network and Service Management, IEEE, 2017, 14 (1), pp.22-33. 10.1109/TNSM.2017.2649045. hal-01398923v2

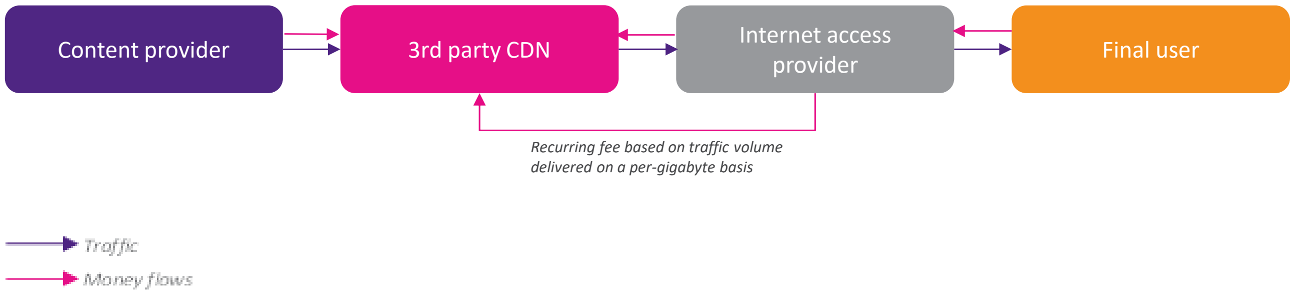
[46] Ibid. For instance, the authors say, "there is a significant amount of power and control at stake in content delivery, and it is inevitably a market controlled by the few that have the scale and capital to make content delivery a successful business. Because of that, there will always be concerns over how companies exercise that power. "

[47] https://publicpolicy.googleblog.com/2008/12/net-neutrality-and-benefits-of-caching.html

The “buy” model is a CDN outsourcing model, where the CDN user does not have to have its own infrastructure. The CDN service provider deploys streaming assets at different places of the infrastructure of the Internet service provider for a recurring fee, usually based on the volume of traffic.

There are different types of agreements between stakeholders that depend on their size in the market. An Internet access provider will negotiate differently with a small CDN provider than with a larger CDN player. The CDN company may have to pay a fee to the access provider to rent a rack in its colocation centre or can have an agreement with the access provider based on resource exchanges in a federation formed by access providers and CDN companies. Given the savings made by Internet access providers from using a CDN, they do not typically charge the CDN for paid peering.

Figure 4.9: CDN “buy” model



In this model, the Internet service provider has no control over the traffic sent by the content provider

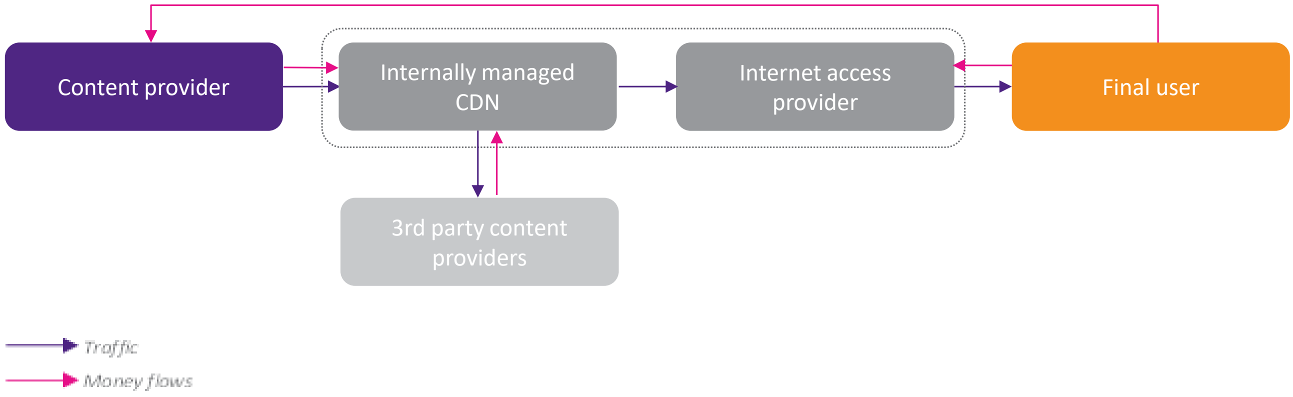
b The “build” model.

The CDN market has high entry barriers as it requires large Capex investment to reach a national or a worldwide footprint, added to the cost of running the service. Because they have a global distributed infrastructure in place, telcos have a strong competitive advantage. They can place servers at the edge of the network, closer to subscribers' access to the network, thus limiting traffic on the main arteries of the network. This deep positioning of edge servers is not possible for traditional CDN companies unless they have a strategic agreement with a telco. Another advantage is that a telco does not have to pay bandwidth to another operator for traffic to edge servers that pass over its network. On the contrary, the traditional actors of the CDN must rent this capacity from the providers of networks that connect their various points of presence. Thus, the telco would save money on backhaul and also save money on traffic transiting other networks.

These advantages also apply to other companies with their own distributed networks in place: For example, a video uploaded to YouTube in Hong Kong and later watched in South Africa, would be uploaded to Google’s servers, then distributed to Google’s CDN network where the South African user fetches it from a local server. The video would transit mostly private links.

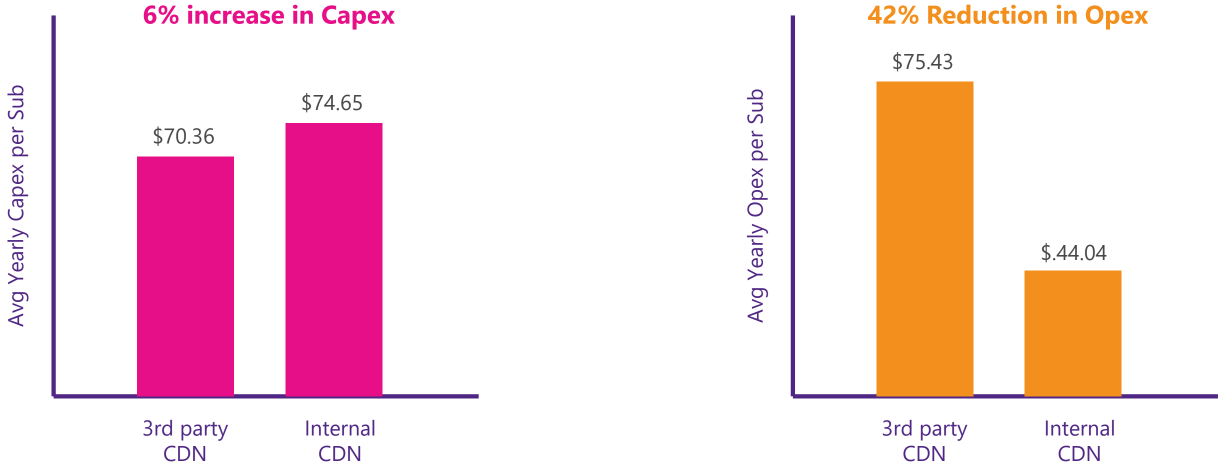
The “build” model, with a CDN insourced by the content provider or by the Internet access provider (example in Figure 4.10), may, optionally, enables the company to generate additional B2B revenues by selling enhanced CDN services to third-party companies. Not all CDN providers do this, (e.g. Netflix does not), as their CDN is highly optimised for their own content. It also enables cost optimisation (e.g. telcos use internal CDN to control traffic flow across their infrastructure and reduce costs, which is not possible with an outsourced CDN), which is why telcos and hyperscale companies enjoy a lower average cost per transaction than traditional CDNs.

Figure 4.10: CDN "build" model



Total Cost of Ownership. Cisco has examined the Total Cost of Ownership[48] (TCO) of both models over a period of 6 years for a hypothetical large network operator (see Figure 4.11). They have found that an internal CDN brings a 6 percent increase in Capex and a 42 percent reduction in Opex.

Figure 4.11: Total cost of Ownership of "Build" Versus "Buy" CDN Models[49]



c Pricing Schemes.

CDN offers vary according to the provider. They are difficult to compare as they are usually bundled with other services like storage, API management, geo-blocking features or security services[50].

The pricing scheme can be:

- a monthly fee (ex. OVH as from 9.99€ per month tax excl. for 3 points of presence, dedicated IP address, and storage in connected network); or

[48] Wholesale content delivery networks: unlocking revenue streams and content relationships, White paper, Cisco, 2012

[49] Source: Source: Wholesale content delivery networks: unlocking revenue streams and content relationships, White paper, Cisco, 2012

[50] What are the top CDN benefits for today's enterprise ? Kevin Tolly, https://www.techtarget.com/searchnetworking/feature/Content-delivery-network-services-The-benefits-of-CDNs

- a pay per volume (ex. Google's caching prices are given per gigabyte or by the number of requests to HTTP/HTTPS cache), with decreasing prices by range of terabytes.

Prices depend on the region of the world (Europe, Asia Pacific, China, etc.)[51].

CDN services used to be very expensive for content owners but are in the reach of smaller content providers (local music producers, local newspapers, etc), as CDNs have become commoditised. This is due to the market development and corresponding economies of scale done by CDN providers, as well as technology improvement (costs of computing and storage have both decreased). CDNs now offer pricing models with pay-as-you-go options (for instance, for the distribution of a blog)[52].

4.2.4 Cloud-based services

4.2.4.1 Service description

This section covers cloud-based services[53] which enable data storage, computing and virtualization of services. These services include giving access to a scalable cloud space and virtual computing resources, where the user can store files and folders in a user-friendly environment. Security features of these services include on-going data backups, redundant sites, industry certifications, or adherence to national data protection regulations[54].

4.2.4.2 Market overview

Worldwide market of cloud services has been estimated at around USD 61.15 billion in 2020, with a forecast of USD 390.33 billion in 2028.

Cloud services have stimulated demand for data centres, since some applications need very high speed to operate, and thus virtualized services need to be topologically close to the user.

The demand for cloud-based services is driven by the rising adoption of autonomous systems and machine learning, as well as the emergence of the Internet of things and remote sensing technologies. The COVID-19 pandemic has also accelerated the trend towards a more distributed work environment enabling people to collaborate and stay connected; all of which is enabled by cloud-based services. During that period, Microsoft, for instance, has increased Windows and Azure cloud credits for non-profit and critical care organizations. Cost is another driver for demand: cloud-based services are attractive because they often offer cheaper services in a single place, compared to replicating hardware, software and storage on different sites. Some hurdles for this market include confidentiality and privacy issues for which some governments and regulatory bodies deploy strict public policy norms.

On the supply side, cloud services have had an increasing role in the delivery of private and public services. This has been driven by the trend to virtualize any service that can be offered in a shared setting. This virtualization has been made possible by advances in connectivity, progressively lower costs of compute power and storage, and improvements in the distributions of cloud service points-of-presence. Market stakeholders include companies like Equinix, Alibaba Cloud, Amazon Web Services, Dell Technologies, Dropbox, Fujitsu Google, Hewlett Packard Enterprise IBM, Microsoft, Oracle, or pCloud. Most of the market is driven by hyperscale companies. Free cloud services are funded by advertising. Examples include IBM, which offers free cloud

[51] https://cloud.google.com/cdn/pricing#pricing-structure

[52] What are the top CDN benefits for today's enterprise? Kevin Tolly, https://www.techtarget.com/searchnetworking/feature/Content-delivery-network-services-The-benefits-of-CDNs

[53] Cloud-based applications (e.g. Zoom, Spotify) have been covered in the content services' section.

[54] Data for better lives, World Bank Flagship Report, 2021

services, and Google with Google Docs, which gives access to word processing, spreadsheet, and presentation software. Paid cloud services can enable storage of 2 to 10 TB. On the supply side, fee-based service plans include yearly fees or lifetime lumpsum offerings.

4.3 Interconnection

4.3.1 Service description

The Internet is sometimes called a "network of networks." The networks that make up the building blocks of the Internet are called Autonomous Systems (AS), and there are about 100,000 of such AS on the Internet today. Each AS is called "autonomous" because each is a network administered independently. When these networks interconnect, they constitute the public Internet as we know it.

To move information around the Internet there needs to be "routes" through the map of interconnected networks. The protocol that makes the interconnections and map possible is called the Border Gateway Protocol (BGP). BGP is the protocol that allows computers to map a route for packets from source to destination using the shortest and cheapest path possible.

Each AS uses BGP to build its own map for traversing the Internet. However, almost no BGP server (which is often a commercially sold router) has a complete global map of all the possible paths for packets on the Internet.

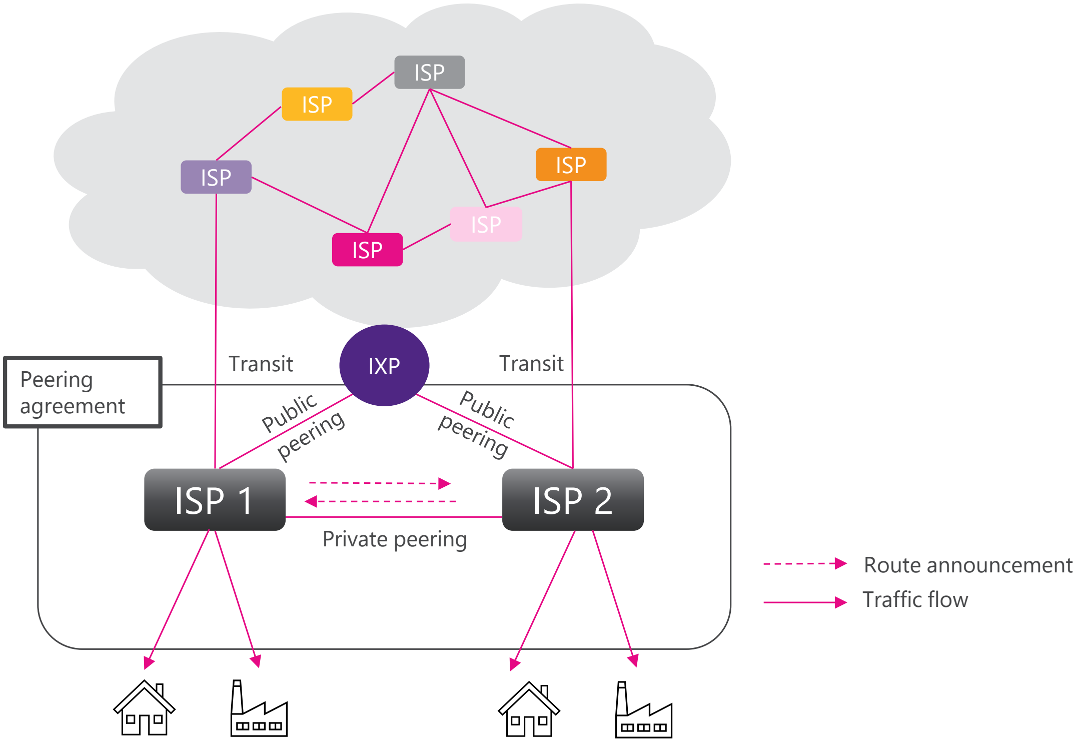
When BGP servers of different ASes talk to each other, they become neighbours. As neighbours they exchange maps of the routes they know about and want to share. Shorter paths for the packets are preferred because that results in less time for the packet to get to its intended destination.

Once the ASes have a map of available routes with their neighbours, they can exchange data. In some cases, the ASes will agree to exchange traffic between the ASes for free – an arrangement called "peering."

Often the size of the neighbours will be different. The word "transit" is used to describe connectivity to any destination on the Internet.

Internet eXchange Points (IXPs) are co-located connections of many ASes for the purpose of exchanging traffic. The IXP is usually located in a data centre which provides the infrastructure to join multiple networks together at a single location. When an AS connects to an IXP, they are creating a new route on the Internet. At the IXP, each AS establishes peering and transit relationships with the goal of establishing faster and more robust access to paths across different ASes.

Figure 4.12: Illustrative example of peering and transit agreements between ISPs



Source: Arcep, Plum

4.3.2 Market overview

Any organization responsible for part of a packet's journey from source to destination has a stake in peering and transit. This includes access providers of any size. ISPs who provide access – using any modality – need a way to route the packet on toward its destination. In addition, the access provider also provides a path to its own customers. That way, packets headed to an ISP customer's endpoint have a path for delivery.

Transit and peering are also essential for network intermediaries. The network connectivity that transit and peering provide make it possible for intermediaries to insert themselves in packet flows between source and destination. Many very large intermediaries[55] have built out networks that are as extensive as Tier 1 networks: global, extensive and with many peers.

Peering and transit are also crucial for content providers. Traditional content providers adopt a "No Peering" strategy, arguing that they focus on the content creation, that transit is inexpensive, and they just assume they can send their traffic to the experts and get Service Level Agreements to ensure a level of quality of service. Large scale, network savvy content providers will behave in a similar fashion to Tier 2 ISPs: participating in Peering Fora, openly seeking potential peers, evangelizing, and leading peering activities, etc. Some have built out global networks that are as extensive as Tier 1 networks.

[55] This includes companies such as Google, Facebook, Microsoft and Cloudflare

4.3.3 Economic dynamics and relationships

Physical interconnection is only one side of the interconnection process. There needs to be an agreement between the different actors so they can send their data to each other. Such arrangements whether they take the form of a peering, or a transit agreement are mostly business decisions.

4.3.3.1 Peering Vs transit

Transit arrangements provide access to the entire Internet, while IP Peering arrangements facilitate the direct mutual exchange of traffic between directly connected players and each party's downstream customers. The two types of interconnections can be both complementary and substitutable arrangements depending on the network configuration chosen by an operator.

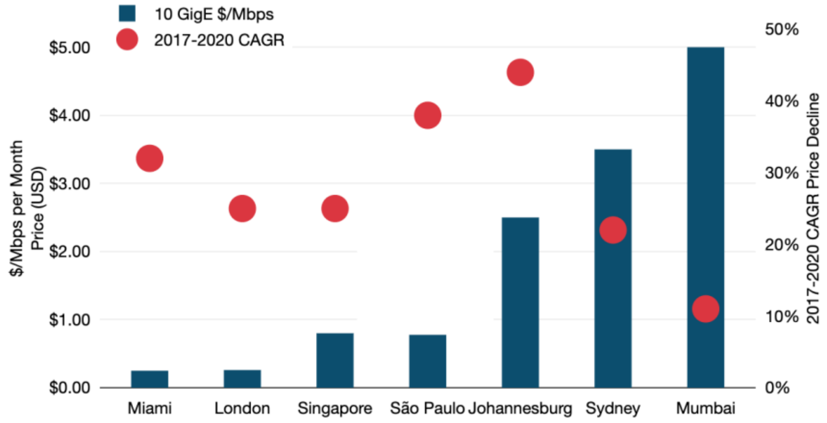
A key difference between transit and peering is that no money is exchanged between networks that agree to peer with one another. The benefit to an operator of an AS to peer is that the arrangement can reduce dependency on upstream transit providers – reducing that dependency has the effect of reducing cost for that operator.

Large networks have very little incentive to peer with potential transit customers. Even though there is strong growth in the number of ASes worldwide, most of the increase in peering is between smaller regional networks, broadband providers, content providers, hosting companies and CDNs.

Unlike peering, transit can be priced as a service. The service can also include protections against distributed denial of services attack or attacks called BGP hijacks.[56]The transit service is usually based on the traffic on the link in Mbit/s calculated at the 95th percentile, which corresponds to the maximum rate at which the client operator will be billed. The top 5 percent of the samples are usually ignored. Additionally, a traffic minimum threshold (called "commit") and a commitment period are usually set up by the transit provider. This way, the transit provider can guarantee a minimum level of revenue from the transit agreement which helps them maintain the global network footprint the transit service provides to the customer.

[56] Resource Public Key Infrastructure (RPKI) is a technology (RPKI) provides a way to protect BGP from unauthorized changes to the routing table. It uses digital certificates to ensure that only legitimate holders of Internet resources can control those resources. This helps routing protocols (like BGP) prevent route hijacking and other attacks. Also, see the description in section 4.3.4.2.

Figure 4.13: Weighted Median 10 GigE IP Transit Prices & Three Year CAGR Decline in Major Global Cities[57]



Notes: Each column represents the weighted median monthly price per Mbps in the listed city. The line represents the percentage decline of the weighted median price calculated as a three year compound annual growth rate. Prices are in USD and exclude local access and installation fees. 10 Gigabit Ethernet (10 GigE) = 10,000 Mbps.

Source: TeleGeography © 2020 PriMetrica, Inc.

Transit prices are not often disclosed as most agreements are under NDA clauses. However, a global decline in transit prices has been observed worldwide despite the geographical disparities (see Figure 4.17). Interestingly, the APAC region accounts for almost half the transit market in value.[58]

Transit providers have been historically grouped into tiers:

- Tier 1 ISPs have global reach: they peer with each other forming a global backbone network on which Tier 2 and Tier 3 ISPs connect. While the Tier 1 providers peer with each other at zero cost, they are likely to charge Tier 2 and Tier 3 providers to transit their networks. While there is no formal definition, traditionally "Tier 1" providers have been considered those who do not themselves buy transit, but can reach every network on the Internet via peering

- Tier 2 ISPs have very large networks and wide global presence (for instance, on one or two continents). Tier 2 providers buy transit from Tier 1 providers and usually peer with other Tier 2 providers as a way to expand their global reach.

- Tier 3 ISPs are usually local ISPs with local or regional reach. Their peer with other smaller ISPs and content providers and try to limit their expenses for buying transit by connecting at Internet eXchange Points.

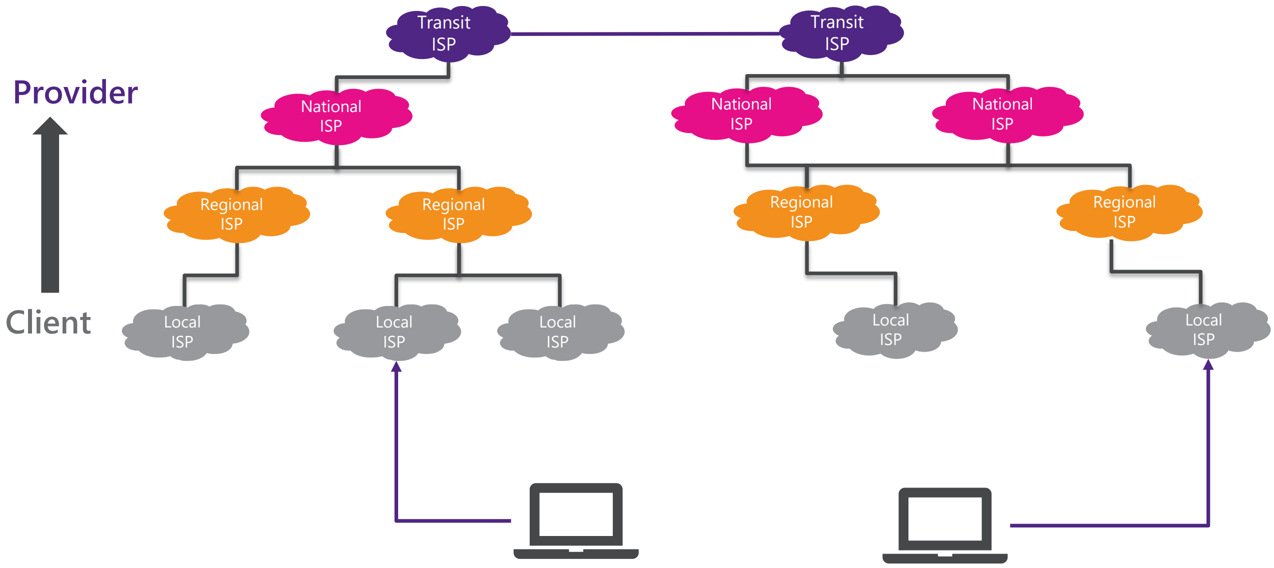
Peering enables the two networks to exchange data and benefit equally. The peering arrangement also has the ASes advertise only their internal customer routes. Although this is a zero-cost arrangement, there is usually costs for both parties associated with co-location, the routes to get to the co-located facility, and the infrastructure connections (for instance, at the IXP). Strategies for peering (and interconnection in general) vary from one operator to another. Those may be explained in a reference document, which is public most of the time and known as the "peering policy", although there is rarely any requirement to stick to this policy in the network's dealings with others. This document generally provides information on the traffic asymmetry ratio, the

[57] https://blog.telegeography.com/global-ip-transit-prices-decline-pandemic-covid19
[58] Transit provider interview

level of exchanged traffic, the geographical distribution of interconnection points, etc. Cloudflare for example has an "open peering" policy and participates at nearly 150 Internet exchanges[59].

In practice, peering agreements are often not covered by a written contract and are established by informal agreements between the two parties. According to PCH, in 2016 about 99.9 percent of the peering agreements were done informally around a handshake.[60] In some cases, a peering agreement can be implemented by ISPs to establish rules and responsibilities for interconnection, and the disclaiming of any liabilities for failure to perform by either side. They may also specify the minimum traffic and desired traffic ratio.

Figure 4.14: Relationships between Tiers of ISPs



Source: Plum

4.3.3.2 Free vs paid Peering

Peering is a form of interconnection that allows two ISPs to directly exchange traffic being routed between their own customers. In other words, Internet peering is the business relationship whereby companies reciprocally provide access to each other's customers[61]. Peering agreements are usually free because they are considered to be mutually beneficial relationships between equals (hence the term peering). Even if traffic flows are not exactly balanced, it is less expensive and scalable to establish a free deal than to meter and charge.

As the number of ISPs became larger, business-wise it was no longer beneficial for some large ISPs to connect with smaller entities without compensation. This resulted in ISPs turning to a more restrictive peering model, where they may sometimes demand payment for peering. In some historical cases, paid peering was the result of disputes on congested peering links[62].

A Paid Peering settlement could take various forms of payment: either fixed amount payments or a variable charge per unit of traffic (or a combination of both). The type of payment could involve asymmetric cost-sharing regarding the technological fixed costs of installing traffic exchange points between Peering partners. Some

[59] https://blog.cloudflare.com/bandwidth-costs-around-the-world/

[60] Packet clearing House, Survey of Internet Carrier Interconnection Agreements (2016): https://www.pch.net/resources/Papers/peering-survey/PCH-Peering-Survey-2016/PCH-Peering-Survey-2016.pdf

[61] https://drpeering.net/white-papers/Internet-Service-Providers-And-Peering.html

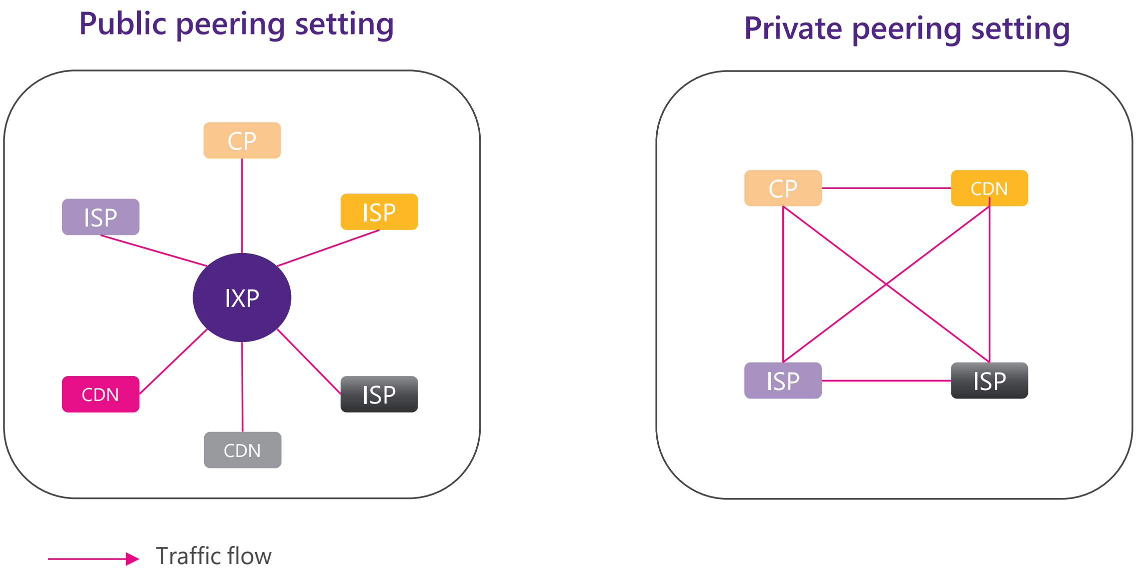
[62] Draft report on IP interconnection. Berec. June 2017. Available at: https://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/7092-draft-berec-report-on-ip-interconnection_0.pdf

large ISPs prefer to have paid peering agreements on a bilateral basis rather than joining multilateral peering at IXPs. This kind of strategy could be seen[63] as a rent seeking strategy, where dominant ISPs try to extract rents from third parties using access customers as leverage in negotiations and paid peering agreements rather than joining multilateral peering at IXPs.

4.3.3.3 Public vs private Peering

Private peering, also called bilateral peering, is generally used when there is sufficient interconnection capacity between the two ISPs involved to make a dedicated interconnection economically viable. Most colocation providers, and sometimes Internet Exchange Points offer or facilitate the interconnect of two parties using some form of dedicated point to point interconnect known as cross connects or circuits, in addition to offering a Public Peering fabric[64]. Public peering on the other hand, has emerged to make direct interconnection for smaller volumes of traffic economically viable. In particular, we assume that the cost of transport, colocation, power, etc. is identical. Only the equipment and peering services costs are considered, along with the operational issues associated with each peering model. We further assume that Private Peering involves interconnecting peers using Ethernet over dedicated cross-connects. The Public Peering fabric is provided by aggregating these same peering sessions across Ethernet ports on an IXP switch platform.

Figure 4.15: Public peering Vs. Private peering settings



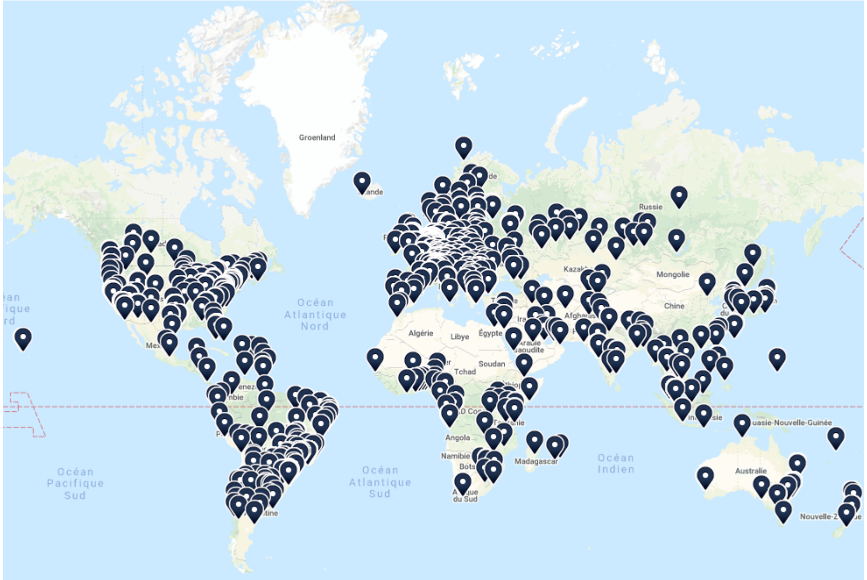
Source: Plum

An IXP can host several ISPs and other players who pay a fee to the organisation. The charges can vary for each tenant and can be decorrelated from volume of traffic. There are hundreds of IXPs around the globe[65] (see

[63] Woodcock/Frigino [(2016), p.12/13]
[64] https://drpeering.net/white-papers/Internet-Transit-Pricing-Historical-And-Projected.php
[65] A public IXP database is available at: https://ixpdb.euro-ix.net/en/

Figure 4.16 below). Equinix is the largest IXP operator with over 5 billion USD in revenue and facilities across all regions including the APAC region (Singapore, Hong Kong, Seoul and Osaka [66]).

Figure 4.16: Internet Exchange Points (IXPs) across the globe



Source: Telegeography[67]

4.3.4 Challenges to peering and transit

4.3.4.1 Non-technical challenges

Challenges to peering and transit are driven by growth in the number of networks, growth in the traffic seen on those networks and growth in the distribution of applications used on the network. In the pandemic, many people have been forced to rely on the Internet as they stay home – for work, education, social interactivity and entertainment. Clearly, the pandemic has been a major change and challenge for peering and transit, but the surprise might be that the Internet, its backbone, and the enterprises that move packets between source and destination have coped well with the new situation.

An early study of the impact of the pandemic on the Internet showed that:

- Looking at demand, the fall 2020 lockdown created a traffic surge of about 15-20 percent for IXPs and ISPs. When the first reopening took place in the summer of 2020 (before Omicron), some IXPs saw that traffic increase remain in place – others saw a decrease of 15 percent. In either case, the annual traffic increase on the Internet was higher in 2020 than in typical, previous years.

- The traffic increases from the early study mostly appeared in non-traditional peak hours. Daily traffic patterns have moved to weekend-like patterns in the pandemic, especially during the early, Delta-related lockdown.

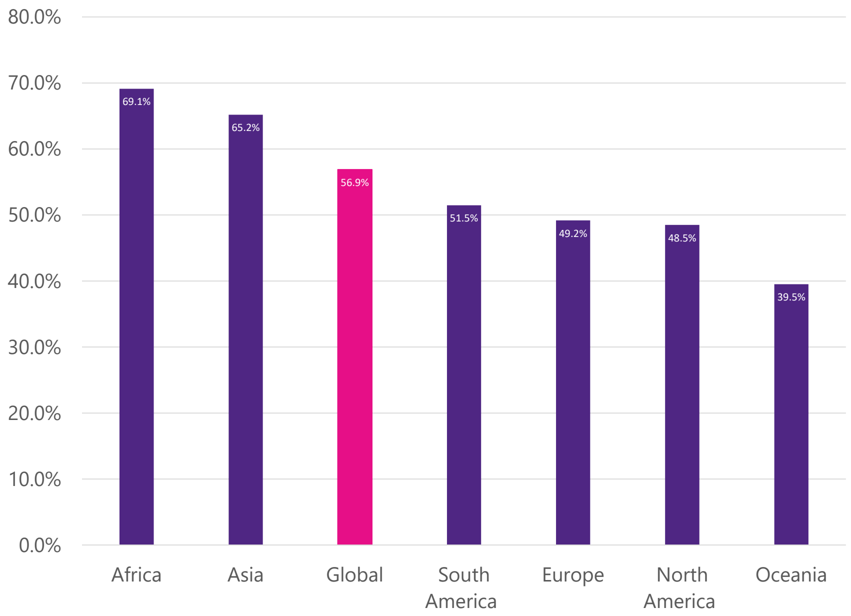
[66] https://ix.equinix.com/home/
[67] Telegeography Internet Exchange Map. Available at: https://www.Internetexchangemap.com/#/

- Traffic related to remote working applications, such as VPN connectivity applications and video-conferencing applications, increased by more than 200 percent. VPN traffic has remained at elevated levels even after the fall 2020 wave of Covid.

The three applications that showed the most growth in this early study were web conferencing, video-on-demand, and network-based gaming. In another study, Akamai reported a growth in traffic increase of 30 percent and expected that traffic to remain in place even after the pandemic has evolved to become endemic.

Much of the pandemic traffic increase is from mobile Internet devices. In 2022 Statista published a study of mobile Internet traffic as a percentage of total web traffic:

Figure 4.17: Mobile traffic share as a percent of all Internet traffic



Source: Statista

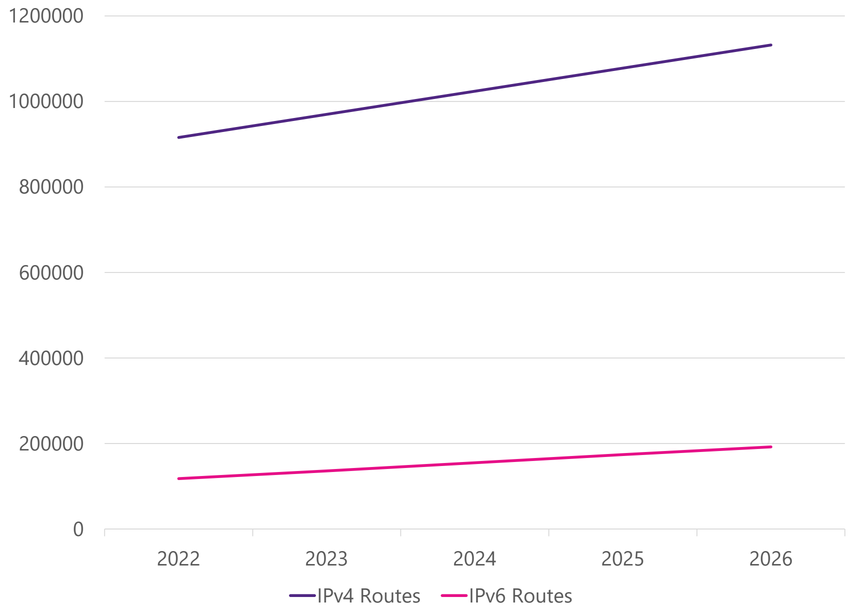
4.3.4.2 Technical ones: routing table growth, streaming video, conferencing, BGP security and threats

The sheer number of devices connected to the Internet puts enormous pressure on peering and transit. Since there are more than 20 billion connected devices worldwide, peering connections play an essential role in providing the reliability, performance, and resilience that end-users demand. Even before the pandemic, the nature of the Internet's traffic was unpredictable. The increase in demand for video and mobile services, the emergence of large-scale network attacks, and the emergence of video and voice conferencing as a leading application has made many enterprises reconsider their network interconnection strategy.

For operators of backbones and ISPs, the number of networks has implications for the size and performance of routers used to forward packets onward to their destinations. The database of forwarding information is called the routing table size. Router vendors routinely upgrade available equipment to make sure that their routers are capable of scaling to ever-increasing limits. The scale limits of router memory and software data structures are usually aligned to some well-known boundary numbers like 128k, 512k, 1024k, 2048k, and so on.

For the routers in the backbone that are expected to handle the global Internet's full routing table, the network operator needs to choose and deploy a router that has the right capabilities (such as CPU or memory capacity). Those choices reflect the need to be able to manage both the current routing table and its expected growth.

Figure 4.18: Predicted Growth in Routing table size



Key milestones in routing table growth are a particular challenge for large Internet operators, significant CDN providers and other intermediaries that provide services on the end-to-end path for a global user base (for instance, video conferencing services). However, the growth of the network, as measured by routing table size, is not the only challenge.

According to Cisco, Internet traffic is expected to grow 26 percent CAGR through 2022, and 82 percent of the traffic is expected to be video. Another significant change is the growth of cloud-based services. Today, more than 95 percent of data centre traffic is cloud traffic. Annual global cloud IP traffic has reached 20 ZB per year (a little more than 1.6 ZB per month). Cloud services used to be imagined as those that allowed you to "store things" in the cloud. Instead, today, cloud and virtualized services are mostly related to delivering services closer to end-users. 94 percent of workloads and compute instances will be processed by cloud data centres with only 6 percent processed by traditional data centres.

Continued growth in traffic demand will require the evolution of the peering networks design. It needs to scale for a larger number of connected devices with traffic sources and destinations all over the Internet[68]. One approach to meeting this requirement is localized peering strategies that place peering or content provider cache nodes closer to consumers of the traffic. This approach attempts to limit capacity on long-haul backbone networks that carry traffic from IXPs to end-users. It is also an essential ingredient in improving the performance for end-users by reducing latency in content delivery flows.

While evolving transit and peering network design is critical, the Border Gateway Protocol (BGP) is the tool used to exchange routing information throughout the Internet. BGP is the tool that routers use to build their view of the Internet and the underlying routing table. Like other elderly protocols on the Internet (for instance, electronic mail), BGP does not have security built-into the protocol. Instead, BGP is largely built on trust

[68] Pricing trends for communications services in the UK, OFCOM, July 2021, https://www.ofcom.org.uk/__data/assets/pdf_file/0013/222331/Pricing-trends-for-communications-services-in-the-UK.pdf

relationships between operators of networks. In the event that malicious actors were to try to affect how packets were routed on the Internet, BGP has no built-in defence to those attacks.

There are two major security issues with BGP:

- Individual sessions can be hijacked; and,
- Incorrect information can be placed into the BGP routing tables.

Session hijacking is when an attacker places himself in between the source and destination and either modifies the packets in transit or simply eavesdrops on the flow between source and destination.

Putting incorrect information into the routing tables can affect a far larger community than hijacking individual sessions. Ensuring authenticity is a way that ISPs, transit and peering operators can ensure that incorrect information doesn't reach the routing table. An addition to BGP, called BGPsec, allows for security to be added to the Internet's routing infrastructure.

BGPsec uses a Public Key Infrastructure (PKI) to authenticate ownership of IP Address blocks, ownership of AS numbers, an AS's identity and a BGP router's identity and authorization to represent an AS. BGPsec's Transitive Path Attribute is used to carry digital signatures authenticating the router information in a BGP update message. In addition, BGPsec uses IPsec for data and partial sequence integrity, which allows the BGP routers to authenticate each other before they exchange BGP control traffic. The emergence of BGPsec does not address all routing security issues, but it does provide an excellent approach to secure inter-domain routing for ISPs, peering and transit providers.

4.4 Content

4.4.1 Service description

The content provision environment involves a variety of services and players, but essentially online content refers to everything an Internet user can look for online: This could be cat videos on YouTube, ideas on Pinterest, news articles on the Washington Post or John Lennon's biography on Wikipedia.
Content provision services vary by type, size, reach and business model, but they all share one common feature: They all seek to capture and keep the consumer's attention.

For simplification purposes, we propose a classification based on the consumer's intention when navigating online (Figure 4.19). We assume that a consumer can either be looking for entertainment, for information, for a service or for socialising.

Content from an enterprise end-user perspective is not discusses here.

Figure 4.19: Different categories of online content and applications

Entertainment-based content	Information-based content	Socialising-based content	Service-oriented content
• Video streaming (Netflix, Disney+) • Online gaming • Musique streaming (Spotify, Pandora)	• Websites (Vodafone's website) • Online newspapers • Knowledge sharing platforms (Wikipedia) • E-learning platforms (Coursera, Udemy)	• Social medias (FB, Instagram, LinkedIn) • User-generated content • Dating platforms (Tinder)	• E-commerce platforms (Amazon, Alibaba) • Apartment rental (Airbnb)

Source: Plum

We should note that the early Internet content was primarily static. A device or application requested content from a server, the server prepared and returned a response, and the device or application presented the results. While some of this static content remains on the Internet, much of the content landscape has changed.

One major change is the rise of mobile applications, where an end-user takes advantage of a mobile device to gain access to services and information. In 2010, there were only 210,000 apps in the Apple App Store. Today the number is in excess of 4.5 million. The Internet acts as the connectivity foundation for the vast majority of those apps, but the tools and protocols in use are very different from the ones used by electronic mail or other, older services.

If mobility has changed the way the Internet work, so have hyper-scale platforms. Platforms such as Facebook and Twitter also use the Internet as the fundamental connectivity tool, but the content of these services is dynamically generated in real-time and in a state of constant revision. The connection between and end device and Facebook's CDN servers is constantly in a state of dynamic revision.

4.4.2 Market overview

4.4.2.1 A multi-sided market

The market for online content provision can be seen as a multisided market involving four categories of stakeholders.[69] The focus of this section is on content providers (CPs) and the economic aspects discussed below are based on the CPs perspective only.

The four categories of stakeholders are as follows:

- **Content providers**: companies that distribute content to end-users (Online newspapers, media streaming platforms, social media platforms, etc.).

- **Content creators**: Individuals or companies who create the content that is distributed online by the CPs (Youtubers, Journalists, bloggers, Wikipedia contributors, movie makers, Songwriters etc.). Content providers can also create their own content.

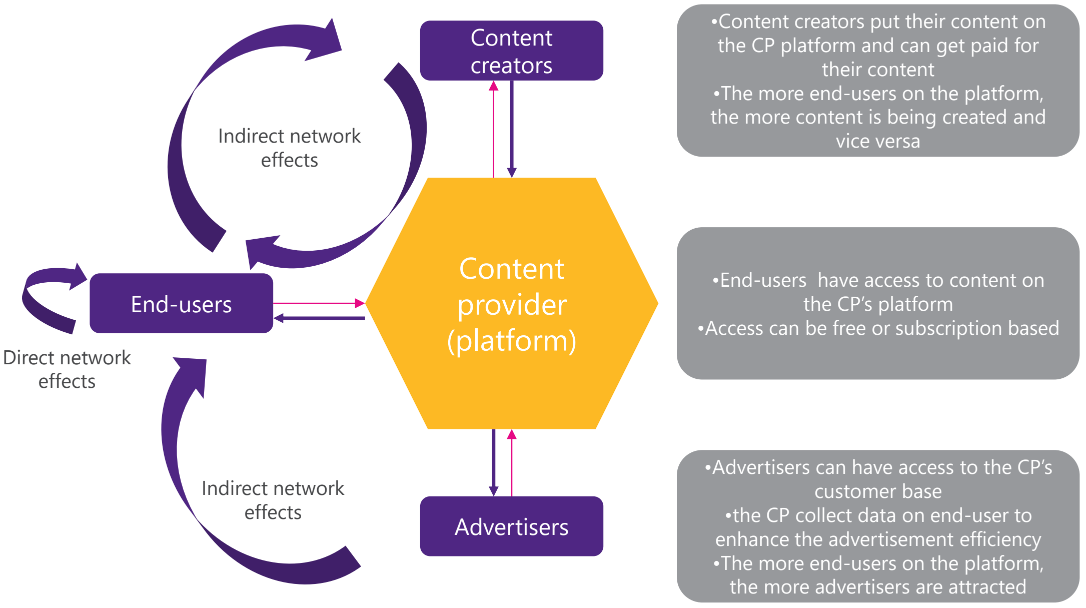
- **Advertisers**: Companies that display ads on the CP's platform.

[69] https://pubsonline.informs.org/doi/abs/10.1287/mksc.2020.1248

- **End-users**: Individual customers or enterprise customers that access the content. Note that end-users can also be content creators in some cases as on Instagram or YouTube. This is generally referred to as User-Generated Content[70].

An online Content provider acts as a market pivot by operating an online platform, hence facilitating interactions and transactions between the interdependent stakeholders or user-groups that represent the different sides of the market. The presence of a user-group usually increases the value for other groups and attract more users: This is called the network effect phenomenon. It can be direct (interaction between embers of the same user-group) or indirect (interactions between members of different user-group) as shown in Figure 4.20.

Figure 4.20: Content provision framework



•Content creators put their content on the CP platform and can get paid for their content
•The more end-users on the platform, the more content is being created and vice versa

•End-users have access to content on the CP's platform
•Access can be free or subscription based

•Advertisers can have access to the CP's customer base
•the CP collect data on end-user to enhance the advertisement efficiency
•The more end-users on the platform, the more advertisers are attracted

Source: Parmentier, Gandia (2017)[71], Plum

4.4.2.2 Demand for content

Technological progress that has led to the mass adoption of portable devices such as laptops, tablets and smartphones has also facilitated the use of online content. The demand for content is growing rapidly all over the world as it can be seen by the growing number of subscribers to services such as Netflix, HBO, Disney+, YouTube Premium, Spotify etc..).

Research from GWI[72] indicates that the "average' Internet user spends almost 7 hours per day online across all devices, which suggest that Internet users are likely to spend 12.5 trillion hours online in 2022. Social media accounts for the largest part of the time spent online with an average of 2 hours and 27 minutes per day, and

[70] https://stackla.com/resources/blog/what-is-user-generated-content/
[71] Guy Parmentier, Romain Gandia, (2017) "Redesigning the business model: from one-sided to multi-sided", Journal of Business Strategy, Vol. 38 Issue: 2, pp.52-61, doi: 10.1108/JBS-09-2016-0097. Available at: https://www.emerald.com/insight/content/doi/10.1108/JBS-09-2016-0097/full/html
[72]GWI. Available at : https://datareportal.com/reports/digital-2022-global-overview-report

the top three platforms in which time is spent the most are YouTube (23.7 hours per month), Facebook (19.6 hours/month), and WhatsApp (18.6 hours per month)[73].

4.4.3 Economic dynamics and relationships

4.4.3.1 Business models

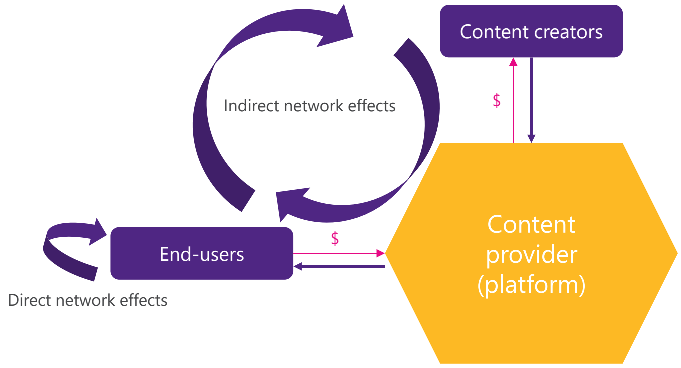
Business models vary greatly from one content provider to another, but they mainly depend on how they allocate the space between content and advertising. We identified three different business models that we discuss below.

a Subscription-only business model

CPs that operate on a subscription-only business model such as Netflix and Disney+ get paid by end-customers through a flat subscription fee. They usually require the customer to sign-up for monthly, quarterly, or annual automatic payment plans and can generate recurrent revenue from an engaged customer base. These CPs may face the potential for higher customer churn or loss than free services.

In some cases, CPs can offer access to exclusive content for paying members, while non-paying members are only given limited access: This is referred to as a "Freemium model".

Figure 4.21: Illustration of a subscription-only business model



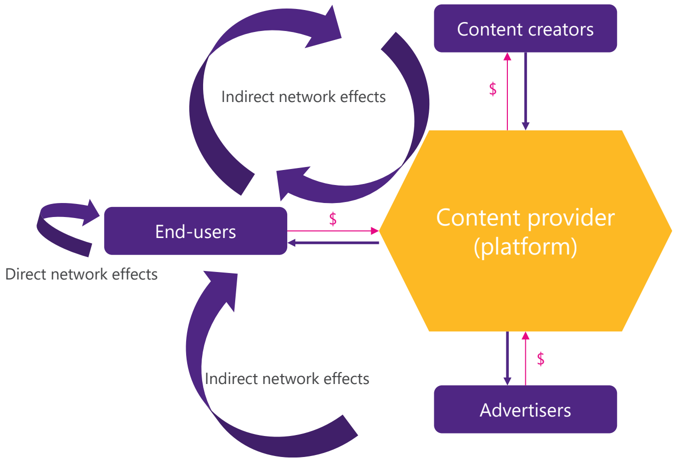
b Subscription-based and advertising-funded model

Other CPs, such as Spotify, get paid by both consumers and advertisers. They may choose to use an advertising network or sell ads privately through their own negotiation.

Non-paying consumers have access to the proposed content but are targeted with adverts, while paying customers can usually benefit from an ad-free service.

[73] Digital 2022 Global Overview Report. Datareportal. 2022. Available at: https://datareportal.com/reports/digital-2022-global-overview-report

Figure 4.22: Illustration of a subscription-based and advertising-funded model



c Advertising-funded only model

Other content providers attract consumers by offering their services for free such as YouTube or Facebook. Although there is no monetary payment involved in this case, there is still an exchange: In exchange for the service (watching videos, communicating with friends etc..), consumers provide their attention and personal data. The data collected enables the content providers to attract advertisers who are willing to pay for reaching their customers based on their preferences and their online activities. This model works best when the volume of users is very large or very specialised.[74] Estimations of the potential audience marketers can reach with ads on platforms is shown in Figure 4.23.

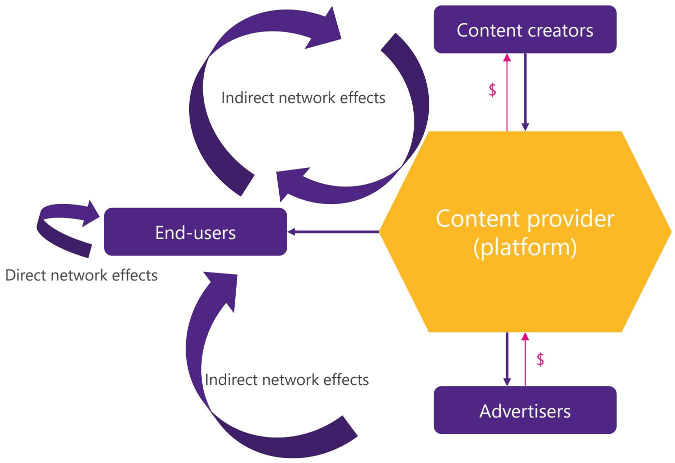
Figure 4.23: The potential audience marketers can reach with ads on platforms (Jan 2022)[75]

Content platform	Potential audience
YouTube	2.56 billion
Instagram	1.48 billion
TikTok	884.9 million
LinkedIn	808.4 million

[74] The Economic and Social Role of Internet Intermediaries. OECD 2010. Available at: https://www.oecd.org/sti/ieconomy/44949023.pdf

[75] Digital 2022 Global Overview Report. Datareportal. 2022. Available at: https://datareportal.com/reports/digital-2022-global-overview-report

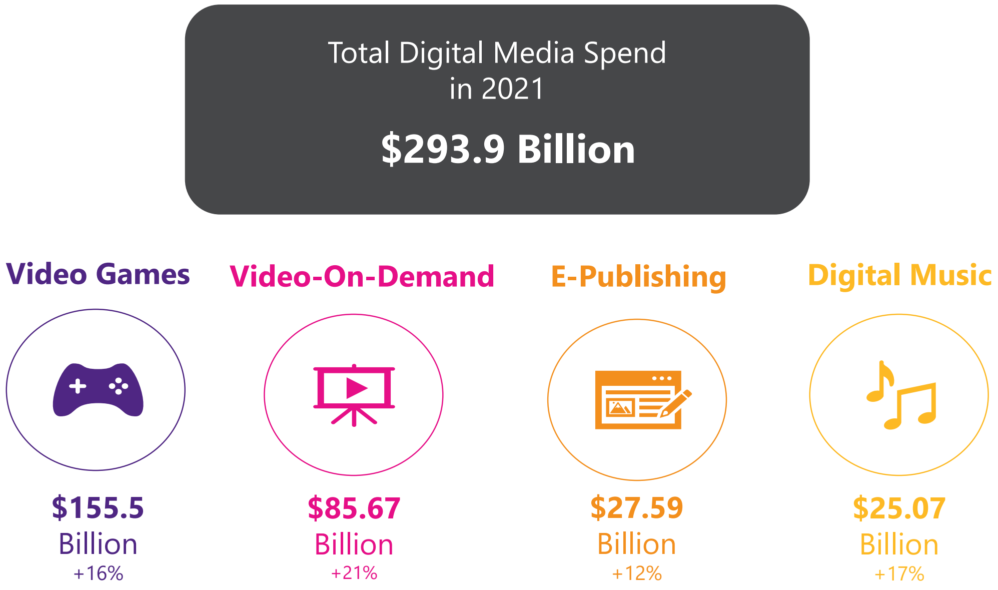
Figure 4.24: Illustration of an advertising-funded only model



4.4.3.2 Revenues

In 2021, Internet users spent an estimated $293.9 billion on digital media, including video games, VoD, E-Publishing and online music. Video games represent 52 percent of the total spend with a year-on year increase of 16 percent as shown in Figure 4.25.

Figure 4.25: Annual spend on digital media downloads and subscriptions



Source: Statista

On the advertising side, worldwide spending stood at an estimated 378 billion U.S dollars in 2020, and this figure is forecasted to constantly increase in the coming years to reach a total of 646.8 billion U.S dollars by 2024.[76]Although the advertising industry can use any form of media to meet its needs, including mediums like prints, television, radio, cinema and outdoor, the digital advertising is heavily invested as it accounted for 51 percent of total media ad spend in 2020.

[76] Statista, May 2021. Available at: https://www.statista.com/statistics/237974/online-advertising-spending-worldwide/#:~:text=It%20was%20calculated%20that%20the,of%20the%20covid%2D19%20pandemic.

Appendix A VPN services

A.1 Service description

Virtual Private Network (VPN) services are for both end-users and organisations. They provide a secure and private network connecting one or more locations, local networks, or intranets together. These services also provide proxy servers to access restricted websites/content (for instance, some online content may not be accessible from all regions in the world for intellectual property rights reasons) and to keep their Internet activity private.

Different forms of VPN services:

- Hosted/cloud VPN: the client connects through a web-based cloud VPN connection.
- Public VPN: VPN hosted and accessed using public networks or the Internet.

VPNs are legal in most countries, but some Asian countries ban them (e.g. only approved VPNs can be used in China, while data related to online activity may be examined by the government)[77].

Benefits for the user is value-added: It enables to an end-user to protect their data and activity by keeping its Internet activity private. In typical Internet connections, packets are transported across the Internet in their native, unencrypted form. A VPN changes this so that only the two endpoints can "see" the content of the packets. For end-users that has particular value when connecting to unsecured public Wi-Fi hotspots and to access content that is geo restricted in its region of the world. In corporate settings, the VPN is valuable for keeping sensitive information private – the content of the traffic cannot be examined by those involved in transporting the packets from source to destination.

A.2 Market overview and economic dynamics

On the demand side, VPN users of VPNs can be organisations or end-users. Each will look at different factors when selecting a VPN host: cost per month, connection speed, number and location of servers, the number of simultaneous connections possible, the apps on offer, quality of tech support, privacy and data logging policies. One VPN account can be used on multiple devices at the same time.

For end-users, VPNs can be standalone services on a subscriber basis, or bundled services that are offered in combination with other applications such as anti-virus tools. For businesses, VPNs are sometimes built into the feature set that the router provides on a dedicated connection. In other cases, the VPN is implemented as an add-on appliance in the business's network.

VPN hosts or VPN service providers include stakeholders like NordVPN, Express VPN, Surfshark VPN, Pure VPN, Vypr VPN, or Hide.me. Some players have developed their own infrastructure (PureVPN, ProtonVPN, Hide.me[78]), which is a considerable asset to ensure an optimal privacy and security service. Pricing schemes are usually monthly subscription fees (Figure 4.7).

[77] https://www.privacysharks.com/vpn/asia/

[78] https://www.clubic.com/antivirus-securite-informatique/vpn/test-16749-pap-avis-hide-me-le-vpn-malais-est-il-a-la-hauteur-des-tenors-du-marche-.html

Figure A.1: Examples of VPN prices

VPN provider	Starting price	Number of servers	New-user offer
NordVPN [79]	$3.29/month or $39.48/ year	5400+	30 days free trial + 30-day money-back guarantee
Surfshark VPN	$2.49/ month or $29.66/year	3200+	30-day money-back guarantee
Express VPN[80]	$6.67/month	3000+	30 days free trial + 30-day money-back guarantee

[79] https://www.clubic.com/test-produit/article-846816-1-test-nordvpn-fournisseurs-vpn.html

[80] https://www.clubic.com/antivirus-securite-informatique/vpn/article-851276-1-prise-en-main-expressvpn-services-vpn-complets.html

Appendix B Other Intermediaries

B.1 Content security and moderation intermediaries

B.1.1 Service description

Content security and moderation services relate to preventing access to specific websites, deleting or flagging posts and content, and blocking users' accounts.

Content moderation services include screening, monitoring, and approving user-generated content – text, image, or video (created in a large number of languages), through an automated or a manual process, or through a combination of both. Their main objectives are to allow only constructive content and identify inappropriate submissions (spammy, vulgar, hateful, predatory). This contributes to preventing cyber bullying, abuse, hate speech, violent threats, and child exploitation, among other harms.

Automated processes catch about 90 percent of inappropriate content[81]. It enables the protection of human moderators from violent or shocking content, and the ability to keep up with the overwhelming demand in content moderation. Limitations of automated tools[82], being AI-based, are reported to include issues of accuracy and reliability, of contextual understanding, and of transparency, among others.

Challenges related to content moderation include the emotional well-being of content moderators, a quick response time and cultural differences in what content is acceptable and what content is not.

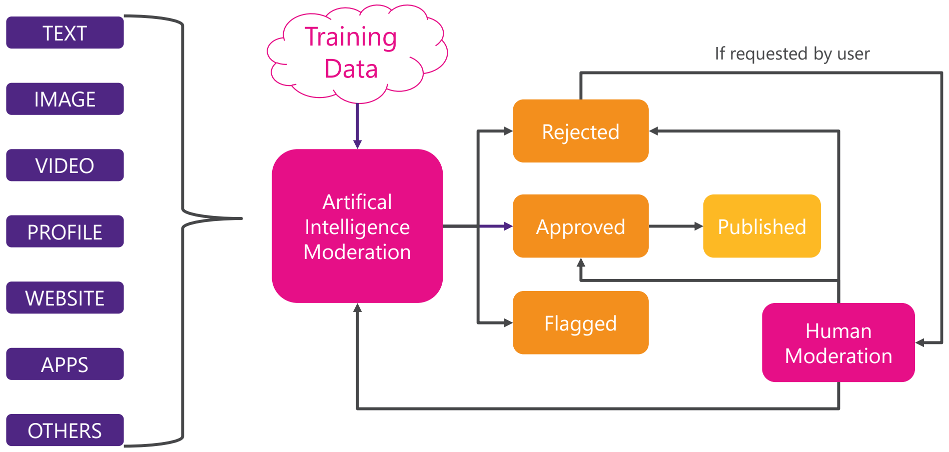
Content moderation services can be classified as follows:

- Pre-moderation: Content is checked and moderated before it is made available for the viewers. This is used by companies willing to maintain a high level of reputation and branding but does not enable real-time discussions and posting.
- Post-moderation: Content is checked after being published, and it is determined whether to maintain or delete the post. This is used by websites that have active online communities.
- Reactive moderation: This also relies on the judgment of the user community, where users have to remove or flag inappropriate content posted.
- Distributed moderation: This type of moderation is not widespread because of the potential risks it entails. Community members, through a voting process, alongside the website moderator, decide whether the content must be moderated or not.
- Automated moderation: Tools and techniques enable to filter, flag or approve content through algorithms.

[81] https://www.aitrends.com/ethics-and-social-issues/content-moderation-becoming-a-big-business-with-ai-enlisted-to-help/

[82] https://www.newamerica.org/oti/reports/everything-moderation-analysis-how-Internet-platforms-are-using-artificial-intelligence-moderate-user-generated-content/the-limitations-of-automated-tools-in-content-moderation/

Figure B.1: Automated moderation process



Other types of content-related services are linked to security issues and national public policies. They prevent access to illegal content and/or redirect the user's request towards legal content. As an example, in China where ISPs are licensed by the government, requests for search engines on global platforms are often redirected to a national (and, government-approved) search engine.

Content moderation is both a regulatory requirement in some cases and a value-added service.

Regulatory requirement

Existing legal frameworks impose content moderation on Internet market stakeholders. A few examples include NetzDG in Germany[83], the Avia law in France[84], the Online Safety Act in Australia[85] and the Network Act in South Korea[86]. In the overall public policy debate, there are existing regulatory tensions on content moderation:

- Quality of information vs. freedom of speech (Organisations may be cautious in their application of content moderation, as they fear accusations of censorship.[87])
- Liability and responsibility for policing.

Metaverse will bring some new regulatory issues related to content security and moderation[88].

Value-added service

By identifying inappropriate submissions, content moderation services enable to keep clients away from negative posts or comments and to protect them from deceptive proposals sent by spammers. Benefits are twofold:

- Provide a safe and healthy customer experience, and

[83] https://webhelp.com/news/legal-frameworks-of-content-moderation-around-the-world-part-1/
[84] https://www.google.com/url?q=https://www.universal-rights.org/blog/frances-watered-down-anti-hate-speech-law-enters-into-force/&sa=D&source=docs&ust=1656671510853321&usg=AOvVaw1pJb8Pyt48xojKOYR8mRLO
[85] https://www.herbertsmithfreehills.com/latest-thinking/policing-the-Internet-australia%E2%80%99s-developments-in-regulating-content-moderation
[86] https://elaw.klri.re.kr/kor_service/lawView.do?hseq=50484&lang=ENG
[87] https://onlinelibrary.wiley.com/doi/full/10.1002/poi3.239
[88] How online content providers moderate user-generates content to prevent harmful online communication: an analysis of policies and their implementation, S. A. Einwiller, S. Kim, Policy and Internet, May 2020, https://doi.org/10.1002/poi3.239

- Build trust with clients and users and maintain a brand's reputation.

B.1.2 Market overview and economics

It seems to be challenging to track how the market value is fragmented between:

- Content moderation companies: These include pure players (companies whose core business service is content moderation) and companies offering content moderation bundled with other services, and

- Insourced content moderation

On the supply side of the market, a few pure players have been identified (such as Besedo), but most content moderation companies are multiservice (Liveworld.com; EuropeITоutsourcing; Icuc.social; Pure Moderation; Crowdsource). Some mergers and acquisitions have taken place, such as the acquisition of Twohat by Microsoft in 2021[89]. Big tech companies also propose content moderation services (e.g. Azure Content moderation by Microsoft) and have internal teams to work on their own content moderation (e.g. Facebook)

Looking now at the demand side of the market, all content providers and online platforms are concerned by content moderation, whatever the sector they operate in (e.g. e-commerce, gaming, media). Regarding the economic incentives to moderate user-generated content, research has shown that platforms under the advertising model are more likely to be willing to moderate their content compared to platforms under subscription -- but will do it less aggressively as they are more concerned about expanding their user base[90].

Regarding pricing schemes, suppliers offer different types of packages:

- Some are fully based on the continuity of service (e.g. 24 hours a day and 7 days a week vs. 8 hours a day and 5 days a week) (Figure B.2),

- Some are a "Pay as you Go" scheme:

  - Whatever the type of content (For instance, Microsoft Azure[91] charges €0.882 every 1000 transactions up to 1 million transactions, then €0.661 every 1000 transactions between 5 and 10 million transactions, then €0.353 every 1000 transactions for more than 10 million transactions.), or

  - Depending on the type of content to moderate – image, text or video, or

  - Depending on the type of content to moderate[92] (adult filtering, violence and terrorism filtering.

Figure B.2: Content moderation prices and packages – Europe IT Outsourcing[93]

	Content Moderation 8/5	Content Moderation 16/5	Content Moderation 24/7
Brand protection from spam & abuse	√	√	√
Better B2C and B2B relations	√	√	√

[89] https://www.twohat.com/blog/announcement/

[90] Liu, Yi and Yildirim, Pinar and Zhang, Z. John, Implications of Revenue Models and Technology for Content Moderation Strategies (November 23, 2021). Available at: http://dx.doi.org/10.2139/ssrn.3969938

[91] https://azure.microsoft.com/fr-fr/pricing/details/cognitive-services/content-moderator/#pricing

[92] Example: https://www.alibabacloud.com/fr/product/content-moderation/pricing#producttabimage-1

[93] https://europeitoutsourcing.com/packages/content-moderation/#get-quote

Better SEO and online visibility	√	√	√
Types & networks			
Pre, post & reactive moderation	√	√	√
Automated moderation integration if needed	×	√	√
All social media networks	√	√	√
Web & mobile apps, blog & forum comments, chatbox, forms inquiries,	√	√	√
Activities			
Hours/day	8/5	16/5	24/7
Replies to messages, comments, question and reviews	√	√	√
Hide, ban, approve comments	√	√	√
Texts, images, video moderation	√	√	√
Reports to manager	√	√	√
Price and Packages			
Price	$1000/month	$1900/month	$3800/month

B.2 Network Security Intermediaries

B.2.3 Service description

Traditional appliance-based firewalls were developed to protect business networks. They provide packet inspection capabilities to filter network traffic based on a set of rules. The intent of the rules is to protect the network from internal and external threats and avoid malicious or unauthorized access to the network. These rules include domain and IP address access rules, web and URL filtering, advanced malware detection, logging, identity management, intrusion detection and prevention.

Because more and more companies have moved their infrastructure, apps and data to the cloud, firewall services have been transitioning into a virtualized service, often called FWaaS (Firewall as a Service). Systems are also now able to predict external threats based on its examination of the patterns of incoming traffic. FWaaS also are able to protect remote connections and often provide VPN and access control applications. This means that the FWaaS application can support a geographically dispersed network – far beyond the devices operating in physically connected offices (as was the case for traditional firewalls).

NGFW (Next Generation Firewall) combine the capabilities of traditional firewalls – packet filtering, address translation, URL blocking and VPN – with features of quality-of-service management, as well as features typically absent from firewalls (including intrusion prevention, SSL and SSH inspection, deep packet inspection (DPI), reputation-based malware detection). Next Generation Firewalls often move beyond traditional rule-based approaches to access control to AI-based traffic examination. Identifying patterns in traffic provides protection against denial-of-service attacks and other exploits that rules-based approaches might not be able to deal with effectively.

B.2.4 Market overview

The global market for Network Security Firewalls[94] is estimated to be growing at a CAGR of 17.6 percent over the period 2020-2027 (from US$3.7 billion in 2020 to US$11.5 Billion by 2027). The US market is estimated at $1 billion in 2020 and China should grow at 21.9 percent CAGR over 2020-2027 with a market size of US$2.6 Billion in 2027. Other important markets are Japan (with 13.8 percent CAGR) and Canada (with 16 percent CAGR).

The network security market is driven by the increasing dependence on IoT, as well as the expanding variety of network exploits. The demand for network security services is cross-sectoral (e.g. finance, public services, education, manufacturing.) and concerns both public and private organisations, where it has become an essential part of providing enterprise IT services.

On the supply side, there are two types of firewall appliances on the market:

- Hardware appliances (which tend to disappear as an organization grows and the appliance fails to scale along with the network traffic at the enterprise), and

- An increasing use of virtual (software) appliance firewalls, including cloud-native firewalls (IaaS Infrastructure as a Service providers) and FWaaS offerings (hosted by vendors).

[94] https://www.researchandmarkets.com/reports/5303650/network-security-firewalls-global-market?utm_source=BW&utm_medium=PressRelease&utm_code=rnckl8&utm_campaign=1561954+-+Global+Network+Security+Firewalls+Industry+(2020+to+2027)+-+Key+Market+Trends+and+Drivers&utm_exec=jamu273prd

Traditional firewall vendors include Cisco, Palo Alto Networks, Fortinet, and Zscaler, and most of them now provide NGFW (Palo Alto Networks, Fortinet FortiGate, Cisco Firepower, Juniper Networks SRX Firewall series, Forcepoint). Major cloud infrastructure vendors (AWS, Google, Microsoft) also provide firewall capabilities.

Firewalls market offerings differ according to performance, ease of installation/use, integration capabilities of third-party security products and pricing. Suppliers offer different types of packages from basic protection (e.g. "Advanced Threat Protection" package by Fortninet) to maximum protection (e.g. "360 Protection" package by Fortinet). As in other intermediaries, there is variety, and complexity in available market offerings, and pricing schemes differ depending on service bundles. Our research has not found any publicly available pricing scheme: most of offerings seem to be tailored to the client's need, so suppliers offer free personalized trials[95].

B.3 Geolocation access control services

B.3.5 Service description

Geolocation access control services enable applications and networks to identify information about an Internet user's geographical location, like the country of connection, region, city, ZIP code, latitude and longitude, as well as information about the ISP used, and even the connection speed. It is a mechanism to establish an individual's identity by detecting its presence at a specific location. Often, this will be to limit access to sensitive or restricted data and services based on the location of the end-user.

These services work through access to a number of databases, with the Regional Internet Registries (RIRs) as a primary source. These are the five, official organisations in charge of distributing IP addresses in specific regions of the world (e.g. APNIC for Asia Pacific, RIPE NCC for Europe[96]). For groups of IP addresses, the RIRs publicly record the name and location that to whom the addresses have been assigned. Using the IP address as an index, these databases can be used to establish where the IP address is being used.

Banks can prevent phishing attacks and money laundering by geolocating the user in its authentication process. E-commerce websites and online payment service companies can use geolocation services to detect online fraud, by cross matching the IP address and the billing address. Public investigative agencies can monitor online trafficking by suspected terrorist organisations or online trading with banned nations.

Another typical application of geolocation is to limit access to information to a specific geographic region. Intellectual property rights or contractual obligations may mean that certain content is only available in certain regions or countries. Using geolocation, the network server can determine whether the end-user has the right to use or see the content based on policy, contractual or regulatory rules.

Geolocation access control services are used not only for security purposes as in the examples above, but also for user customisation features of a website. Depending on its location, the website to which a user connects will dynamically present the content in the appropriate language. This is what happens when typing www.paypal.com for instance.

B.3.6 Market overview

Overall, the market demand is stimulated by the growing scope and sophistication of frauds and cyber-attacks.

[95] https://www.paloaltonetworks.fr/network-security/next-generation-firewall

[96] For more details on Regional Internet Registries, see: https://whatismyipaddress.com/rir

Asia-Pacific is the fastest growing region globally for the access control market, with China as the fastest-growing country in the region. Drivers identified for growth in Asia-Pacific are increasing concerns in businesses, the willingness of governments to enhance security due to increased terror threats, lucrative opportunities in economies like China and India, and rapid technological advancements and increased awareness about security.

The demand for these services is cross-sectoral and comes from both private companies and public entities. On the supply side, companies like Huawei Cloud[97] and Comarch offer these types of services.

[97] https://support.huaweicloud.com/intl/en-us/usermanual-waf/waf_01_0013.html

This document has been commissioned by our client and has been compiled solely for their specific requirements and based on the information they have supplied. We accept no liability whatsoever to any party other than our commissioning client; no such third party may place any reliance on the content of this document; and any use it may make of the same is entirely at its own risk.