NOKIA

Nokia Deepfield Network Intelligence Report: Networks in 2020*

Service provider traffic and consumption trends in the internet's rollercoaster year

* January-September 2020

Foreword

Foreword from Dr Craig Labovitz,

Chief Technology Officer, Nokia Deepfield

Having been personally involved in the internet's evolution for more than 25 years, and having witnessed its major architectural changes and growth, I have been very impressed by the performance and resilience of service provider networks and the internet in this year of upheavals.

The networks were made for this. Performance across all constituent parts of the internet – service provider networks, content delivery networks (CDNs), and large content and application networks – is testament to the exceptional work of engineers, network planners, and security and operations teams everywhere.

We are seeing great examples of digital cooperation between telecom service providers, cloud providers, regulators, and governments. Now, more than ever, we need strong commitment to further network investments and to grow, connect, and secure network infrastructures worldwide to ensure resilience and lessen digital divides.

Our Nokia Deepfield portfolio of software applications has allowed service providers to understand activity in their networks in these critical times, enabling them to ensure continuity of service and create value for their customers.

Foreword from Manish Gulyani,

Vice President and General Manager, Nokia Deepfield

COVID-19 has taught us that networks matter now more than ever before. They have become our lifeline, figuratively and literally. We use networks to work and collaborate, to learn, to entertain ourselves, and to communicate and stay in contact with family and friends.

As a leader in the community of network and cloud builders, Nokia has played an important role, making sure that networks delivered on all important fronts: performance, service quality, user experience, and security.

With our networks providing the underlying connectivity fabric for business and society to function, there is a greater than ever need for holistic, multidimensional insights across the network, services, applications, and end-users. One question we hear a lot is: "While my network delivered the best it could under the strain of increased demand and incredible traffic growth, can you help me get the control I need to deliver flawless service with the best possible customer experience?"

Our answer is yes. With Nokia Deepfield, service providers can obtain the necessary network visibility and actionable analytics to improve the network and service capabilities while providing customers with assured quality, enhanced security, and a reliable network environment. The data and insights we've drawn on for this report shows how.

Table of contents

Executive summary

The networks in 2020: Key findings

This report draws on data recorded by network service providers across Europe and North America between February and September 2020. Many networks experienced a year's worth of traffic growth – 30–50 percent – in just a few weeks, as COVID-19 lockdown measures were implemented.

By September, the data indicated that traffic had stabilized at 20–30 percent above pre-pandemic levels, with further growth to come. However, as of the second half of October,* partial lockdowns and other public health and safety measures are being re-instituted in many countries and regions – possibly with new effects which are yet to be recorded.

* Time when this report is finalized and sent for production.

The networks in 2020: Key statistics

First weeks of lockdown compared to the previous week:

30–50%
increase in **network traffic**

NETFLIX 50–100%
increase in **Netflix traffic**

350–700%
increase in **videoconferencing traffic**

100–150%
increase in **gaming traffic**

One month into lockdown:

40%
increase in **DDoS attacks**

100%+
increase in **peering traffic** as on-net caches reached their capacity

Six months into the pandemic:

Traffic levels stabilize at 20–30% above pre-pandemic levels

Key takeaways

#1 "[Service provider] networks were made for this"*

Despite seeing the equivalent of a year's traffic growth in just a few days, networks were able to take the strain – a testament to the foresight and engineering expertise of both communications service providers and cloud services providers.

While the networks held up during the biggest spikes in demand, data from September 2020 indicates that traffic levels remain elevated even as lockdowns are eased. The big question now for service providers is how much capacity to engineer into the networks now for future eventualities – or how to get the required headroom capacity when needed.

#2 Internet-based content delivery chains are evolving

Demand for streaming video, low-latency cloud gaming and videoconferencing, and fast access to cloud applications and services all placed unprecedented pressure on internet-based content delivery paths. Just as we saw content delivery networks (CDNs) grow in the past decade, we expect the same to happen with edge/far edge cloud in the next decade, bringing content (storage and compute) closer to end-users.

Service providers have an opportunity to develop win-win partnerships with internet applications, content and services providers, and with the content delivery networks (CDNs) that host and deliver their content. To capitalize on this opportunity, service providers must have a full visibility of the internet service delivery chain, not just of their own network.

#3 Residential broadband networks have become critical infrastructure

The COVID-19 pandemic events highlighted the role of our residential broadband connectivity as vital for society. Thanks to service providers' and cloud operators' agility and immediate actions, people in lockdown could use their network connections to work, play, socialize, get help, and provide help to others.

The challenge for service providers is to find ways to improve overall network resilience and offer tailored work/play/connect packages. They must also address dynamically – shifting consumer needs – ranging from uninterrupted access to critical communications to soaring demand for high-bandwidth, low-latency content and services. Accelerating the rollout of new technologies – such as 5G and next-gen FTTH – that will improve access and connectivity in rural, remote, and underserved areas would go a long way toward bridging the digital gap in many societies.

#4 Deep insight into network traffic is essential

This analysis of internet traffic in 2020 provides significant insights into the changing patterns of consumption and demand in service provider networks and cloud networks. While the COVID-19 era may prove in many ways to have been exceptional, the likelihood is that it has only accelerated trends in content consumption, production, and delivery that were going to happen anyway. Recent data from September 2020 supports this notion.

By understanding network traffic trends in detail and in real time, service providers can gain more in-depth insight into evolving subscriber needs and preferences. That will allow them to develop partnerships and offers that elevate their role to providers of valuable, differentiated services.

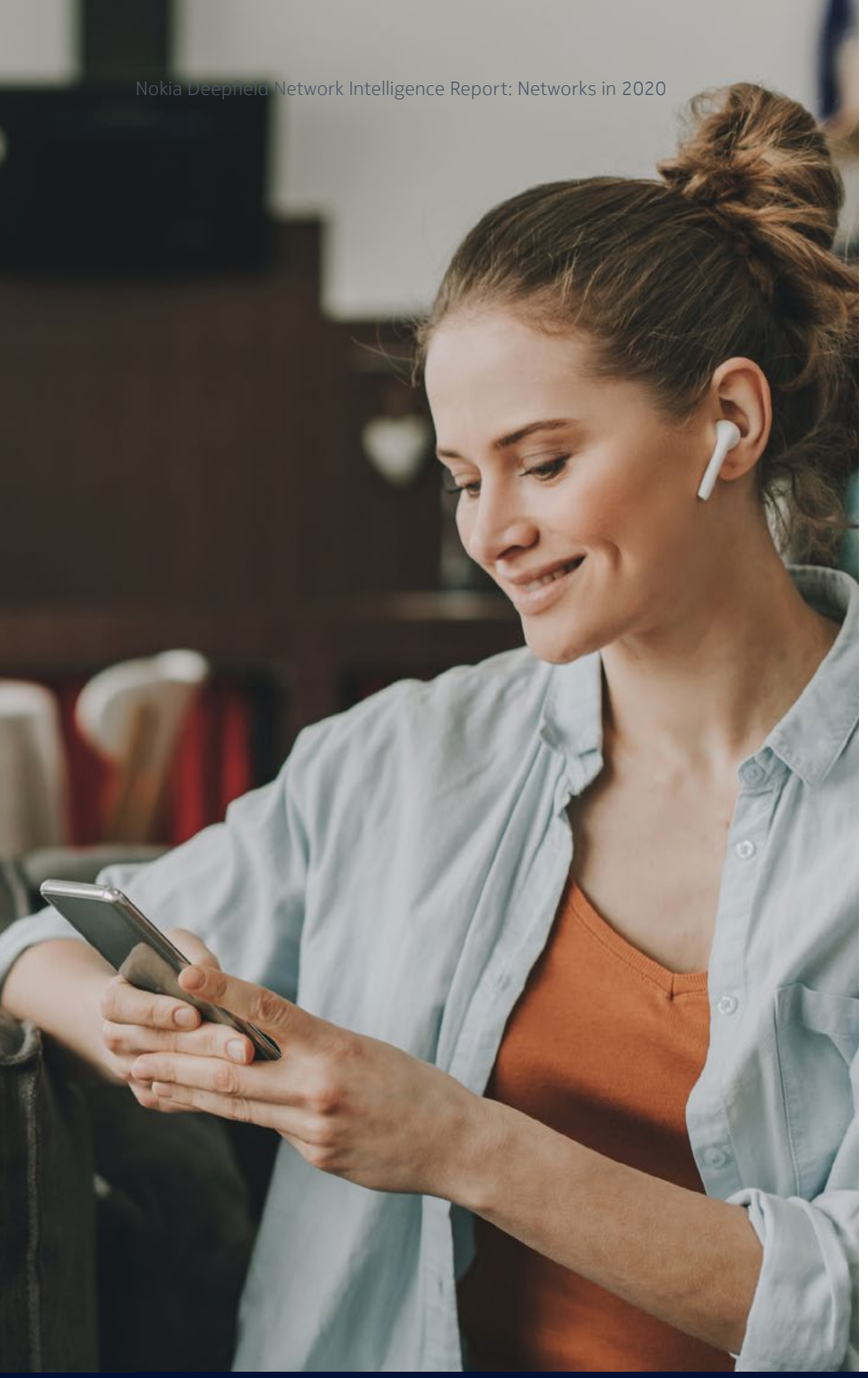
#5 Security has never been more important

In normal circumstances, distributed denial of service (DDoS) attacks can threaten a business's livelihood and reputation. In situations where broadband connectivity is an essential service, protecting network infrastructure and services becomes critical. In particular, the rise of online gaming has led to more and shorter DDoS attacks, often targeted at a single host, creating challenges for service providers in detecting and protecting against attacks.

The need for robust, 360-degree network security DDoS protection is critical. Service providers will need to find better and more cost-effective ways to detect and minimize new forms of DDoS attacks that may go undetected or unmitigated by legacy security tools and approaches.

* Dr Craig Labovitz, CTO, Nokia Deepfield, in ITU/UN webinar on broadband connectivity and digital cooperation in the time of COVID-19, 22 April 2020.

https://www.youtube.com/watch?v=ti7G1dDW7HQ&feature=youtu.be&t=2285



Introduction

Network traffic and consumption trends in 2020

2020 was a rollercoaster year for the internet. Emergency measures to combat the COVID-19 pandemic led to behavioral changes that transformed the internet's shape and how we use it, literally overnight.

Fortunately, the decade prior to the pandemic had seen massive and transformative changes in the internet – both in service providers' networks and in the architecture of cloud content delivery. As we'll show, those changes meant the networks were mostly ready for COVID-19 when it arrived.

A year's worth of traffic growth in just a few weeks

While the networks kept going – and kept us going – the sweeping changes brought about by the pandemic raise big questions for service providers. The data in this report shows that many saw a year's worth of traffic growth in just a few weeks. What does that mean for capacity planning, marketing and service planning, traffic engineering, network security, and network operations?

Traffic patterns during three key periods of 2020

To help answer those questions, this report looks at what was happening in the networks in three key periods of 2020:

- January–February: Before the pandemic took hold
- March–May: As national and regional lockdowns (or shelter-in-place orders) set in
- September: Six months into the pandemic.

We examine the immediate and longer-term changes wrought by the pandemic, both in terms of overall traffic and in four key application areas: streaming video on demand, videoconferencing, gaming, and security.

We look at the role played by CDNs, transit, peering, and access networks as the world's activities moved online. We show how key events – like presidential announcements, the launch of Disney+, and the release of Call of Duty: Warzone – played out in service providers' networks. And we highlight some of the success stories of the pandemic, including Netflix, Zoom, and Microsoft Teams.

Key insights and takeaways for service providers

In doing so, we show how COVID-19 accelerated trends that were already underway in content delivery and consumption, remote collaboration, online gaming, and security.

Finally, we explore why it's more essential than ever for service providers to understand network traffic in detail and in real time, and how they can use insights like those in this report to plan effectively for the future – whatever it may hold.

How we got to 2020

Internet megatrends 2009–2019

This report examines some of the most significant changes as they played out in service providers' networks. We look at how these changes happened, what they mean for networks' immediate and longer-term future, and what service providers can learn from them.

However, to understand the extent and impact of those changes, we must first look at the internet as it stood on the eve of the COVID-19 pandemic.

Four defining internet trends, 2009–2019

Over the last decade, networks evolved so much that the pre-pandemic internet of 2019 was virtually unrecognizable from the internet of 2009. Four megatrends define a decade of evolution:

1. The internet is getting bigger – but also smaller

The internet has grown tremendously, in terms of the number of connected devices and the volume of traffic. As traffic volumes grew, the number of large originating domains (or autonomous systems (AS) as they're called in technical circles) consolidated to the point where, in 2019, as few as five large internet domains were responsible for 50 percent of traffic in service provider networks. What's more, over 90 percent of content was originating from fewer than 150 sources.

2. The rise of hyperscale giants…

Hyperscale (or webscale) giants such as Alibaba, Amazon, Apple, Facebook, Google, Microsoft, Netflix, and Tencent expanded their networks and businesses globally, using the internet to create a global super-network of distributed cloud data centers. New 'edge cloud' network architectures have been introduced, bringing content, applications, and services closer to users and subscribers.

3. …whose content needs to be delivered everywhere

The need to bring content closer to subscribers saw the growth of a new type of network player. CDNs emerged as mechanisms for delivering streaming video, online games, and other web content to users globally and across service provider networks. Evolving from a few centralized servers in 2009 to thousands of edge- and metro-level CDNs in 2019, the rise of CDNs meant the internet on the eve of COVID-19 was essentially a vast content delivery mechanism.

4. An expanded and shifting threat surface

As the internet grew, so did the potential for malicious activity. Over the decade, DDoS attacks evolved from large-scale attacks on select hosts to sophisticated and shape-shifting attacks on a much larger number of hosts and domains, significantly affecting the availability and quality of network services. With terabit-level attacks becoming more frequent, the potential for massive network outages and loss of connectivity dramatically increased.

Four defining internet trends, 2009–2019

Let's look at these trends in more detail, illuminated with insights gathered by Nokia, using our Deepfield portfolio of network intelligence and analytics tools

1. The internet is getting bigger – but also smaller

One of the biggest trends of the past decade was the way the internet – the global network of networks – simultaneously grew and shrank.

In terms of traffic volume, the internet grew massively from 2009 to 2019. Rates varied between different service providers' networks, but typical growth rates were in the region of 40–50 percent CAGR, with daily traffic typically measuring in petabytes.

Part of the reason was the exponential growth in the number of devices connected to the internet. Many of them have public IP addresses (both IPv4 and IPv6) of their own, but a much larger number still reside as connected devices behind home routers using Network Address Translation (NAT). The rapidly depleting IPv4 address space was augmented with the IPv6 address space to allow billions of new devices and systems to be added, including myriad Internet of Things (IoT) devices.

In 2009, people had only a few connected devices per household – mainly laptops, mobile phones, and tablets. By 2019, reports indicated that in US and UK residential networks, this number was above ten. Other reports reveal that the number of connected devices per person will surpass ten in 2021. Some digitally savvy consumers admit to having over 30 connected devices in their homes, including laptops, smartphones, games consoles, home automation sensors and controllers, smart speakers, and internet-connected TV sets and streaming devices.[1] All these devices have access to more bandwidth than ever before.

At the same time, we can say that the internet got smaller, in the sense that the number of traffic-originating domains reduced significantly. In 2009, half of the internet traffic on most service providers' networks came from 150 originating domains. By 2019, that number was down to just five. In fact, by 2019, 90 percent of internet traffic in service provider networks was originating from fewer than 150 sources.

While these few domains vary from network to network and from region to region, they are typically hyperscale giants – the largest providers of streaming video, online games, and cloud content.

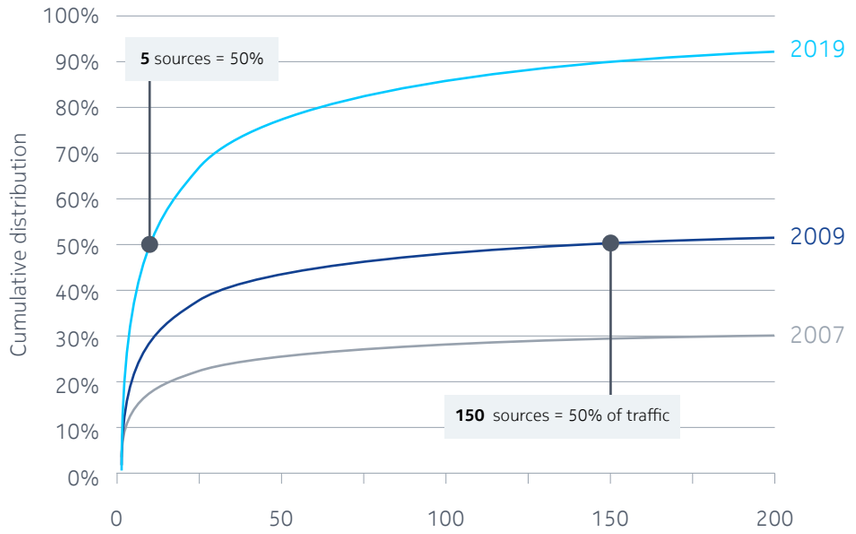
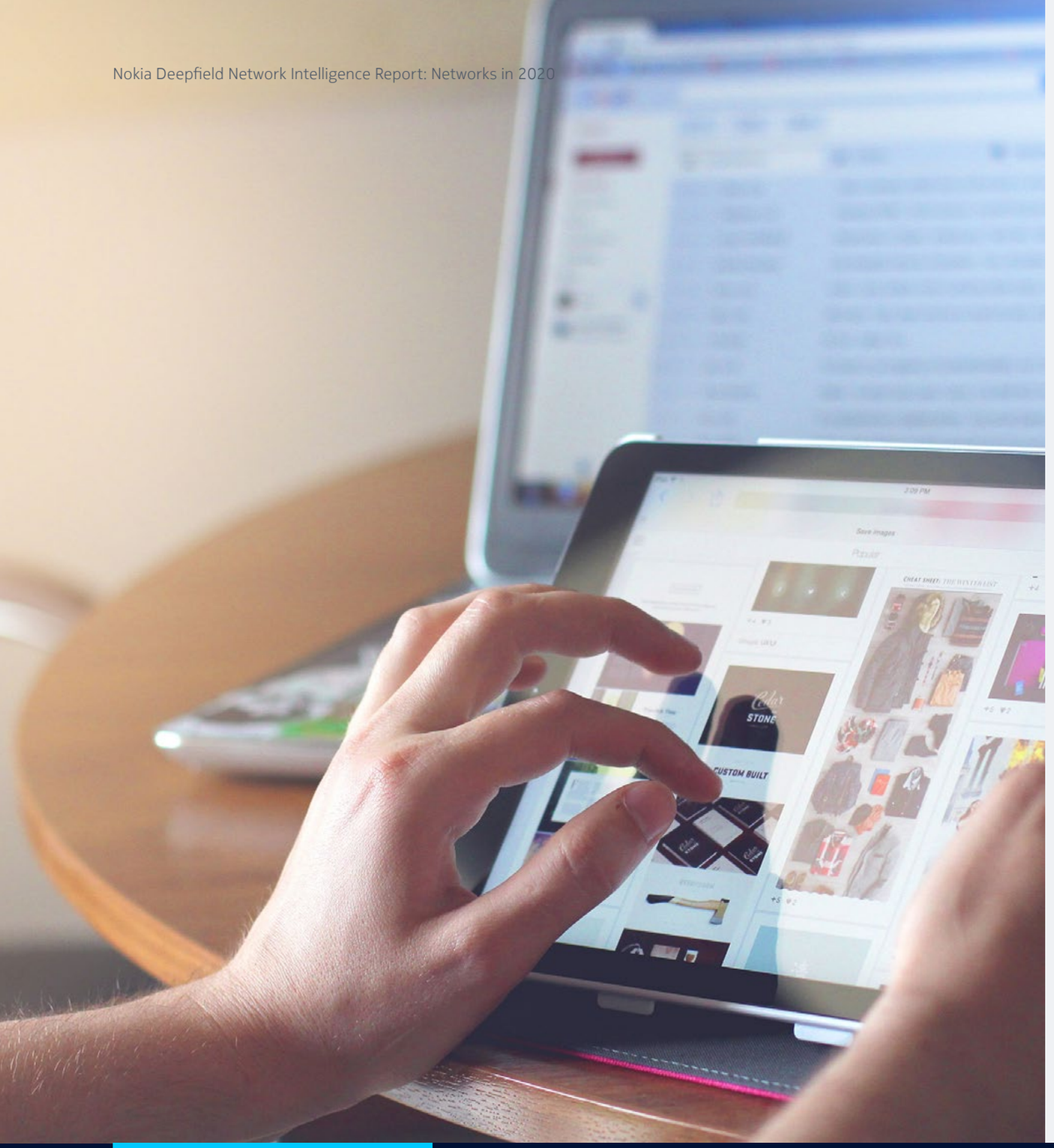


Figure 1. Consolidation of the internet from 2007 to 2019. By 2019, 50 percent of all internet traffic was coming from a small number of internet ASNs

Source: Nokia Deepfield

1. Big 5G Event Keynote, May 2019



2. The rise of hyperscale giants...

With the help of advanced network technologies like 4G/LTE and cloud computing, hyperscale giants like Amazon, Apple, Facebook, Google, Microsoft, and Netflix found ways for their content to reach end-users and subscribers faster, broader, and closer to home.

As more content came from the internet, this created an opportunity for service providers. Rather than delivering content without knowing much about where it was coming from or how it was delivered to their customers, some seized the opportunity to move beyond basic connectivity and focus on quality of service and customer experience as a way to win and retain subscribers.

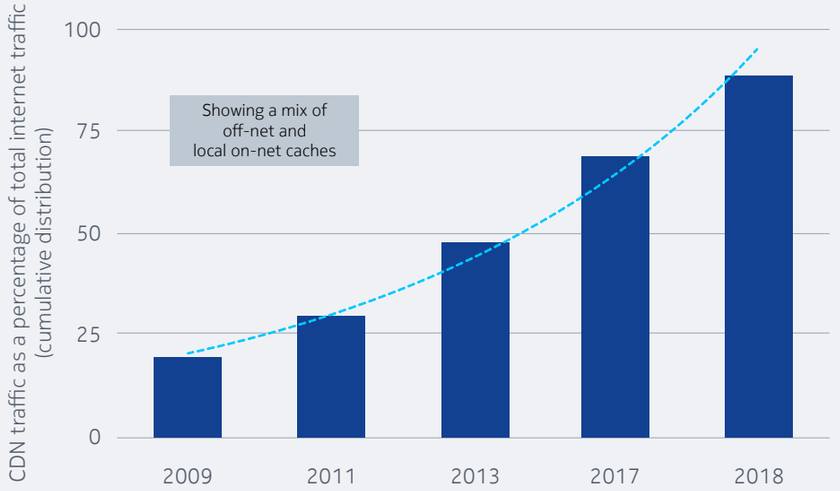


Figure 2. Growth of Content Delivery Networks (CDNs) between 2009 and 2019

Source: Data from SIGCOMM 2010 “Internet Traffic” and Nokia Deepfield research

3. ...whose content needs to be delivered everywhere

As hyperscale giants started to gain huge global subscriber bases, they began to have problems. Soaring demand for video, applications, and services meant that hosting hyperscale content in large, centralized cloud data centers and delivering it over internet transit networks became punitively expensive. What's more, the distance between data centers and end-users introduced latency and sometimes affected quality of service for subscribers.

The hyperscale giants needed to get their content closer to consumers, and the solution came in the form of a new type of provider; the content delivery network. The decade saw a massive upsurge in CDNs, from content-generalists like Cloudflare and Akamai that deliver many different types of content, to CDNs like Netflix's Open Connect or Google's GGC that are optimized for specific content types.

Initially, CDNs brought popular content closer to consumers by hosting close to major national and regional peering sites (internet exchanges or IXPs). Later, they brought it even closer by hosting it within the networks of individual service providers, who evolved their network architectures to incorporate these local (on-net) CDN caches.

Popular content continued to get closer to subscribers, with local edge- and metro-level CDN caches becoming the norm. By 2019, these local caches were delivering ultra-high-definition video, gaming updates, mobile updates, and other services to growing numbers of subscribers, facilitating premium experiences.

CDNs went from carrying less than 25 percent of internet traffic in 2009 to delivering almost 90 percent of it by 2019. The internet was effectively a vast content delivery mechanism, dominated by video and games.

In many ways, this was a win-win-win: subscribers gained high-bandwidth, low-latency, and ubiquitous access to content; hyperscale content providers amassed subscribers while minimizing transit costs; CDNs expanded their business, and communications service providers were able to introduce value-added content bundles on top of basic connectivity plans, and compete in providing best end-user quality of experience.

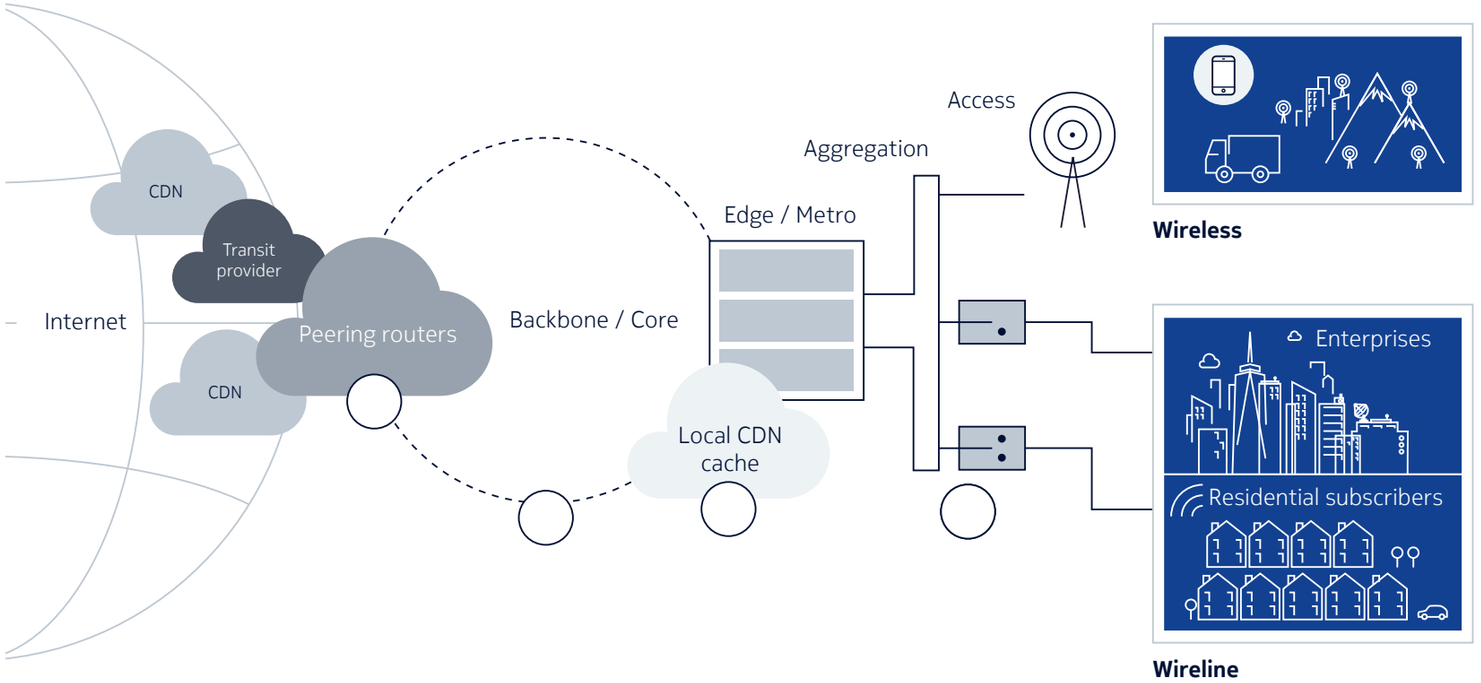


Figure 3. A simplified view of the internet content and services delivery chain

DDoS attacks have entered the terabit era
Both bandwidth and packet intensity are on the rise

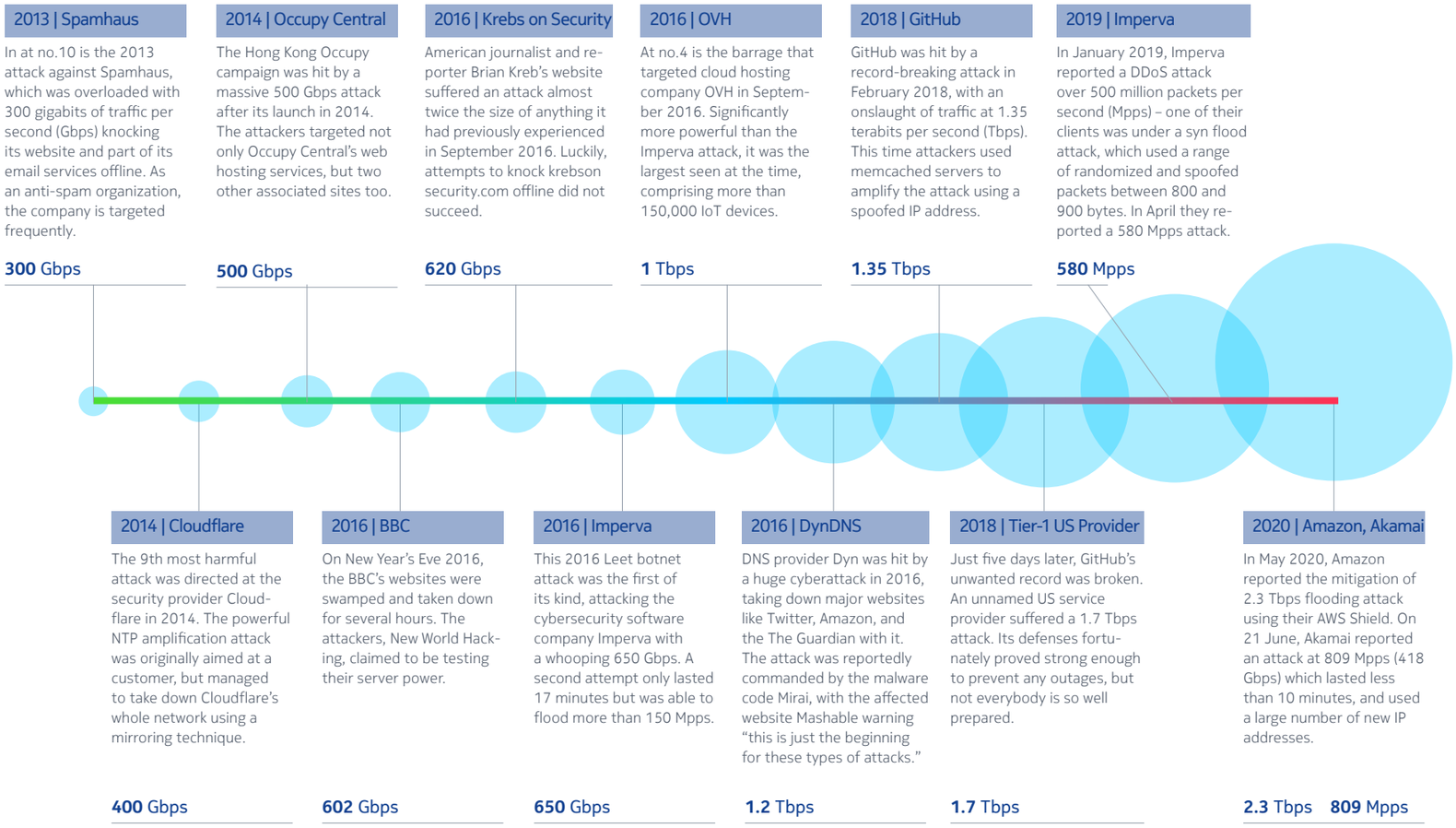


Figure 4. Evolution of major, publicly reported Distributed Denial of Service (DDoS) attacks between 2013 and 2020: Both the bandwidth (in bits per second, bps) and packet intensity (in packets per second, pps) are on the rise

4. An expanded and shifting threat surface

As the internet grew and evolved, the potential for malicious activity also changed significantly, driving service providers to adapt and evolve their security strategies.

The proliferation of connected devices and the expanded worlds of residential and industrial IoT dramatically increased the threat surface. With connected devices having access to much larger bandwidth, and their security capabilities often difficult to understand or control by end-users, the threat surface expanded to the network edge. Malicious actors exploited security vulnerabilities to access millions of unsecured IoT devices and use them as 'botnets' to launch massive DDoS attacks.

Attackers also started to use combinations of attack techniques and vectors to 'shape-shift' their DDoS attacks, changing the mix and intensity of attacks over time and across different parts of the network. Unsecured virtual loads in large-capacity data centers started to be used to launch terabit-level attacks. These attacks can take large parts of network infrastructure out of service, degrade network and cloud services, limit connectivity, and seriously affect critical services like public safety.

Summary

A decade of investment meant networks were in good shape

The decade leading up to the COVID-19 pandemic saw massive and transformative changes in the global network of networks that we call the internet. Some of those changes meant the networks were relatively well prepared for the pandemic when it arrived in 2020.

In particular, CDNs were catering to elevated global demand for cloud-based streaming video and online gaming updates. Many service providers had built out capacity to handle a year or more's growth, modeled around peaks they were already seeing in areas like weekend video streaming. Networks were being designed for elasticity, able to dynamically allocate resources to address changing demand. When COVID-19 came, this prior focus on scale and flexibility meant the networks were largely able to handle the additional demand.

At the network edge, a decade of investment in 4G, fiber networks, and network infrastructure overall allowed service providers to quickly adapt to new circumstances. Consumers in large networks and urban areas found they could rely on their broadband connection for the new demands of home working, homeschooling, videoconferencing, cloud collaboration, and increased video streaming and online gaming. But there were also signs of strain in access networks, especially in remote and rural areas where the new traffic patterns put more stress on the 'last mile.'

One emerging challenge for service providers has been monitoring network activity across all parts of the network. With the majority of traffic originating from the internet, understanding the complete service delivery chain required vast amounts of data collection and analysis. Providers that were able to track how traffic moves from the internet, across CDNs and their network to end-users, were well placed to weather the upheavals wrought by COVID-19. The ability to react swiftly to changing network realities was largely dependent on the holistic internet service chain visibility.

But for the most part, as the pandemic up-ended our lives, our networks kept going – and kept us going, too. Continued network performance in these difficult circumstances served as a great testament to the performance and resilience of service provider networks globally.

Big questions remain for service providers

While the networks by and large held up, the sweeping changes brought about by the still-ongoing COVID-19 pandemic still raise big questions for service providers.

Many saw a year's worth of traffic growth happen in just a few weeks. Will demand ever return to 'normal' pre-pandemic levels or is COVID-era consumption here to stay? If it's here to stay, what does it mean for capacity planning, marketing/service planning, traffic engineering, network security, and network operations?

To help answer those questions, this report looks at what was happening in the networks in 2020 in three key time periods:

- Before the pandemic took hold (prior to March 2020)
- As national lockdowns (or shelter-in-place orders) set in (March–May 2020)
- Six months into the pandemic (September 2020).

We examine the changing traffic patterns first in terms of overall traffic, and then in four key application areas: streaming video, videoconferencing, gaming, and security.

About the data in this report

Data sources

This report contains our findings from two key sources:

Network traffic insights from select service providers

More than 50 communications service providers (CSPs) worldwide use the Nokia Deepfield portfolio of network intelligence, analytics, and security applications to understand and analyze their network traffic in great detail.

With the kind permission of a select number of our customers, we have reproduced in this report the most critical and common insights observed in many networks. Some providers also released public statements about their network performance, which we used to validate our findings.

While every network has its own traffic patterns and characteristics, many providers observed similar effects following the implementation of lockdown measures in their country or region, allowing us to draw parallels and make generalizations about the trends across networks and geographies.

Detailed knowledge about the internet from the Deepfield Genome

Deepfield Genome is our proprietary, detailed map of internet applications and services, and the internet service delivery chain. Its data feeds contain up-to-date information about billions of IPv4 and IPv6 endpoints and IP flows worldwide, categorized by originating domains, CDNs, ISPs, traffic categories, and applications. We have maintained this map for over a decade, and continue to do so with daily internet crawls, scanning anywhere between 200 million and 500 million IP addresses.

You can find more about Deepfield Genome and the Nokia Deepfield portfolio on pages 48–50.

Timescales covered

This report aims to show how network traffic volumes and patterns changed throughout 2020 as the COVID-19 pandemic forced major shifts worldwide in the way we live and work.

It should be noted that the dates and durations of lockdowns varied from country to country. In instances where we refer (for example) to ‘the first week of lockdown,’ we are not referring to a universal reference week, but rather to the week indicated in the accompanying graphic.

Most of our insights were sourced from service provider networks in Europe, the US and Latin America. For that reason, the periods in our report are generally taken as:

Before the pandemic:

- **January–February 2020:** The time of COVID-19 national emergency in China, before the pandemic reached Europe and the Americas.

Early months of the pandemic:

- **March–May 2020:** After the WHO announced a global pandemic on 11 March, with national lockdowns starting from 9 March and easing from May onwards.

Six months into the pandemic:

- **September 2020:** We look at the situation in the month of September, with national lockdowns mostly lifted and many – although by no means all – schools and universities back in session (in person, on-line, and hybrid).

Macro effects of the COVID-19 pandemic

Changing traffic patterns

The investments made in the decade leading up to the COVID-19 pandemic meant that the internet, our global 'network of networks,' was architecturally in good shape to adapt to the massive shifts in traffic volumes that were about to happen.

However, nobody knew exactly how this hybrid combination of networks, data centers, and physical and virtualized infrastructure would cope with the pressure it was about to experience. What would the pandemic impact be on internet traffic, and what would it mean for service providers?

Let's start with some general observations on how traffic patterns changed as lockdowns got underway.

The smoothing of the 'jagged mountain'

In looking at the impact of the pandemic, it helps to know what traffic looks like on a normal day. In many networks, it follows the diurnal nature of human activities: slowly rising during the daytime to reach its peak values in the evening hours.

In normal times, traffic types tend to change during the day, with cloud-based online collaboration, VPN connections, and videoconferencing dominating daytime hours, making way for video streaming and online gaming later in the day. The result is the familiar 'jagged mountain.'

As lockdowns got underway, the shape of the 'mountain' immediately changed. It became much wider, reflecting the prolonged intensity of network traffic during the day, and reached higher peaks, reflecting increased consumption of bandwidth-heavy streaming video. Online gaming increased too, overtaking p2p and social media use in terms of traffic volumes.

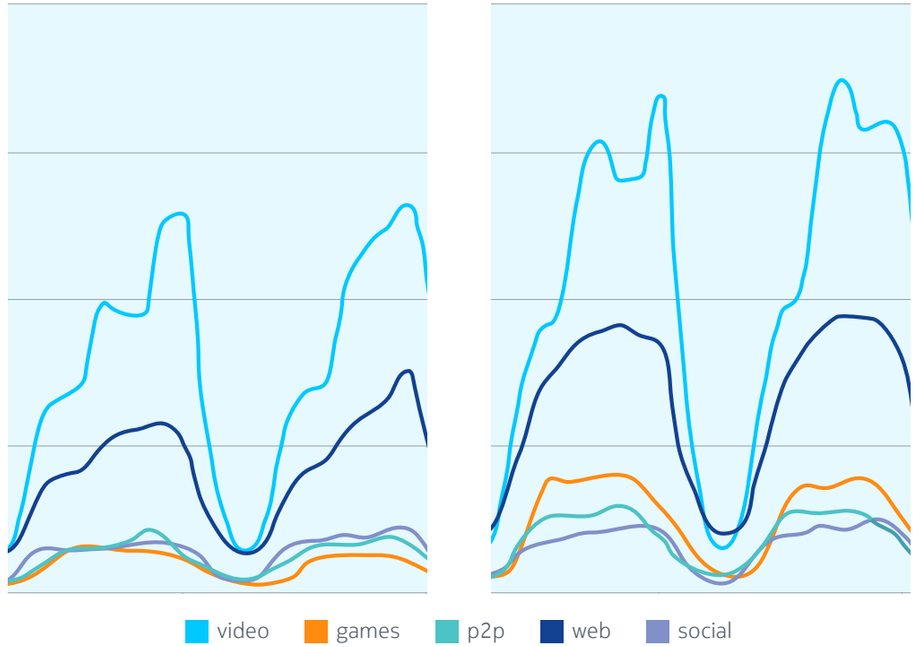


Figure 5. Comparison of weekend diurnal traffic patterns: Pre-pandemic weekend pattern (L) vs. first weekend in a lockdown (R)

Huge increase in the use of messaging apps

What was underlying those shifts? As countries started to implement lockdowns, one immediate change was a significant increase in the use of certain applications.

In the first days of lockdown, the most significant increase recorded was in the use of WhatsApp and other communications apps. People turned to messaging apps to stay in touch with friends, school friends, family, and colleagues.

But while messaging apps saw significantly increased use, their overall impact on network traffic was minimal. Of much more concern to service providers was the increase in bandwidth-heavy traffic types like video streaming and cloud-based gaming applications. Sudden massive demand risked causing congestion on the network, affecting quality of experience for consumers and even connectivity for critical communications.

A year's worth of network traffic growth in just a few days

As service providers had feared, traffic increased immediately and significantly across all application types. At peak hours, traffic increased in the order of 30–50 percent. That represented a year's worth of growth in just a few days, and absorbing most of the headroom built in for the rest of the year.

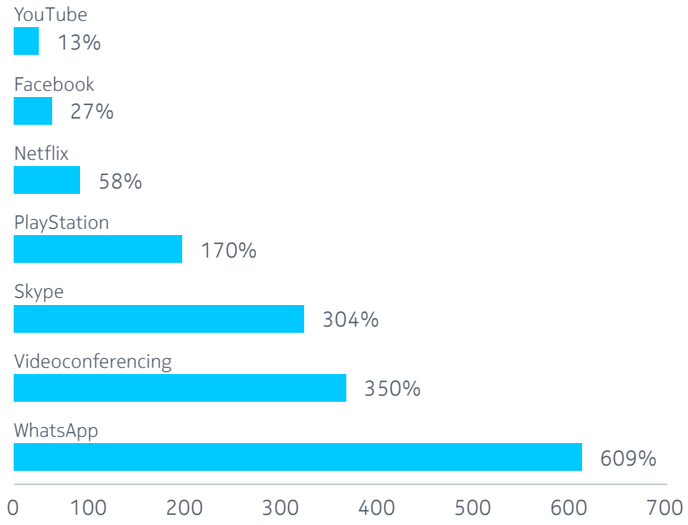


Figure 6. Applications usage change after one week of lockdown – data aggregated from multiple service providers in the EU

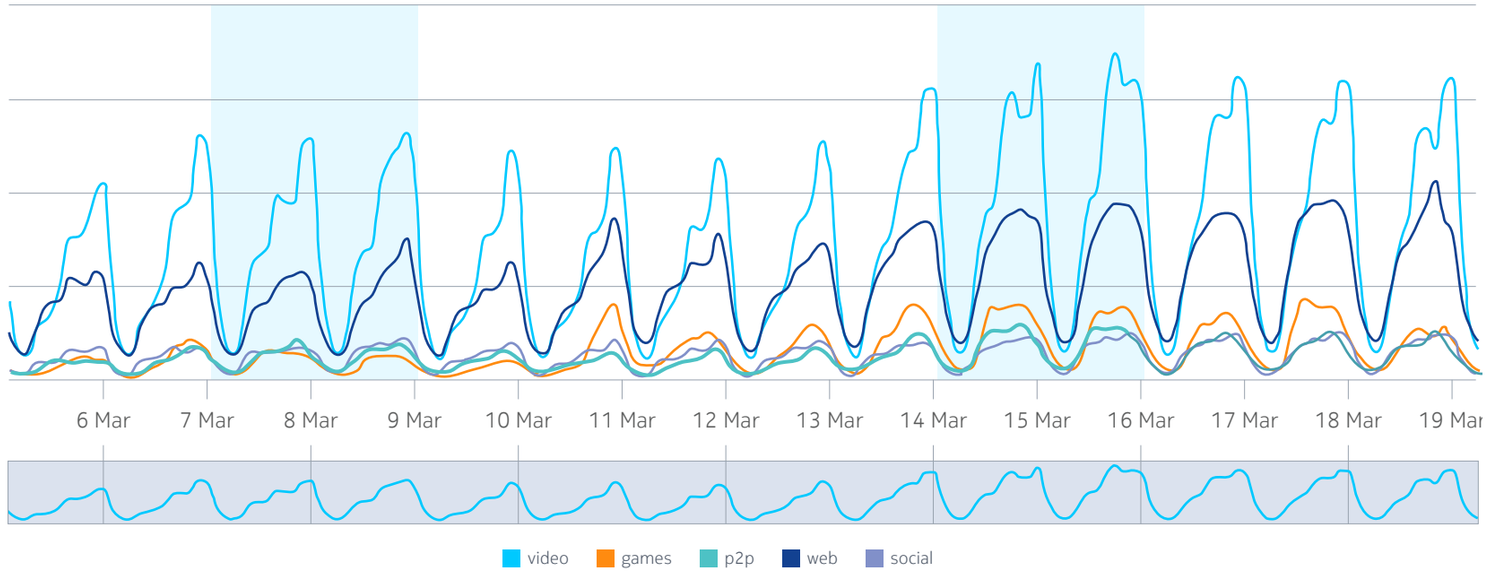


Figure 7. Traffic increase across different traffic categories – data aggregated from multiple service providers in the EU

There were also large increases in aggregate traffic volumes, recorded in MB/GB/TB per day. As more people stayed at home, internet usage became heavier throughout the day, with significant traffic increases during previously 'quiet' times. Snapshots from the first weekday and first Sunday of lockdown show major traffic increases at 09:00 on the weekday and at 13:00 on both weekday and Sunday.

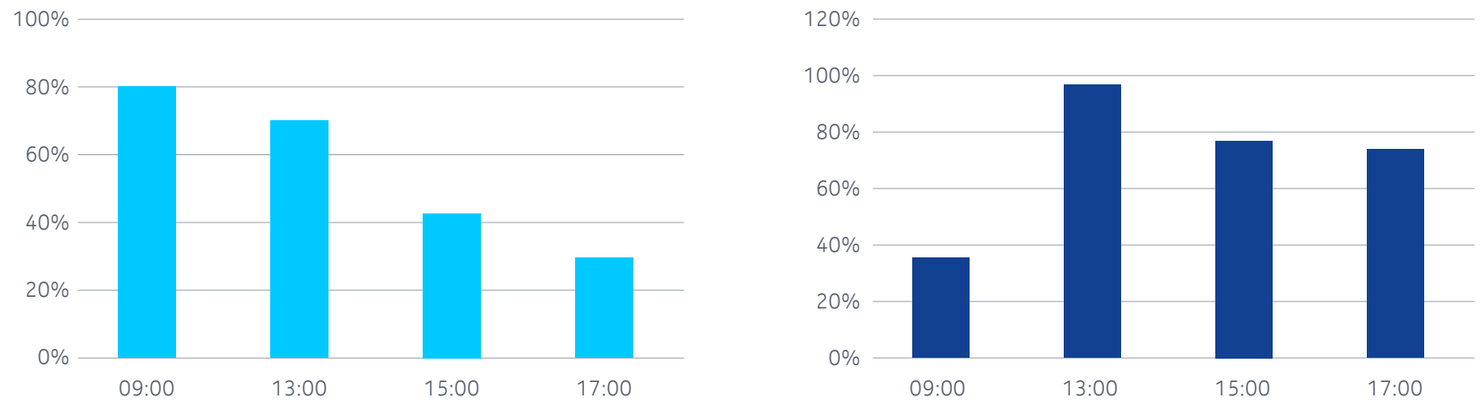


Figure 8. Traffic increases during the first week of lockdown, showing the first day (L) and the first Sunday of lockdown (R), compared to the same days of the previous week – data aggregated from multiple service providers in the EU

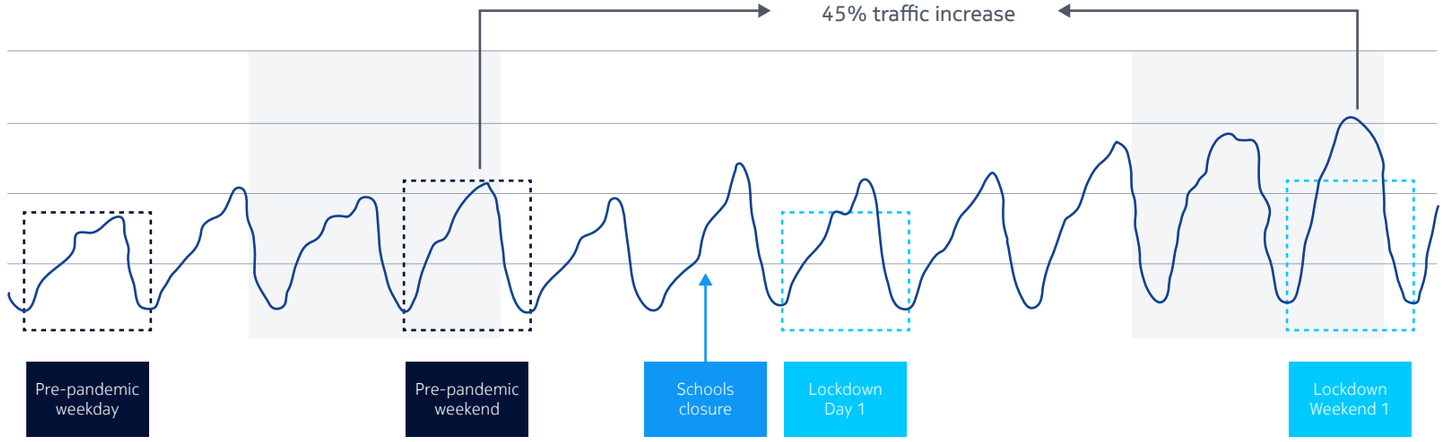


Figure 9. Overall network traffic in one European network shown as diurnal weekly graph and capturing the first week of lockdown

Note: Shaded areas indicate weekends (Saturday and Sunday)

Different service providers saw different patterns

The effects varied between networks, countries, and regions, and often reflected the nature of end-users and customers. Some providers – those catering primarily to an enterprise customer base – even noticed lower traffic levels, as people worked remotely from home.

In the early weeks of lockdown, the concern was that peak traffic levels might continue rising, exceeding the engineered network capacity. By and large, those fears were not realized, as networks across regions continued to perform under increased network loads.

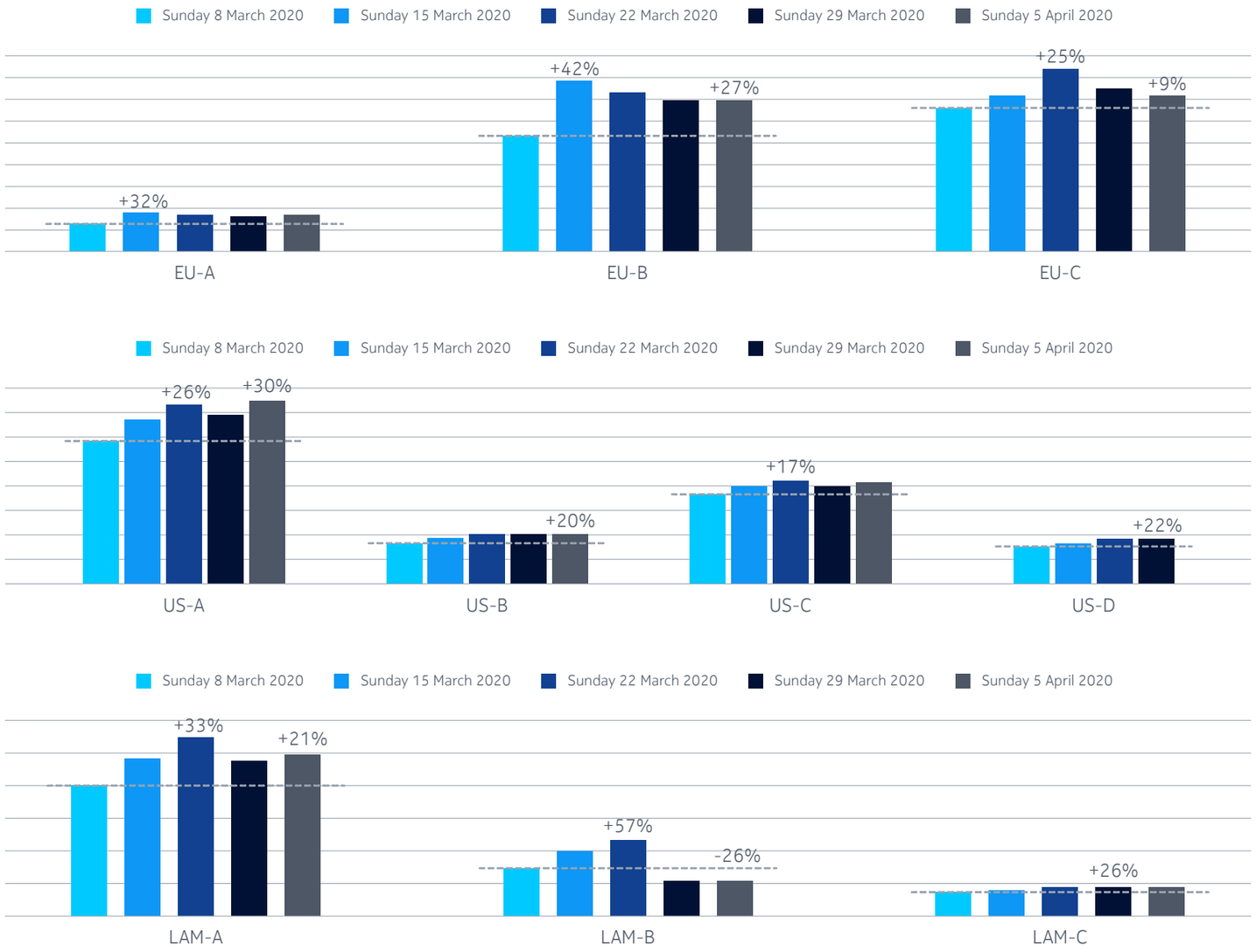


Figure 10. Week-to-week evolution of peak Sunday evening traffic in March 2020 across several networks in Europe (EU-A/B/C), the US (US-A/B/C/D) and Latin America (LAM-A/B/C)

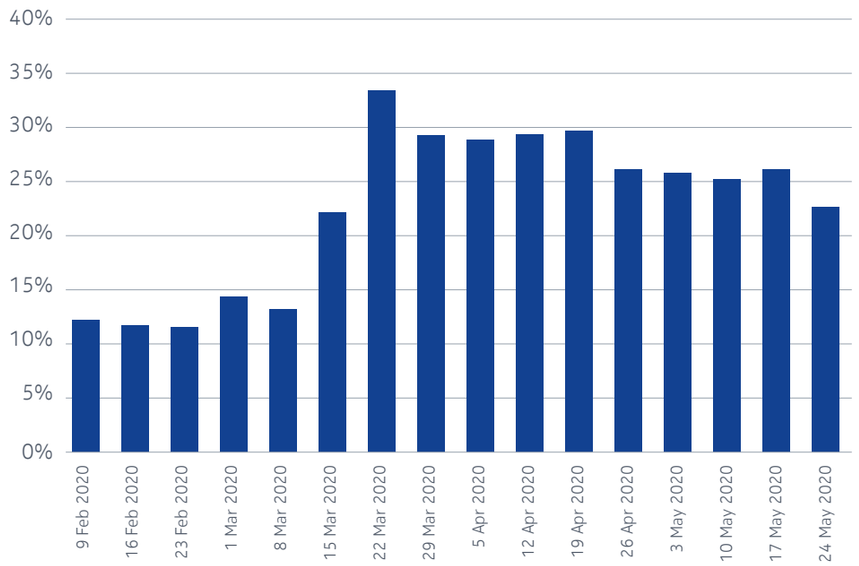


Figure 11. Stabilization of traffic volumes in April-May 2020 at 20-30 percent above their pre-pandemic values – data aggregated from multiple service providers

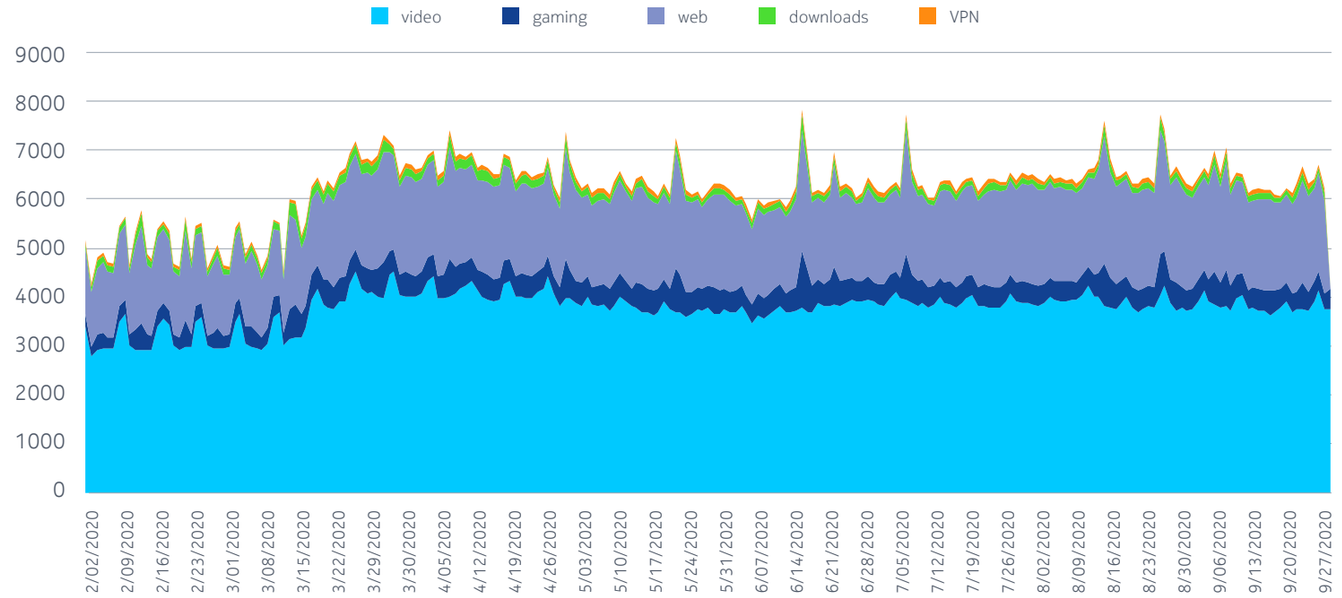


Figure 12. Long-term view on network traffic from February to September 2020, showing average daily traffic per category (in Tbps) – data aggregated across several US providers

May–June 2020: Traffic levels stabilize at 20–30 percent above 'normal'

By May, many lockdowns were starting to be eased or lifted. Peak traffic levels reduced from the first week of lockdown and stabilized in the range of 20–30 percent above pre-lockdown levels.

September 2020: A new network traffic 'normal' – but will it rise again?

In September 2020, we liaised with several service providers globally to gain a longer view of traffic between February and September. Notable regional differences can be observed in the data. In the US, for example, traffic has remained more or less at the same elevated levels since May, with only small variations. Aggregated data from several US networks shows traffic at 20–30 percent above pre-lockdown levels, with increases across all of the most impactful traffic types.

There's a different picture in Europe, where the usual seasonal dip in internet usage occurred over the July and August vacation period. However, overall network traffic still remained above pre-pandemic levels, and by September it was starting to rise again, as it typically does in the final four months of the year.

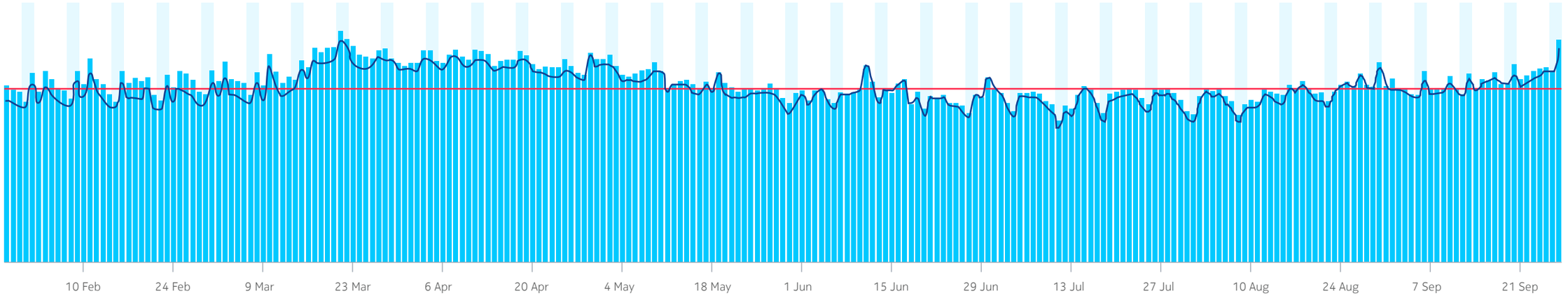
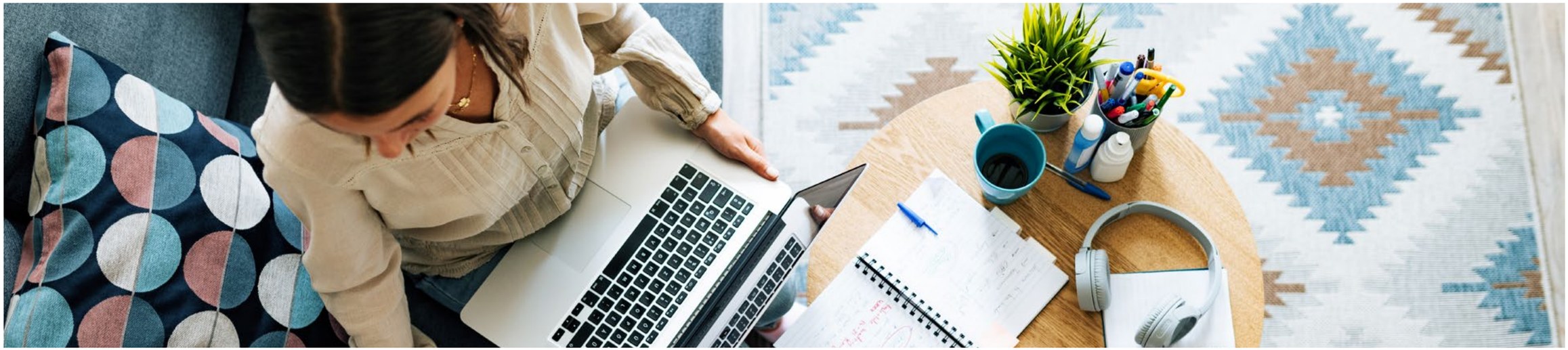


Figure 13. Long-term view on overall network traffic from February to September 2020 from one European network



It remains to be seen what impact this seasonal increase will bring, especially combined with any additional COVID-19 restrictions that may take place in the remainder of the year. However, at the time of writing this report in September 2020, there are no signs of a return to a pre-pandemic 'normal.' Rather, it looks as though we have entered a new network 'normal,' with elevated usage reflected in increased traffic levels.

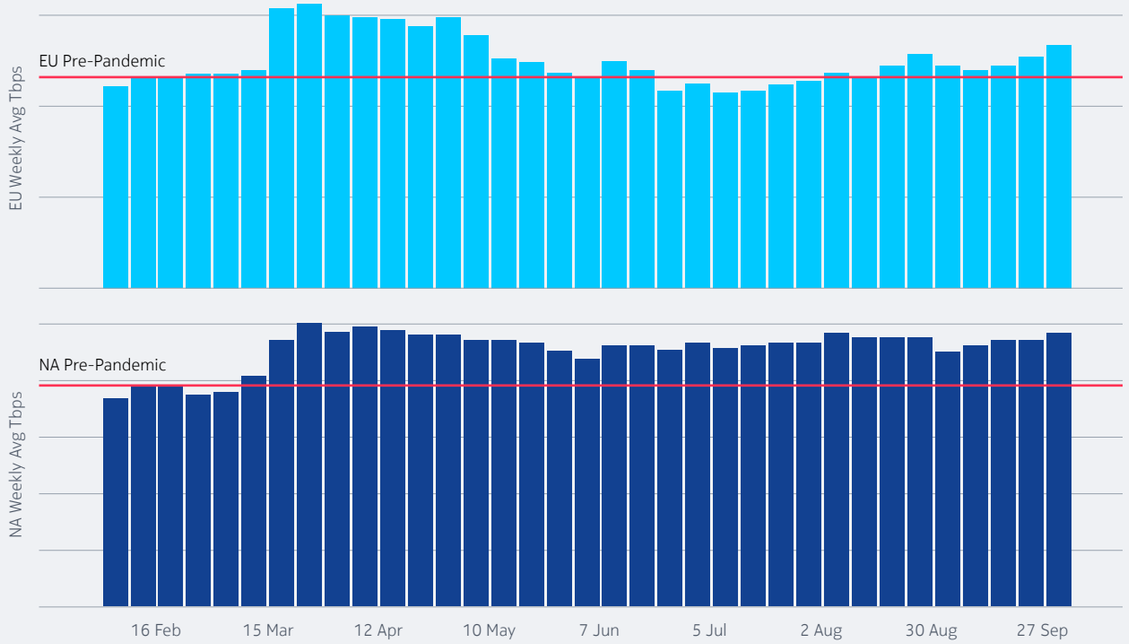


Figure 14. Long-term comparison of the overall network weekly traffic from February to September 2020: European networks (top) vs. US networks (bottom) – data aggregated from several service providers in each region

The diagrams show weekly average totals (in Tbps) and include sent and received traffic across representative number of EU- and US-based service providers. By October 2020, European traffic volumes remain 10–20 percent above pre-pandemic levels while US-based traffic stays 25 percent above pre-pandemic levels.

The world at home

Streaming video on demand

With millions of people confined to their homes, service providers knew they would see an increase in video consumption. This was of particular concern as streaming video on demand – also known as SVOD, video unicast or over the top (OTT) – is the most significant contributor to the overall network traffic. Would the networks be able to take the strain?

Networks were ready for the challenge

When engineering network capacity to address peak demand, service providers typically consider their busiest time of the week – the so-called busy hour (or hours, in case of video). For video streaming, these peaks happen on weekend evenings, usually between 21:00 and 23:00 on Friday, Saturday or Sunday night.

Network capacity is engineered around those peaks, usually with a year's projected growth – some 30–40 percent – built in as headroom. So, when COVID-19 struck, service providers would have had enough capacity for a typical Saturday 21:00 busy hour, plus an extra 30–40 percent of headroom to accommodate the next 12 months' growth.

For their part, video streaming providers and their CDN partners had implemented sophisticated adaptive mechanisms that would allow the speed of streaming connections to adjust to changing network conditions. This means a temporary reduction in the quality of video signal until network conditions improve, but no disruption to the streaming session itself.

Additionally, many video content providers had forged business arrangements with service providers to place 'on-net' video cache servers within their networks, enabling the most popular content to be served within the network, ensuring better service control and quality. So how did these dynamics play out during COVID-19?

Immediate surge in streaming video consumption

As we saw in the previous section, the first thing that happened as lockdown got underway was an immediate surge in overall network traffic volumes. The 30–40 percent increase that would usually happen in a year took place over just a week. As expected, a significant proportion of the surge was increased consumption of streaming video.

Peak video streaming levels were way above the headroom most service providers had built into their networks. Streaming video risked eating up all of the providers' bandwidth, leaving no capacity for essential activities like remote learning, work videoconferencing, or keeping in touch with vulnerable relatives and friends.

Then two things happened that allowed the networks to keep running, and consumers to keep watching their favorite shows and movies. One was a voluntary reduction in streaming bitrates, and the other a shift in the way content was delivered to subscribers. Let's look at each in turn.

Regulatory pressure leads to voluntary reductions in streaming speeds

Service providers saw surging traffic volumes from all big streaming video providers in the first week of lockdown, including Netflix, YouTube (Google) and Prime Video (Amazon). Compounding the problem was the EU launch on 24 March of Disney+ and its much-awaited Star Wars spinoff show, The Mandalorian.

As peak demand put an unprecedented load on internet infrastructure, the European Commission started to consider regulatory measures against Netflix and other streaming platforms to force them to switch from high definition (HD) to standard definition (SD) streaming quality.

In a move to pre-empt any mandated regulatory decisions, large video streaming providers took voluntary action to reduce their streaming bitrates and video quality. On the days leading up to 20 March, with lockdowns underway in several European countries and more imminent, Netflix, Google, and Prime Video (Amazon) announced their intention to switch to SD streaming in Europe.

Deepfield network data provided to us by a selection of European operators shows an immediate reduction in overall Netflix traffic volume on the second weekend of lockdown, while Google/YouTube and Prime Video (Amazon) reduced their streaming speeds in late March. The notable exception was Disney+, which launched with HD streaming in several EU countries on 24 March. Disney+ appeared not to have reduced its bitrate at all during the lockdown period, continuing to stream above 4 Mbps (average bitrate), and potentially delivering better video quality than its competitors.

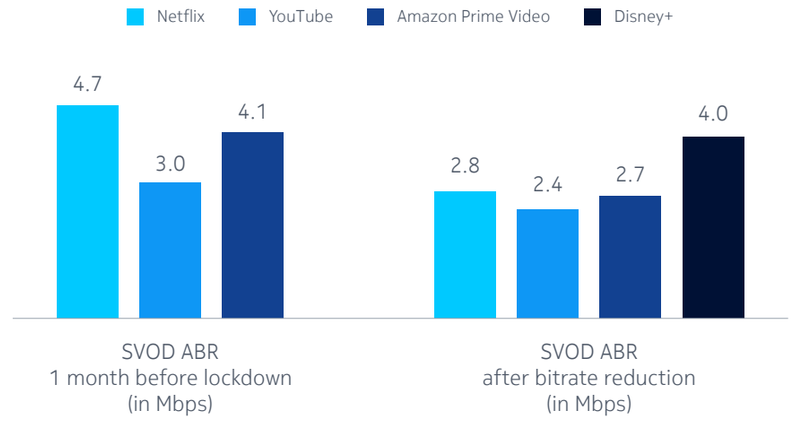
Interestingly, in one network, the decrease in average bitrate (ABR) of Netflix streaming sessions coincided with a further increase in the number of individual Netflix streams from the previous record-breaking weekend.

However, even with more video sessions being watched, reduced streaming rates brought significant relief to the network. Overall traffic peaks stabilized at 26 percent above their pre-pandemic levels, compared to a 59 percent of traffic peak increase during the previous weekend.

Overall network traffic

+59%
increase from pre-pandemic levels

+26%
increase from pre-pandemic levels, after 20% of streaming video speed reduction



Note: Netflix reduced their streaming speeds in EU on March 19/20.

Figure 15. Streaming video on demand average bitrates (SVOD ABR) for four major video providers in the EU, before and during lockdown

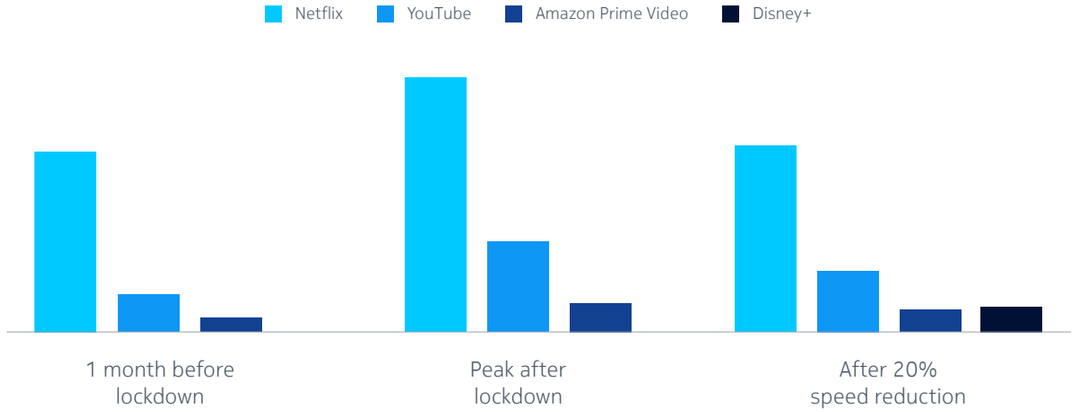


Figure 16. Overall streaming video traffic volumes for four major video providers in the EU, before lockdown (L), during lockdown (center) and after 20 percent of speed reduction (R)

Demand overwhelms on-net caches, prompting a doubling of peering traffic

Reduced streaming bitrates weren't the only reason the networks held up. While consumers may have noticed no difference in the quality or availability of streaming video, service provider networks saw a significant shift in how the streaming video was delivered.

In pre-pandemic times, more than two-thirds of streaming video content would typically be delivered from on-net CDN caches, close to subscribers. These caches would serve the most popular or current content to subscribers without requiring that content to be delivered from the internet.

Deepfield data shared with us by service providers shows that the explosion in demand for streaming video quickly overwhelmed many on-net caches, forcing the demand to be satisfied by the content delivered from the internet – across peering and transit routers.

This resulted in about 20 percent growth in traffic delivered from on-net caches, as they seemingly hit the limits of their capacity. Delivering additional content from the internet resulted in an incredible 101 percent growth in traffic delivered across the peering layer.

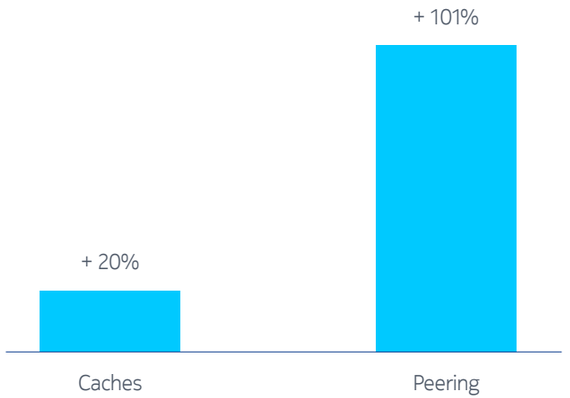


Figure 17. Comparison of increase of Netflix traffic in lockdown: delivered on-net (from caches) vs. off-net (across the peering layer) from one EU network

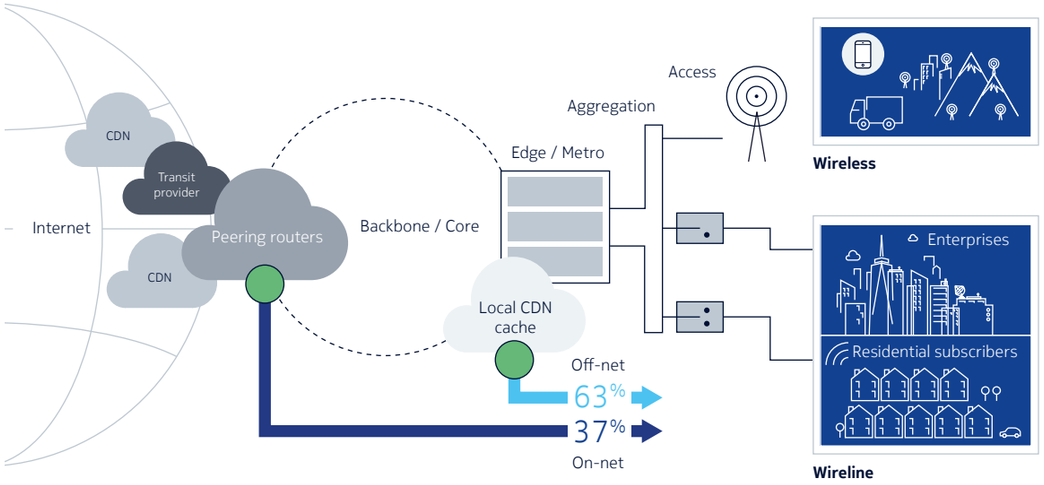


Figure 18. Comparison of Netflix traffic ratios during lockdown: delivered on-net (from caches) vs. off-net (across the peering layer) from one EU network

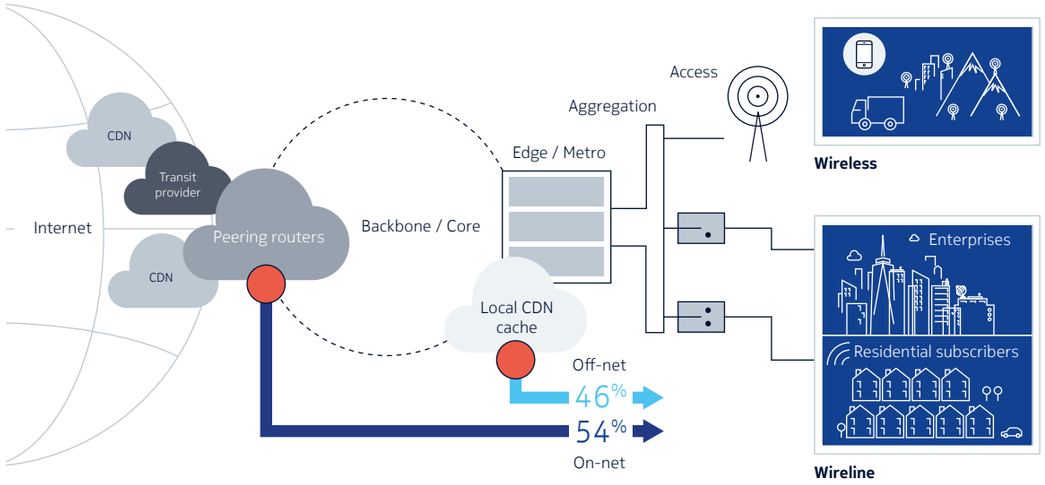


Figure 19. Comparison of Netflix traffic ratios before the pandemic: delivered on-net (from caches) vs. off-net (across the peering layer) from one EU network

The shift can be seen in the ‘before’ and ‘during’ illustrations of the Netflix delivery chain. In the EU network shown here, before the pandemic, 63 percent of Netflix content was delivered from local on-net caches. During the pandemic, that fell to 46 percent, with the majority (54 percent) of content being delivered directly from the internet across the peering layer.

It was an impressive stress test for the whole video service delivery chain. This particular service provider continued to satisfy customer demand and ensure the customer experience by delivering additional content from the internet while incurring additional strain on their network.

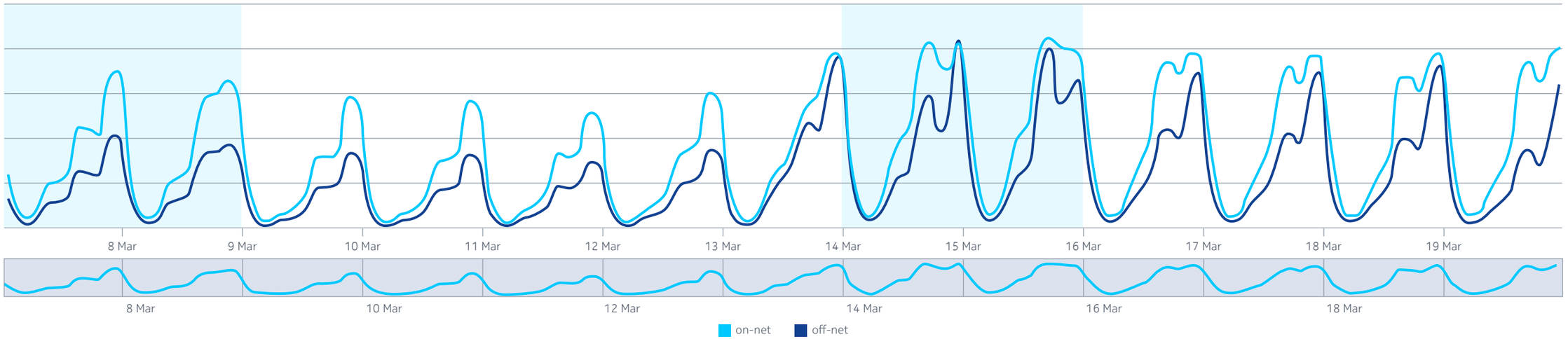


Figure 20. Diurnal graphs showing Netflix traffic in lockdown: delivered on-net (from caches) vs. off-net (across the peering layer) from one EU network

Note: Shaded areas indicate weekends (Saturday and Sunday)

Case study: Netflix

As the world's biggest streaming video provider by subscriber count, Netflix typifies the massive shifts in video consumption patterns that occurred in the first week of lockdown.

Firstly, people started watching Netflix earlier in the day. There was a 97 percent increase in morning traffic volumes over the previous week and a 27–42 percent increase in the early afternoon. By contrast, weekday evening viewing remained relatively manageable, with only a 20 percent increase over a pre-pandemic weekday evening. Weekend streaming, however, skyrocketed. At the first 'busy hour' after lockdown, there was a 54–72 percent rise in Netflix traffic volume over the previous weekend's busy hour.

Netflix viewing increased even further in the second weekend of lockdown. The launch of individual shows also had a measurable impact. In one EU network, the release of a new Netflix season contributed to 36 percent increase in number of individual streams, resulting in new lockdown weekend peaks.

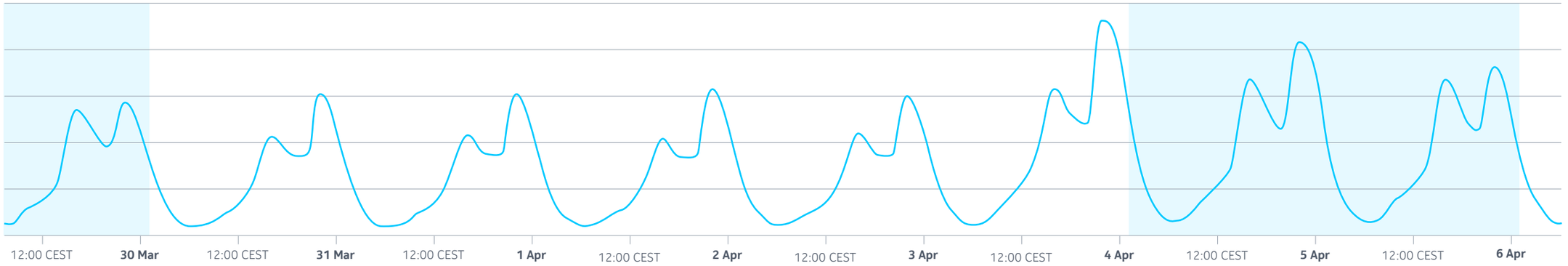


Figure 21. Diurnal graph showing Netflix traffic in one European network

97%
increase in morning traffic

27-42%
increase in the early afternoon

20%
increase in weekday evening viewing

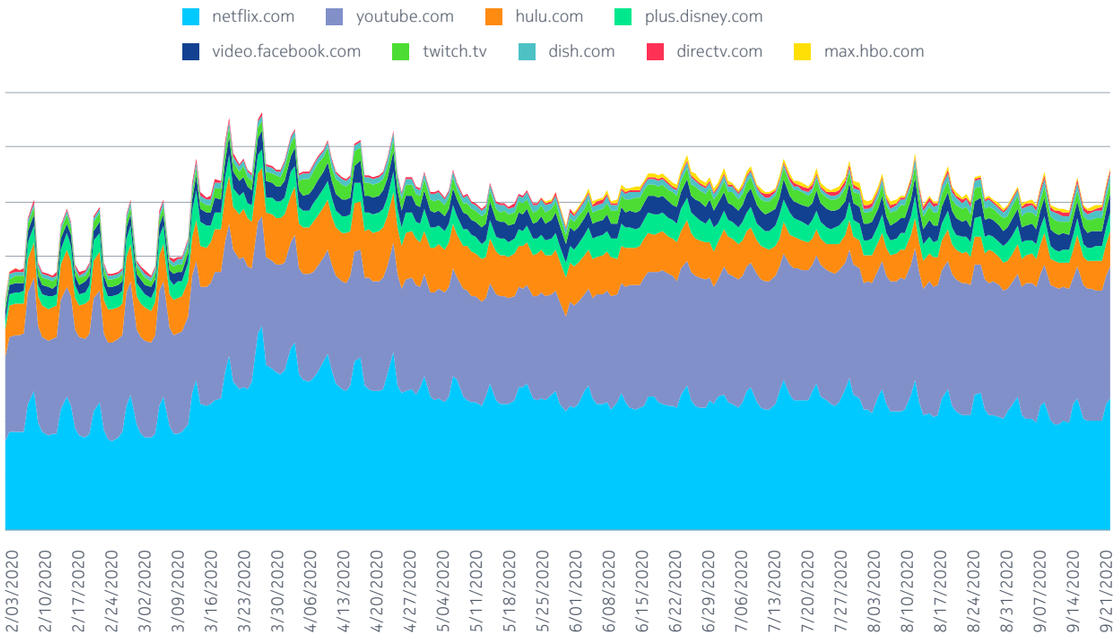


Figure 22. Streaming video traffic by video providers between February and September 2020 – data aggregated across multiple US service providers

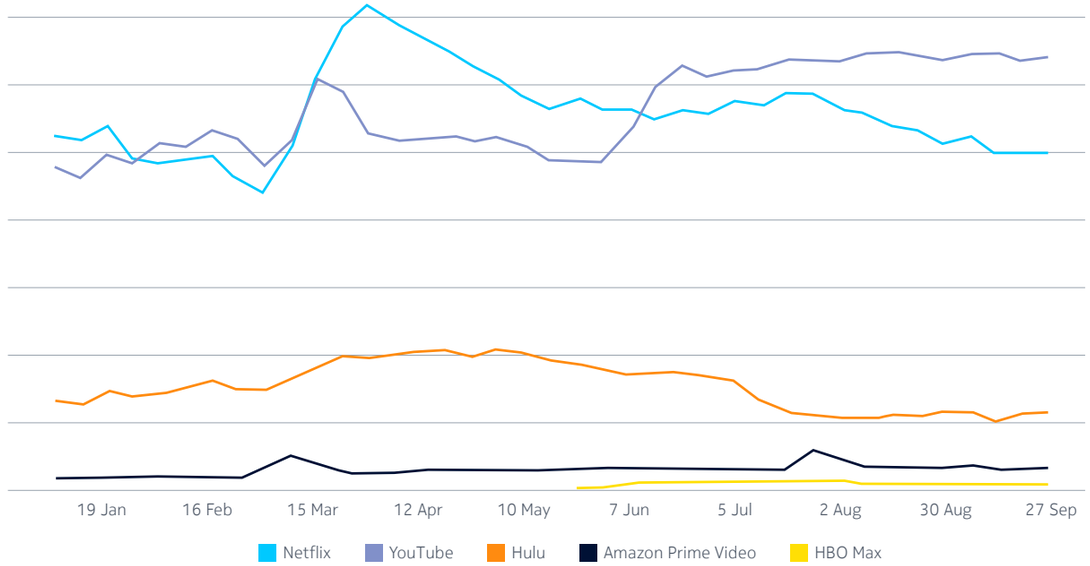


Figure 23. Streaming video traffic by major video providers between February and September 2020, data aggregated across multiple US service providers, showing relative traffic proportions

September sees a return to familiar patterns – but at a higher level

After the initial rush, video streaming traffic began to normalize by June in many areas worldwide. Both peak traffic and aggregate traffic levels stabilized at 25–30 percent above pre-pandemic levels, and video providers gradually restored HD streaming over the course of June and July.

Netflix and YouTube continued to dominate the 'new normal,' accounting for the majority of video streaming traffic in many networks. In the US, YouTube even overtook Netflix to become the leader in terms of network traffic.

In the EU, meanwhile, Netflix restored normal streaming speeds in different countries at different times. Data from one network in Spain shows that 'normalization' to pre-pandemic speeds happened as late as in July.

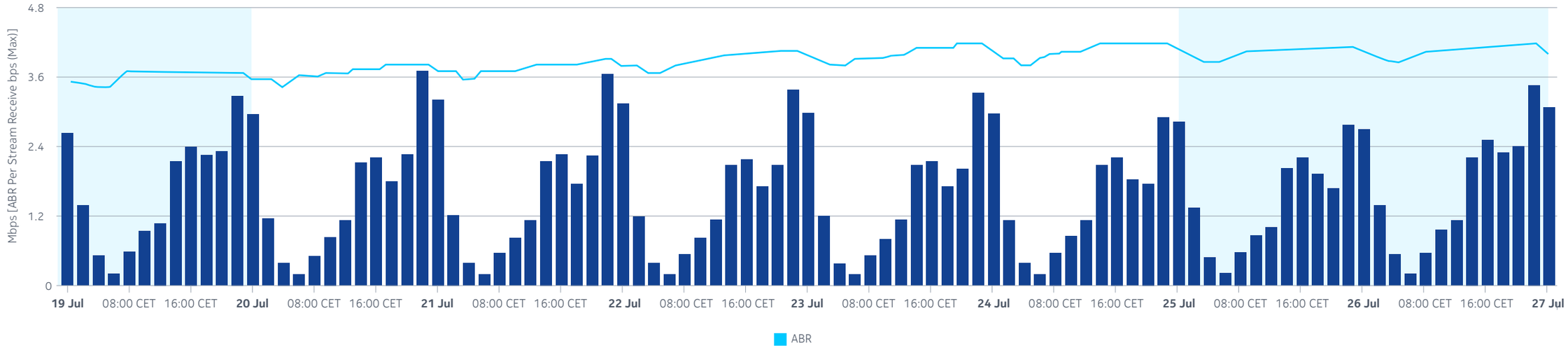


Figure 24. Netflix streaming speed returning to normal – data from one European network. Bars indicate the number of concurrent video streams

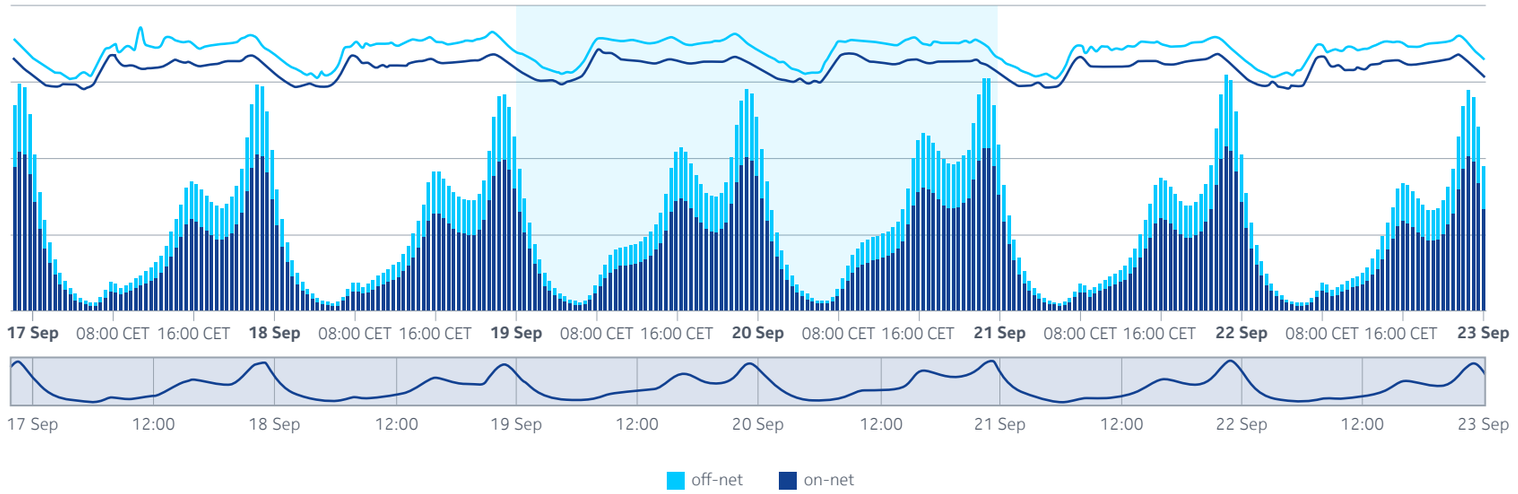


Figure 25. Netflix on-net and off-net traffic ratios returning to their pre-pandemic ratios – one European network

The split between on-net and off-net content was also returning to normal, pre-pandemic ratios by September. Data from one EU network shows the ratio to be roughly 2.20:1 on-net vs. off-net, which is very similar to the pre-pandemic split we described earlier.

Group watching emerges as a new trend

An interesting new trend allows physically dispersed people to watch movies simultaneously using a form of controlled and limited multicast. Plex was first to launch in May 2020,[2] followed by Disney+ with its GroupWatch feature.[3] Spotify also introduced similar functionality for music streaming.[4]

2. TechCrunch, Plex launches a co-watching experience for its on-demand library, 28 May 2020
3. The Verge, Disney+ is slowly rolling out a new party watch feature, 11 September 2020
4. TechCrunch, Spotify officially launches a shared-queue feature, 11 May 2020

Changing habits as people watch more video earlier in the day

The data shows that streaming habits also changed during the year. A comparison of weekday streaming traffic patterns in February and September reveals that 60 percent of peak traffic is now reached by 13:00 in September, compared to 45 percent of peak traffic by 13:00 in February indicating more users watching video both earlier and throughout the day.

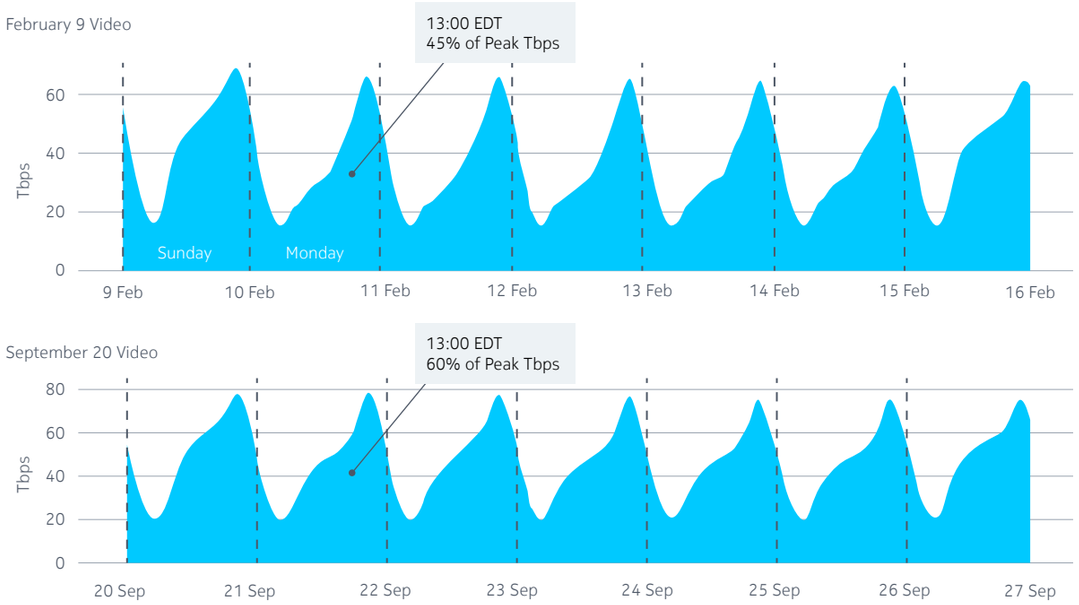


Figure 26. Comparison of streaming video diurnal traffic patterns in February and September 2020 – data aggregated from several US-based service providers

A 30 percent increase in new IP video endpoints adds to traffic levels

It appears that not all of this additional streaming video traffic was due to increased consumption by existing subscribers. We looked at the number of new unique IP addresses consuming streaming video – indicating customer premises equipment endpoints such as residential gateways and cable modems. Data from US networks shows a significant increase of around 30 percent in unique IP addresses,* indicating a significant rise in the customer base (all video streaming providers combined). The 30 percent increase in unique subscribers consuming video suggests that previously discussed increases in video and overall traffic are largely due to more consumers watching video rather than stemming from the increased video usage of pre-pandemic subscribers.

* We define unique IP addresses as either AAA or a unique IP address. Note that this unique IP represents a single customer endpoint that may include multiple users and devices in a household.

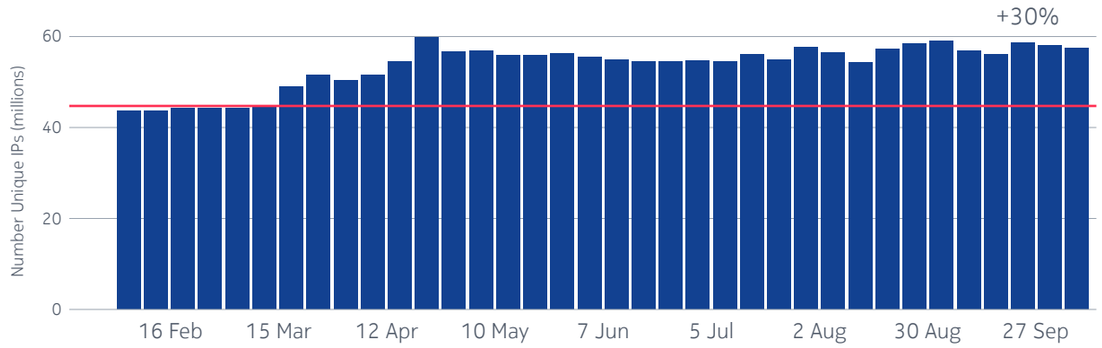


Figure 27. Unique IP addresses consuming streaming video (multiple US networks)

Key takeaways for service providers

Streaming video

The long-view data from 2020 shows that video streaming is not going away. With demand remaining high, more platforms coming to market, more new subscribers, and rising adoption of multiple video streaming subscriptions, we may see additional strain on networks in the future.

Service providers therefore need to understand how traffic is being delivered and consumed, and how this consumption is changing and evolving. An essential requirement is to fully understand the complex video streaming delivery chain. Many video providers use several CDNs in parallel to ensure premium quality, which can obscure the source of the traffic for service providers.

For example, Deepfield data shows that in some European networks, Disney+ was using up to six different CDN providers at launch to get its content out to subscribers. The ability to capture this level of detail is vital for service providers to better understand and benchmark these services.

The same data can also inform sales and marketing strategies – using streaming video insights to understand which video platforms and shows are most popular with select demographics, and create offers, bundles, and optimize their service plans accordingly.

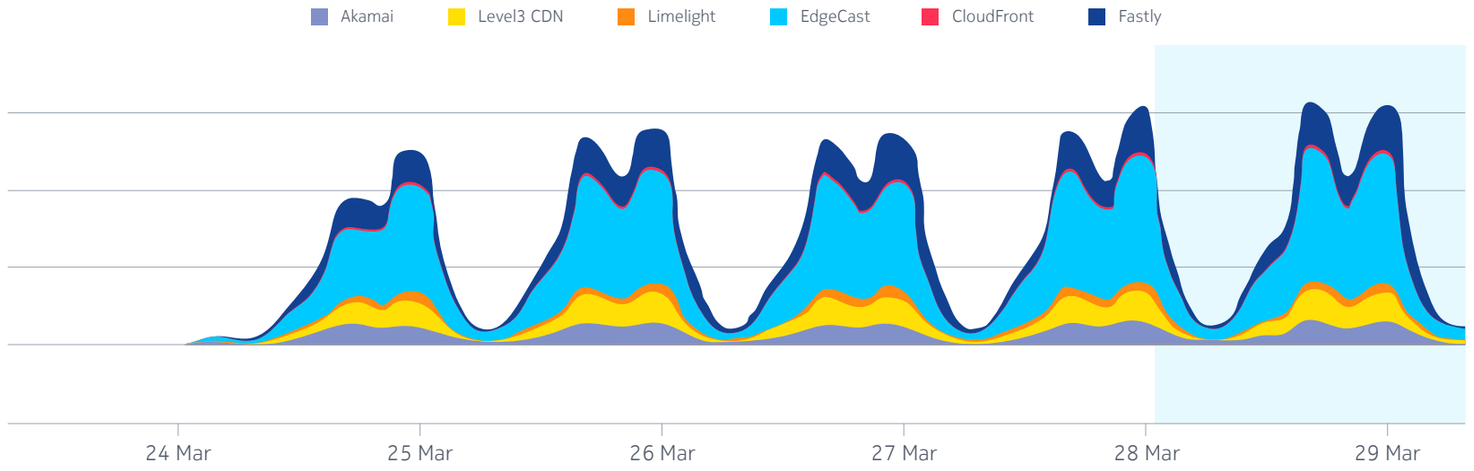


Figure 28. Disney+ used six CDNs to get content to subscribers in its first week of new service launch in a number of EU countries

All these insights may also feed into planning and decision-making around the 5G rollout. With broadband access already under pressure in consumers' homes, 5G (in both its enhanced mobile broadband (eMBB) and fixed wireless access (FWA) incarnations) could provide improved access as an in-home backup or addition, or a replacement of the fixed-line internet – enabling more consumers to enjoy streaming video while offering much-needed cost efficiency to service providers.

How Nokia Deepfield can help

Nokia Deepfield can provide deep insights and at-a-glance analytics for the most important aspects and tracking parameters for streaming video. For example, on a single screen, Deepfield can visualize the number of streaming sessions and average bitrate for on-net and off-net traffic (see graphic).

As users embrace multiple video streaming services, service providers can benchmark, monitor, and track the adoption of new video services, to continuously improve delivery and subscriber experience. In the example (below), a US operator captured initial uptake of HBO Max, introduced on 27 May.

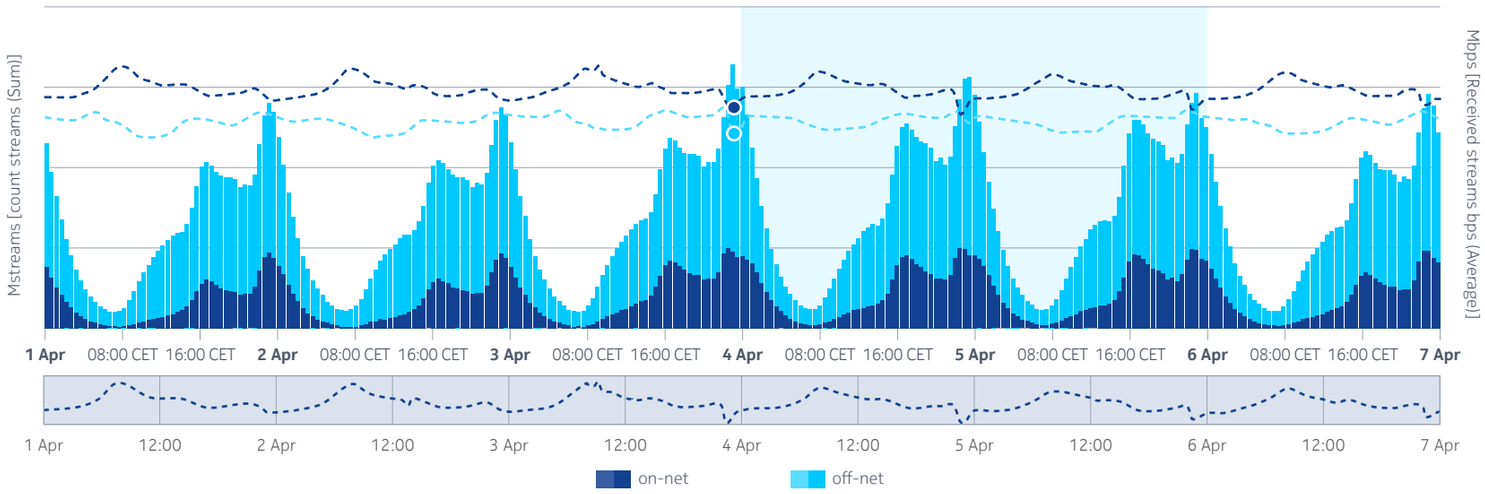


Figure 29. Using Nokia Deepfield to get real-time, at-a-glance insights into video streaming

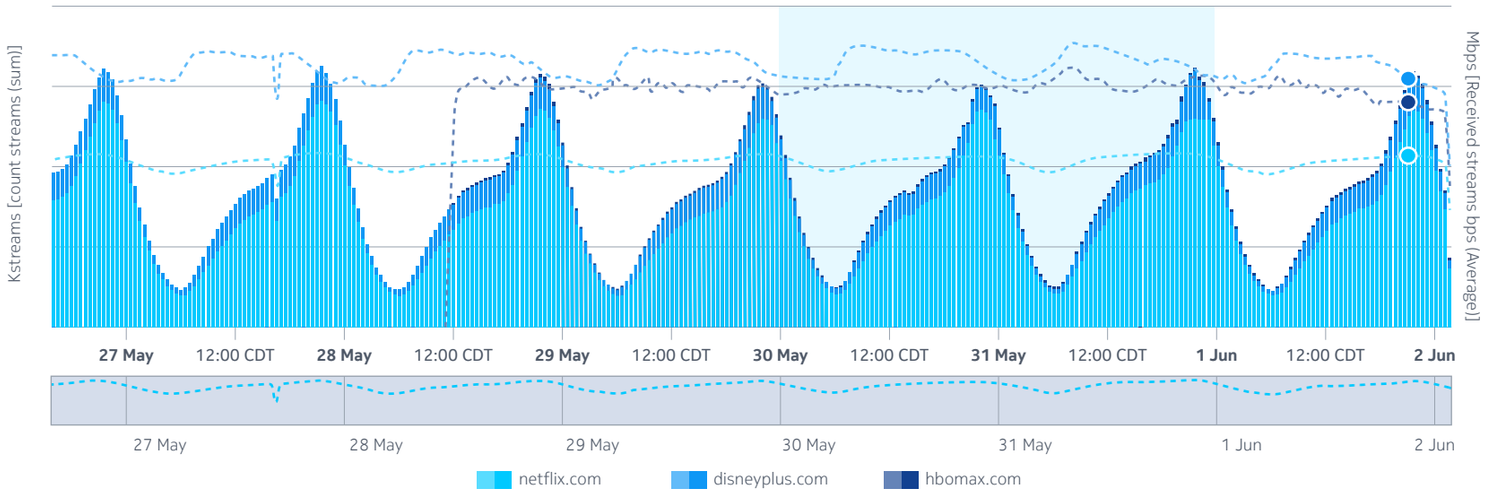


Figure 30. Using Nokia Deepfield to track the introduction of new streaming service (example of HBO Max, one US-based network)

The world at work

VPNs and videoconferencing

The COVID-19 pandemic didn't just transform downstream video consumption. Patterns of upstream traffic shifted too, as people started working from home en masse. Generally, Deepfield customers recorded an upstream bandwidth increase in the range of 30–35 percent, attributed mainly to the increased use of cloud collaboration and videoconferencing.

Many companies that use corporate virtual private networks (VPNs) to allow remote workers access to corporate networks and resources found that increased demand was bringing their VPN infrastructure to a halt. Moving to cloud-based collaboration tools and resources such as Microsoft Office 365 took pressure off their VPN networks and shifted traffic toward the use of webscale-based infrastructures.

Meanwhile, meetings that would have taken place face-to-face moved to videoconferencing platforms instead. As the videoconferencing bug took hold, audio calls shifted to those platforms, too, often becoming video calls instead. Platforms like Zoom, Webex, Microsoft Teams and Google Meet experienced tremendous growth, starting a competitive battle for corporate users.

And teleconferencing wasn't just for work. Schools introduced remote video learning for students of all ages, and friends and families who could no longer meet in person began to keep in touch over video. For many, it was their first time using the technology, with videoconferencing providing a vital lifeline to their families, friends, and online communities.

The shift created significant challenges for providers, with videoconferencing platforms overwhelmed with demand for real-time video processing, and service providers having to deal with huge demand for upstream bandwidth from residential connections that weren't designed for heavy upstream use. To provide some context around the shifts service providers and videoconferencing companies had to deal with, let's look at consumer videoconferencing in more detail.

Rise in VPN use

Lockdowns had an immediate effect on VPN use. Service providers saw a rise in VPN traffic as people connected from home. While this initial growth was not significant in some networks, others recorded growth of about 80 percent, with significant traffic on weekends.

Many corporate VPN infrastructures were seriously challenged, as they had not been designed to support that many remote workers concurrently. The solution for many companies was to move to cloud-based collaboration.

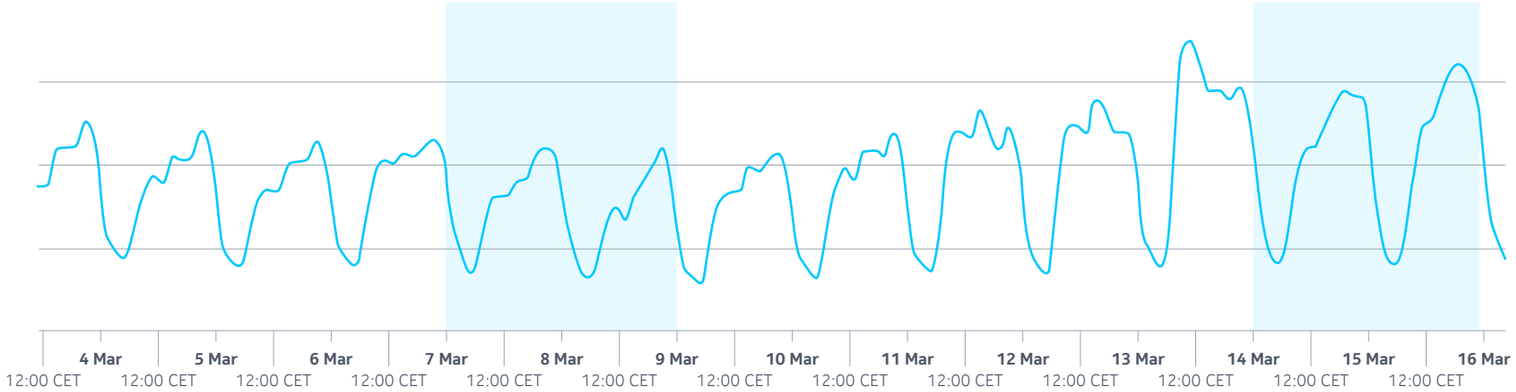


Figure 31. Example of an EU-based network operator seeing 80 percent increase in VPN traffic in the first week of lockdown

Week 1 of lockdown sees a 350 percent jump in teleconferencing

The impact of the lockdowns was immediately visible. The first week of a lockdown saw a 350 percent increase in teleconferencing traffic as people scrambled to move their daily in-person meetings to videoconferencing calls. While it has long been touted as a transformational technology and a viable replacement for business travel, videoconferencing had never been seen on this scale before.

Case study: Zoom

Between March and June 2020, Zoom emerged as the most popular videoconferencing platform, eclipsing rivals like Microsoft Teams, Skype, Webex and Google Meet.

Already perceived as the 'trendy' option for business teleconferencing, with some (at the time) differentiating features like 'gallery view,' Zoom greatly benefited from the increased demand. Deepfield data from one Tier-1 US provider shows a 700 percent increase in Zoom traffic in the first week of lockdown, far more than Webex and Skype (whose traffic also spiked, just not nearly as much).

While generally thought of as a business platform, Zoom also saw spikes on weekends. In certain parts of the US, this correlates to churches with large congregations switching to online services. At the same time, Zoom's free entry-level service plan allowed calls of up to 40 minutes; enough time for non-commercial users to use it to keep in touch with family and friends.

How did Zoom cope with the surging demand? Deepfield data shows that it started to use external, cloud-based resources in addition to its own servers. This was especially visible for Amazon's AWS-based Zoom service (see graphic).

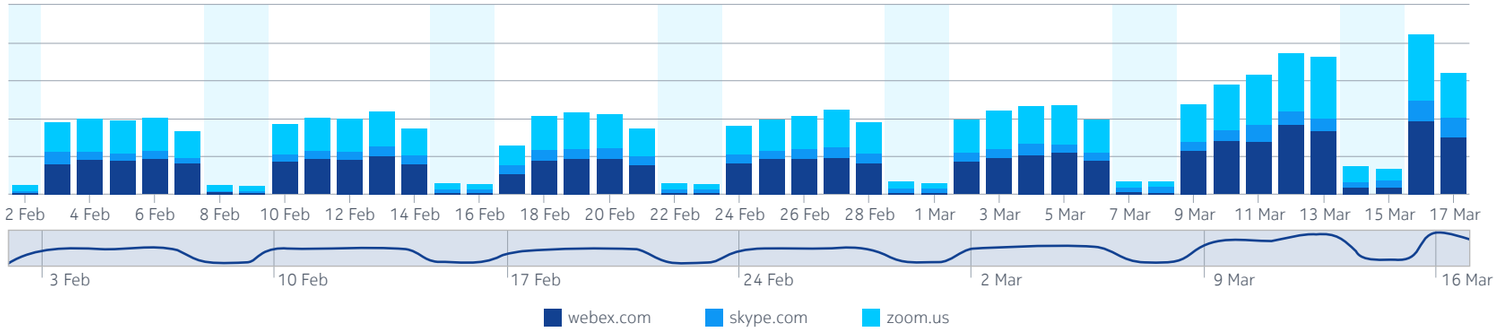


Figure 32. Bandwidth distribution across major videoconferencing services, February-March 2020 (Tier-1 US network)

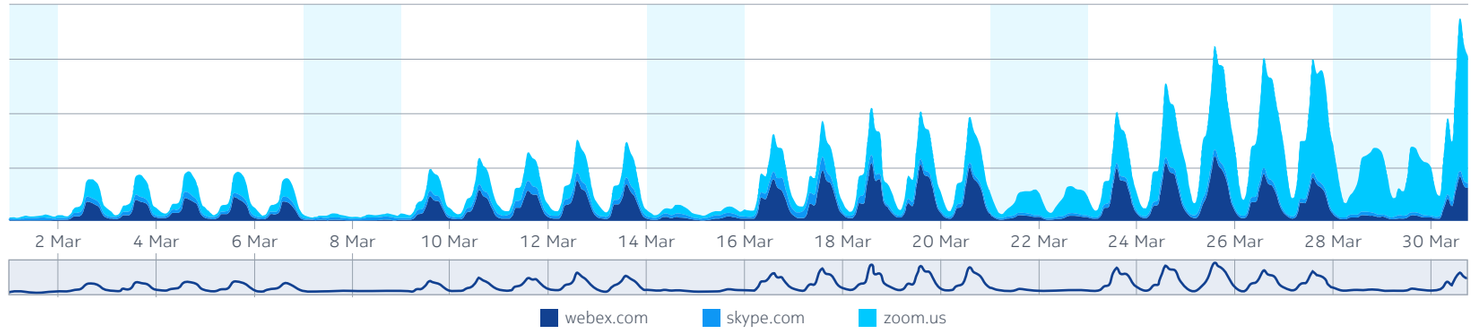


Figure 33. Phenomenal growth of Zoom traffic in the first weeks of lockdown (Tier-1 US network)

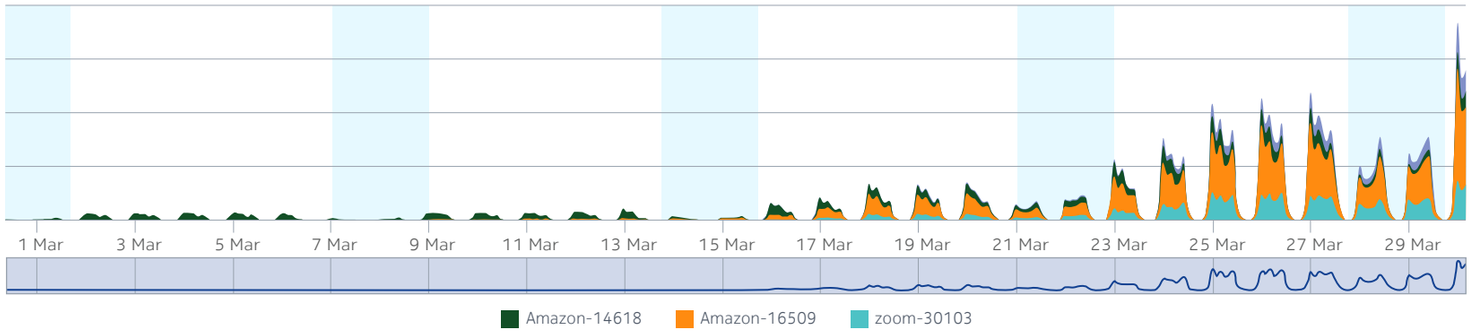


Figure 34. Zoom uses multiple cloud platforms to deliver videoconferencing services as lockdown gets underway

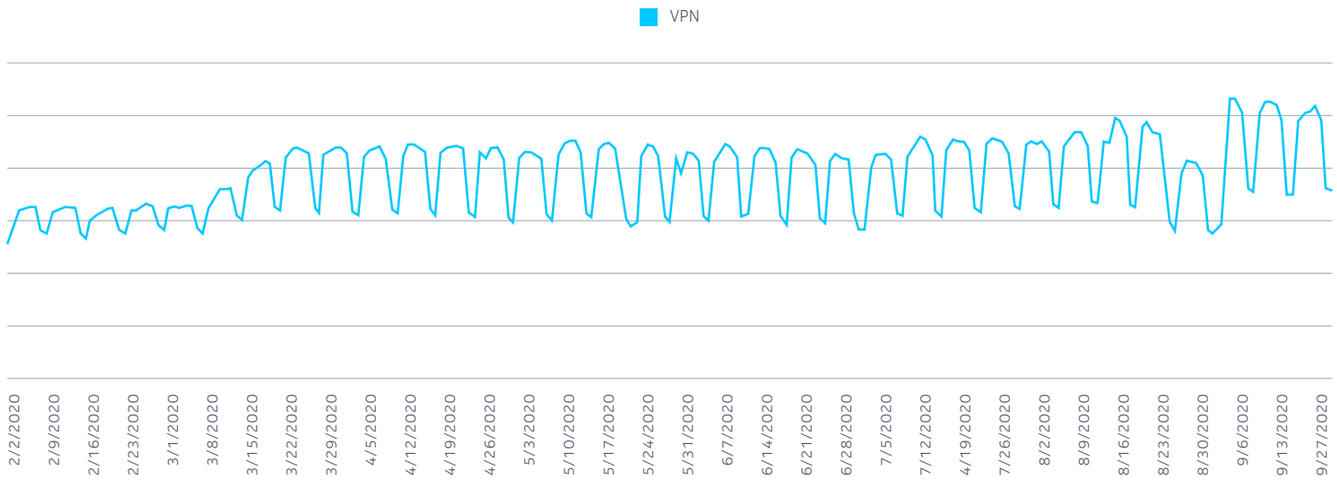


Figure 35. Aggregated VPN traffic from several US service providers, February-September

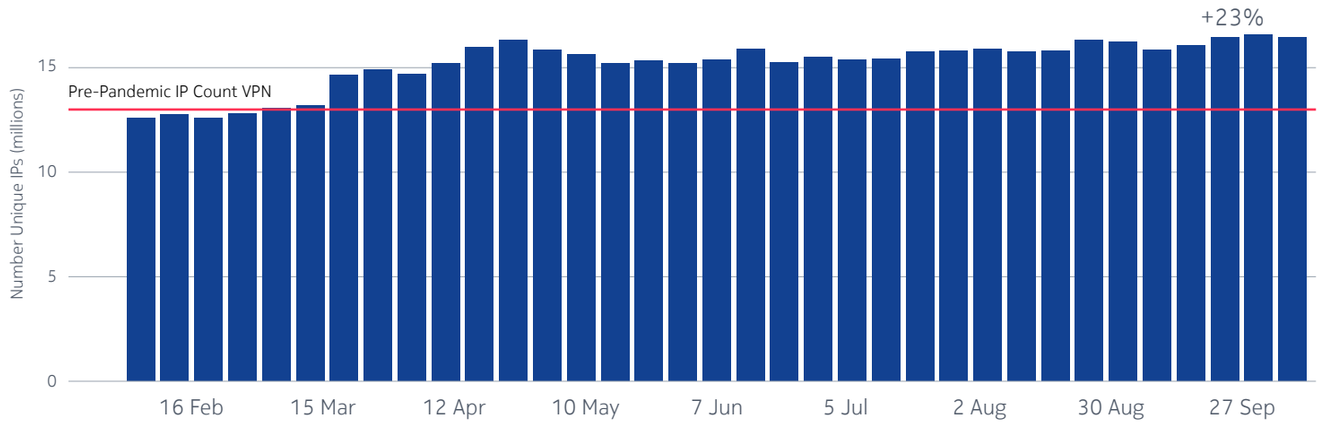


Figure 36. Increase in number of VPN endpoints between February and September 2020 – data aggregated from several US service providers

Service providers respond with service plan upgrades and removed data caps

As videoconferencing took off, service providers struggled to manage the bandwidth needs of consumers making unprecedented use of videoconferencing services from their homes.

Most residential networks weren't designed for heavy upstream use – in some cases due to the limitation of technology, and in others due to a design assumption that downstream consumption of data would be at least an order of magnitude higher than upstream data generation and sharing.

Deepfield data from some European networks showed a 35–40 percent increase in weekday upstream wireline traffic, potentially reaching capacity limits for some connections. Operators responded where they could, either by rebalancing upstream and downstream capacity where remote configuration was possible, or by upgrading customer service plans.

Many service providers introduced other measures to help their customers, such as removing data caps for bandwidth-metered connections. Despite this, many consumers struggled to achieve high-quality video connectivity through their home connections, particularly in remote and rural communities where high-speed broadband remains challenging.

VPN traffic continues to rise in September

VPN traffic levels remained elevated from May to August, despite seasonal variations due to the summer vacation period. The beginning of September saw additional growth as people continued to work remotely; a trend that warrants further continuous monitoring as September marks the beginning of the new business cycles in many countries.

We also noticed a significant increase in the number of VPN endpoints between February and September. In the US, the number of VPN endpoints increased by 23 percent, as shown in Figure 36.

Figure 37. Downstream and upstream videoconferencing traffic, February-September 2020 (one EU network). Note the different scales of measurement, with April and September traffic several orders of magnitude above February

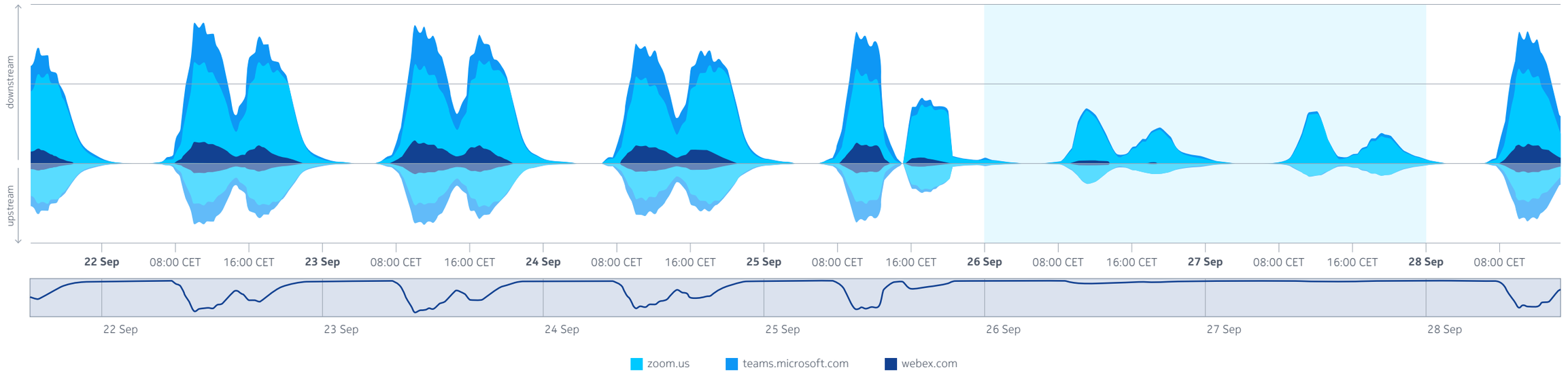


Figure 38. Continued heavy use of Zoom for conferencing on weekends - data from one EU-based service provider

Videoconferencing stays high into September, Microsoft Teams shows strong growth

Videoconferencing traffic levels remained high in September. Data from one EU network shows continued elevated levels of downstream and upstream videoconferencing traffic in September, as well as striking growth of Microsoft Teams between March and September, noted as a proportion of that traffic. It's interesting to note that the use of Zoom continues at weekends.

Key takeaways for service providers: Videoconferencing

Although many consumers were unable to take full advantage of cloud collaboration and videoconferencing due to limited-bandwidth connections, overall delivery of teleworking-related services held up, thanks to the combination of cloud, CDNs, peering, and a robust IP and optical internet backbone.

By understanding demand and consumption patterns for videoconferencing from residential addresses, service providers may uncover opportunities to market higher-bandwidth connections and videoconferencing-inclusive service plans to consumers who are likely to spend more time working from home. Some operators – such as BT in the UK with its Dedicated Connection service – started to offer a second home broadband connection as a more reliable option for remote working.

As 5G rolls out, it will be interesting to see how the promise of 5G FWA will help overcome these access issues. With its high bandwidth and low latency, and combined with fiber-based access, 5G may enable new types of services where low latency will be as crucial as high bandwidth – not just for corporate services but also for new and growing applications such as cloud-based gaming.

The world at play

Gaming

Even before COVID-19, online gaming had become a significant contributor to total internet traffic. More games are now played online in real time, facilitated by cloud-based platforms. Gamers had started to take advantage of low-latency connections enabled by FTTH, 4G, and early 5G deployments.

With these dynamics in mind, the initial months of the COVID-19 pandemic provided some interesting insights into how online gaming traffic and related consumption may evolve.

Lockdowns prompt an immediate increase in online gaming

Unsurprisingly, traffic data shows that locked-down gamers turned to their consoles for consolation. One US-based Tier-1 service provider network saw online gaming traffic almost double (from 4.26 percent of total traffic in the week of 3–10 February to 8.16 percent in the week of 9–16 June) in a period during which their overall network traffic grew by 30 percent.

In other words, online gaming grew three times faster than the rest of the traffic, and, in absolute terms, gaming-related traffic on their network increased by 142 percent over the period.

One US-based service provider saw gaming traffic almost double from 4.26 percent to 8.16 percent of their total traffic.

A broader view of internet traffic and service provider networks bears this out. Data aggregated from multiple providers shows a big upsurge in traffic from major gaming content providers, with volumes more than doubling on the 14–15 March weekend from the previous weekend.

One US-based service provider saw gaming traffic almost double from 4.26 percent to 8.16 percent of total traffic.

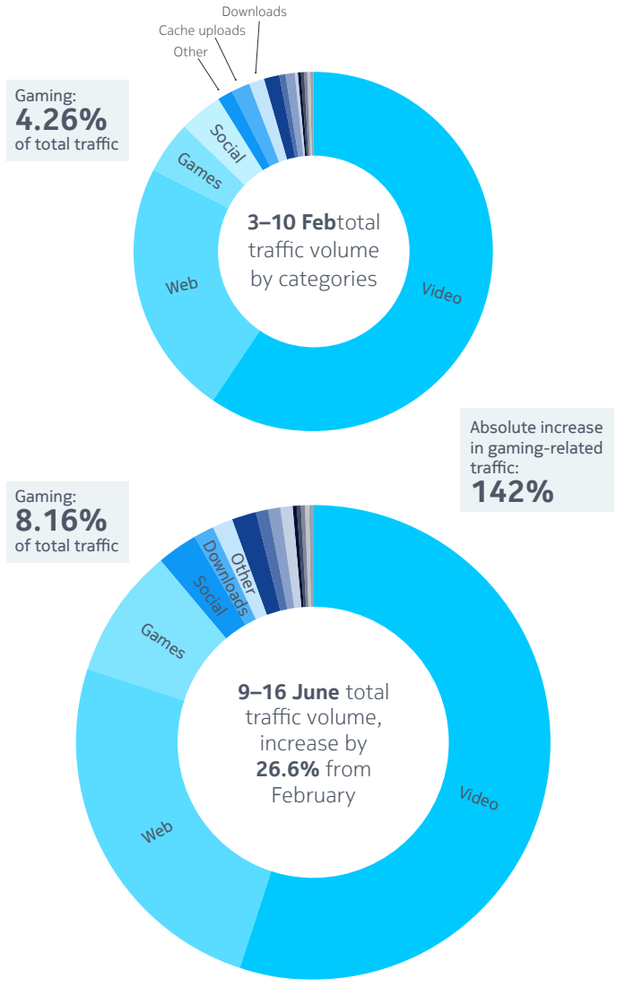


Figure 39. Comparison of gaming traffic between February and June 2020 – data from one US service provider

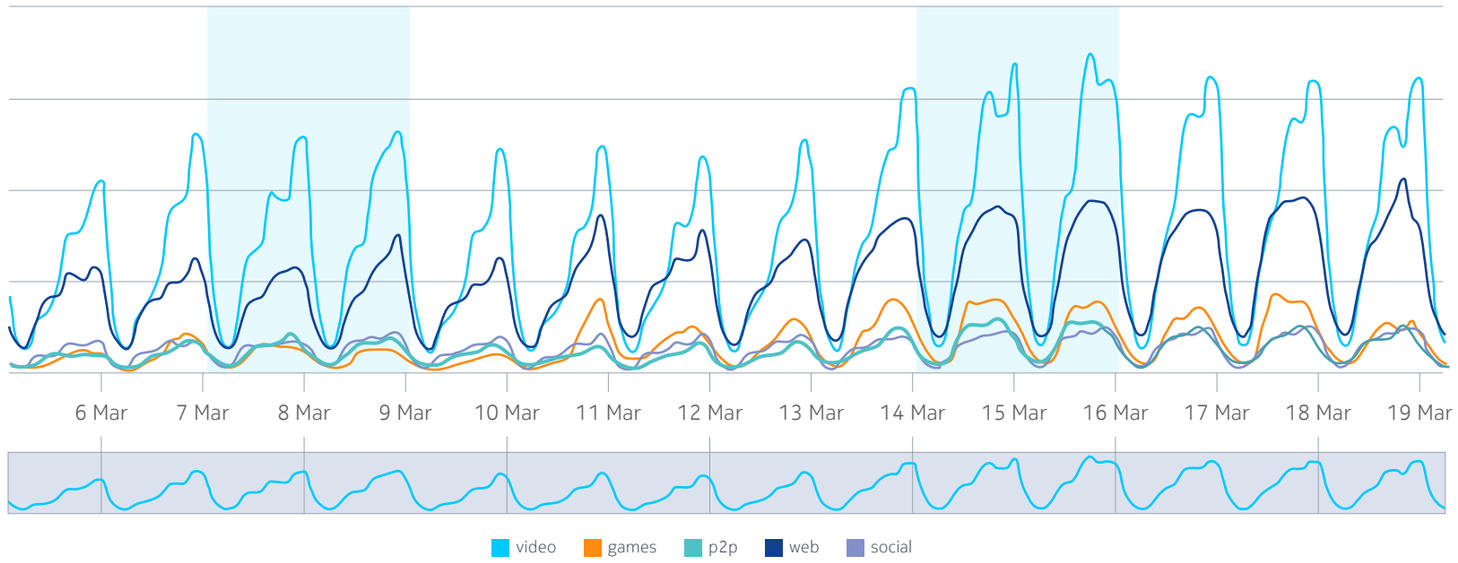


Figure 40. Traffic increase across different traffic categories – data aggregated from multiple service providers in the EU

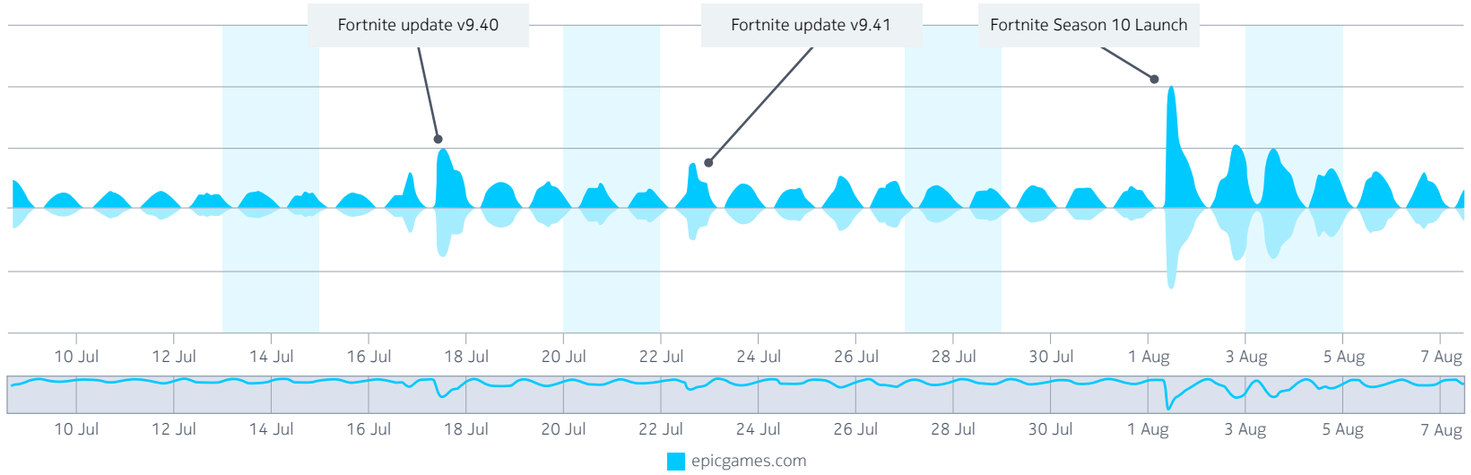


Figure 41. Traffic spikes arising from Fortnite updates and releases in August 2019 – one European provider

Two different traffic types: game updates and online gaming

Gaming differs from other traffic types, firstly because it doesn't follow typical diurnal traffic patterns, and also because it's split into two distinct traffic types: game updates and online game play.

Gaming updates have been a network traffic phenomenon for the past few years. When a new game is released online, CDNs play a key role in delivering it to as many users as possible as quickly as possible. Game releases and software updates tend to cause significant traffic spikes. Some operators warned about the impact of those way back in 2018, and that impact has been more significant in 2020.

> "When Fornite (sic) pushed out an update recently, the network went insane for two hours."
> –one European service provider, 2018[5]

The most significant game release of the early COVID-19 period was Blizzard's Call of Duty: Warzone on 10 March. Deepfield data from multiple providers shows the resulting traffic spikes on Thursday and Friday of Week 13.

Meanwhile, online game playing represents processing-intensive traffic that demands high bandwidth connectivity. The introduction of COVID-19 lockdowns tested service providers' ability to facilitate high-bandwidth, low-latency online gaming. The week of 9 March, for example, saw a 170 percent increase in traffic from playstation.com and a 75–150 percent increase in traffic from xbox.com.

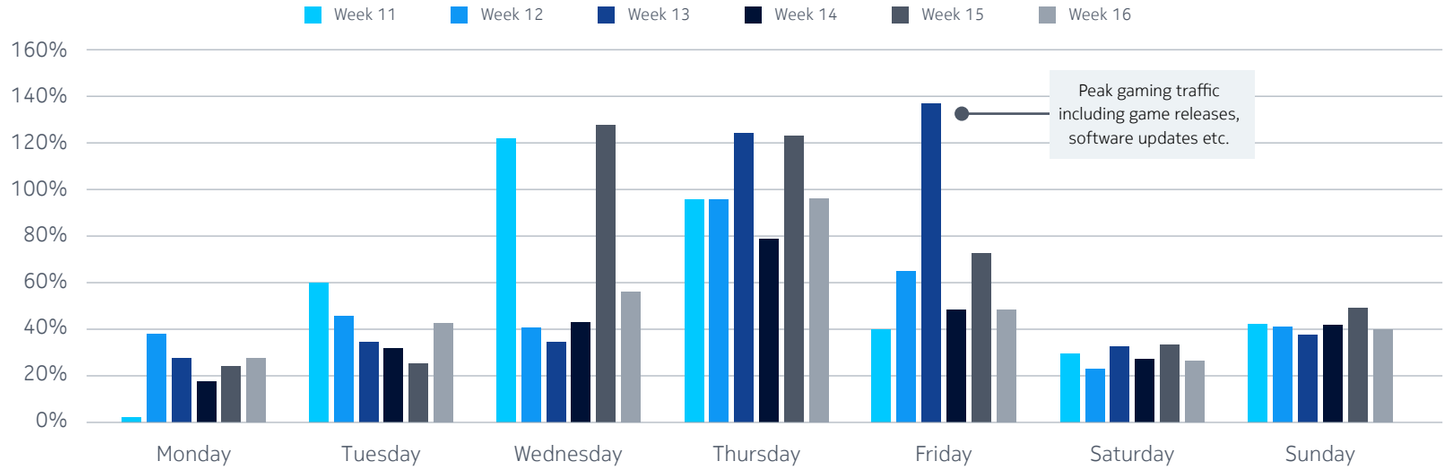


Figure 42. Week-by-week gaming traffic in March and April 2020 – multiple European providers; Spikes in week 13 are likely related to the release of Call of Duty: Warzone

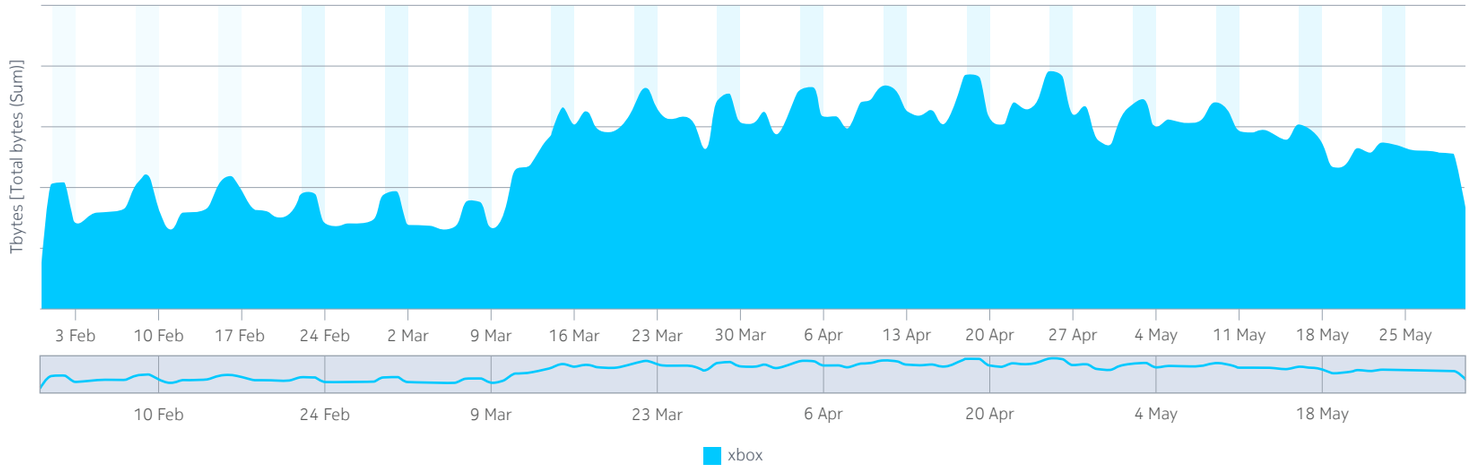


Figure 43. Example of increase in gaming traffic: Xbox (in total bytes per day): 75–150 percent increase since February

5. https://www.lightreading.com/automation/bts-mcrae-on-operator-led-innovation-telemetry-and-curiosity/a/d-id/746972

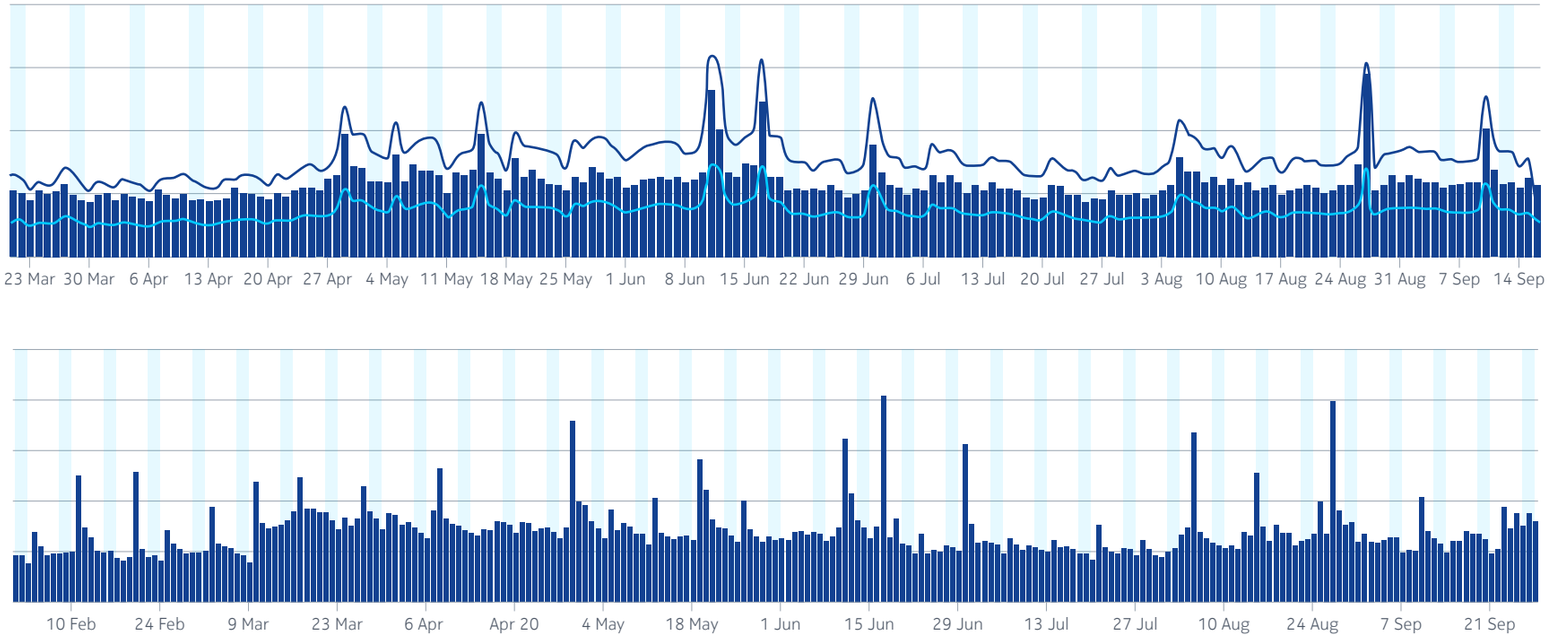


Figure 44. Gaming traffic, March-September 2020 – two European networks

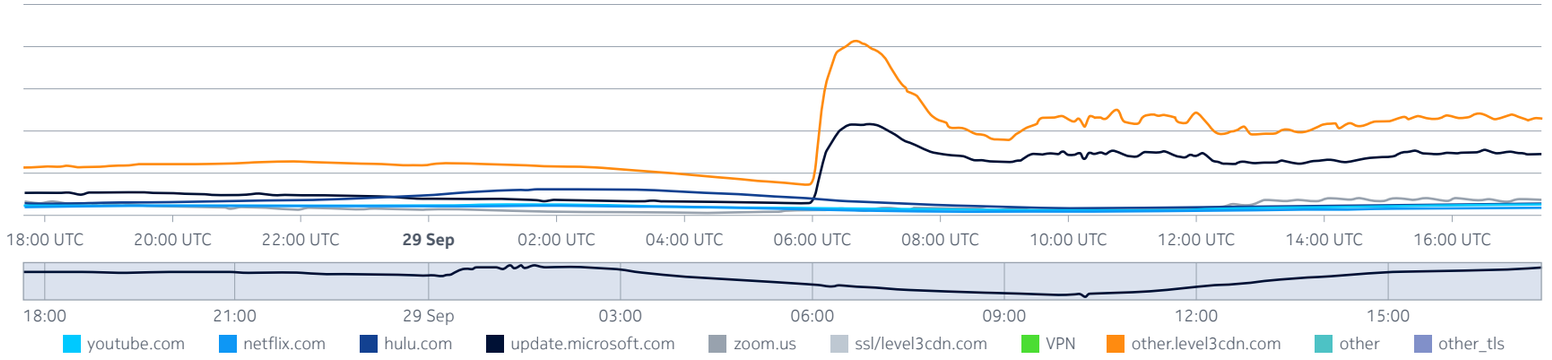


Figure 45. Traffic patterns relating to the release of Call of Duty: Season 6 – one US network

While some of this traffic may be due to the launch of Call of Duty: Warzone, which was available for both PlayStation and Xbox, traffic levels for both providers remained elevated throughout the lockdown period, indicating that gamers were spending more time playing overall.

The situation in September 2020

More recent September data shows gaming continuing to make a strong contribution to overall traffic, in some networks getting close to representing 10 percent of it. Data from two European networks shows an overall increase in online gaming through the year, with peaks indicating the release of new gaming downloads including Fall Guys and Among Us.

It's a similar picture in the US, where events such as the September 29 release of Call of Duty: Season 6 continue to significantly impact overall network traffic.

Key takeaways for service providers: Gaming

Online gaming was increasing in popularity even without the COVID-19 pandemic, and the promise of even higher bandwidth and lower latency enabled by edge cloud and 5G are likely to drive further adoption.

With online gaming growing at a higher rate than the overall network traffic, service providers have both a challenge and an opportunity. The challenge is to optimize their services to accommodate the growth, and the opportunity is to develop tailored offers, plans, and services targeted at gamers. Both require deep insight into how gaming traffic is delivered to their subscribers.

As with video streaming, it's critical to understand the entire online gaming service delivery chain and to be able to attribute traffic from CDNs back to the original gaming provider. By understanding these delivery paths, service providers can adjust and optimize their network to ensure the best possible performance.

Additionally, most online gaming companies specialize in select audience profiles. Understanding consumption patterns for online gaming may also help service providers better understand their customers, and customize and tailor their service packages for different audiences.

With more games requiring ultra-low latency to be truly enjoyable, consumption patterns can also provide insight into where additional network investments may be required, including expanding their 5G services to target online gamers.

How Deepfield can help

Deepfield can provide customized, real-time and chronological reports, and visualize all important aspects of the service delivery chain. In this example, online gaming traffic is mapped across five data realms: from the originating domains, across CDNs, transit and peering layers, all the way to the service point of presence (PoP) to which subscribers are connected.

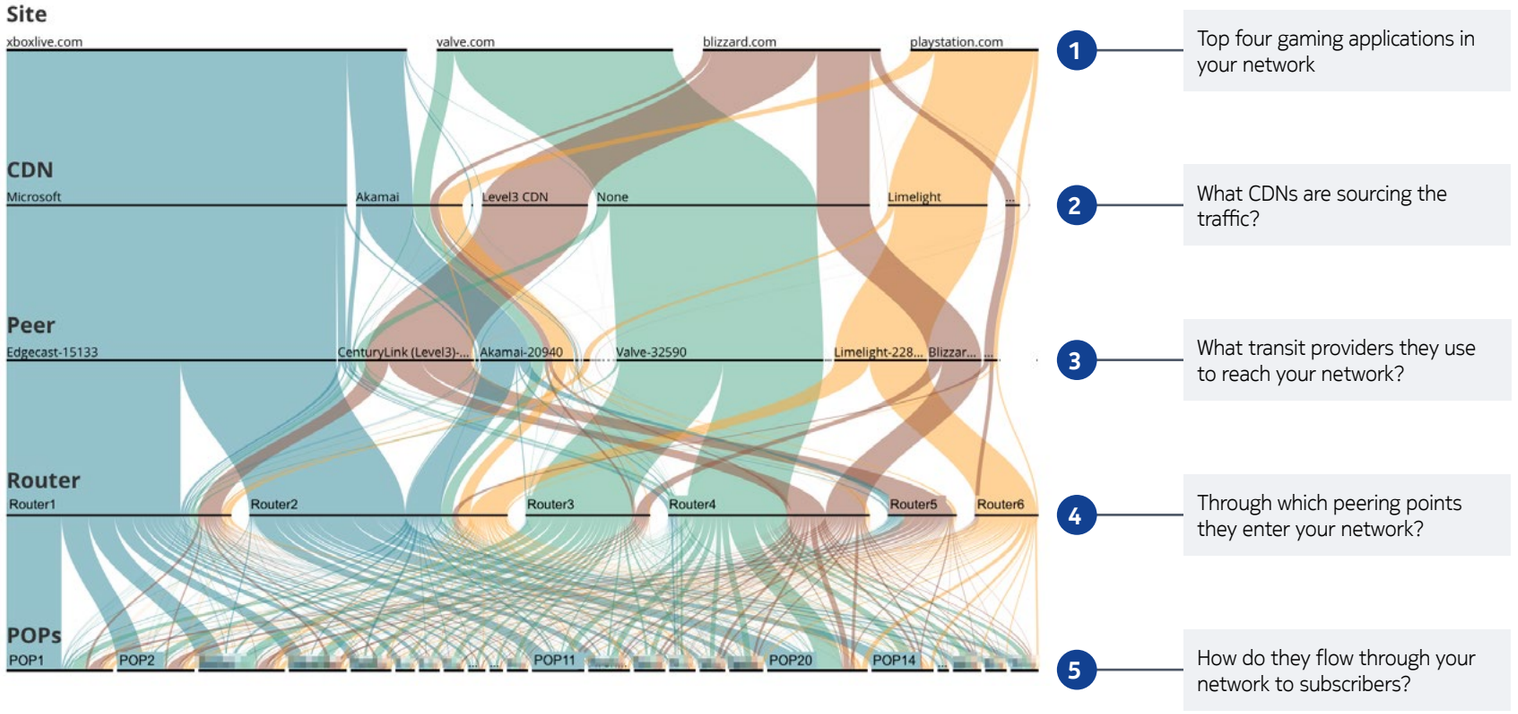


Figure 46. Detailed insight from Deepfield allows service providers to closely monitor online gaming traffic and trends

The world at risk

Security

Whenever online behavior changes, the threat landscape changes too. Deepfield data shows that the substantial behavioral shifts brought about by the pandemic were reflected in shifting patterns of DDoS attacks across networks globally.

DDoS traffic is malicious traffic aimed at rendering websites or online services inoperable. Attackers use many different techniques for achieving this goal, but the result is the same. Network infrastructure and online services are seriously affected – slowed down or out of service – and users are left without access to internet services, applications, or content.

Increase in DDoS attacks in the first weeks of lockdown

One of the first noticeable trends as the pandemic took hold was a steady increase in the overall volume of DDoS traffic. Aggregated data from five large service providers showed that by April, DDoS traffic exceeded pre-pandemic levels by 40 percent.

DDoS traffic (in terabytes per day) – aggregated for five major providers

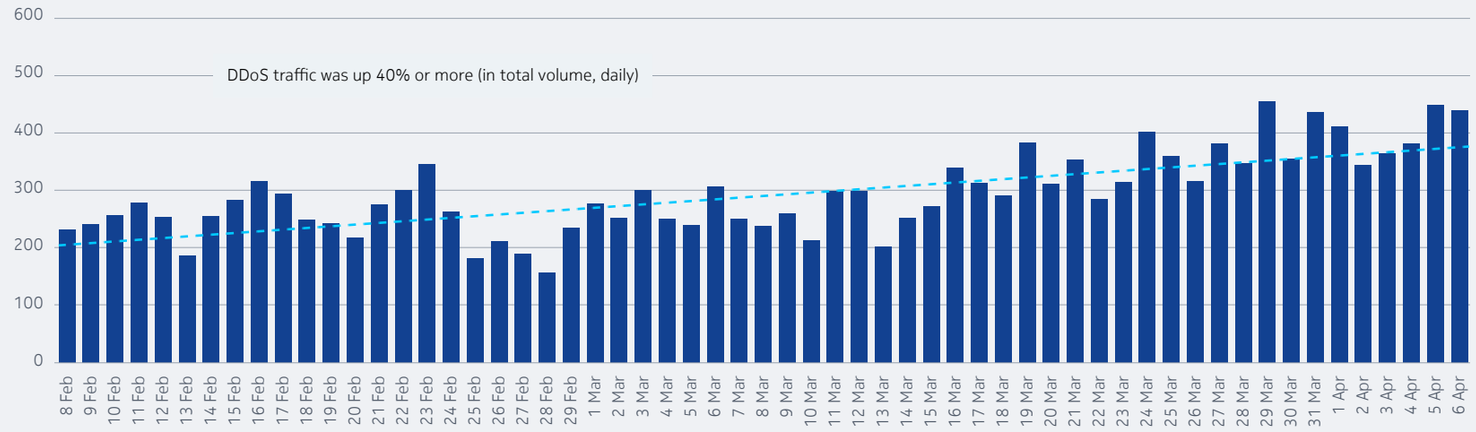


Figure 47. Distributed Denial of Service (DDoS) traffic in terabytes per day – data aggregated for five major US service providers

We attribute this increase to two main factors: an increase in gaming activity and an increase in abuse of NA and EU DDoS amplifiers. Let's look at each of these in turn.

DDoS traffic correlated with growth in gaming

The increase in online gaming is likely one reason for the increase in DDoS attacks we saw during the lockdown period.

Online gaming and gambling have long been accompanied by DDoS traffic. These gaming-related DDoS attacks are typically targeted at individual IP addresses and last only for a few minutes. This pattern represents gamers attempting to 'boot' rivals out of a game for just enough time to allow them to win a game round.

Denying opponents access to the service or 'booting your adversaries' has grown to the extent that there are many 'commercial' websites that offer DDoS services for hire and many more on the darknet where DDoS toolkits can be found and downloaded.

For about US$30 per month (mostly in Bitcoin), a malicious player can get unlimited 5-minute DDoS attacks aimed at single victim IPs. Most of these usually employ the technique of simple amplification using pre-defined lists of amplifiers.

As we saw in the previous section, gaming traffic increased significantly during lockdown; in some cases doubling in its overall volume. The 40 percent increase in DDoS traffic in the same period partly relates to gaming and gaming-related DDoS attacks. Short-lived gaming-related attacks on single IP addresses can be hard to identify with standard DDoS identification and prevention software, meaning service providers need to find new ways to identify and neutralize DDoS traffic.

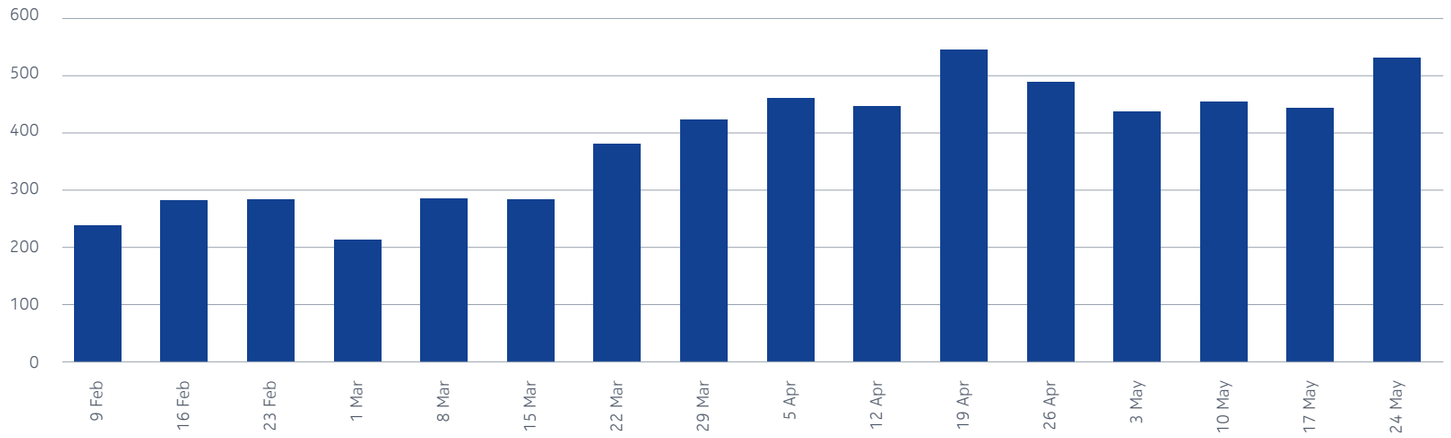


Figure 48. Aggregate Distributed Denial of Service (DDoS) traffic in terabytes per week - data aggregated across several US service providers

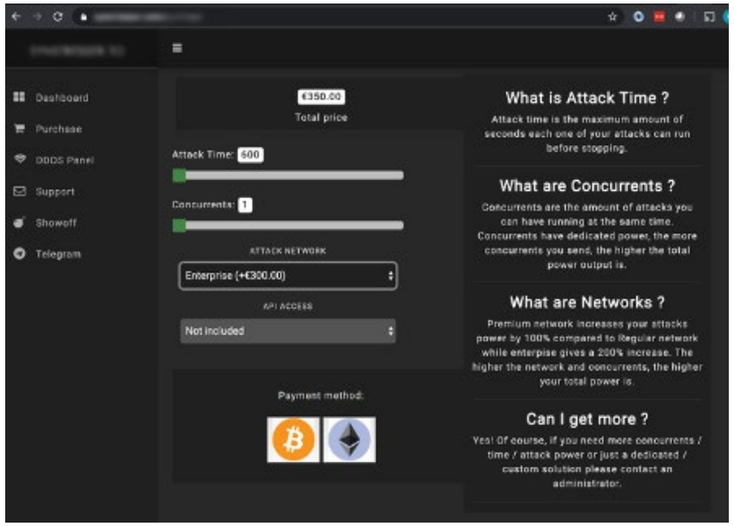


Figure 49. Examples of commercial websites offering DDoS service for hire

Increase in abuse of NA and EU DDoS amplifiers

In addition to gaming-related attacks, DDoS growth was partly driven by increased abuse of North American and Europe-based amplifiers/reflectors. A DDoS amplifier is any server that can be used to reflect and amplify a spoofed request, sending an amplified volume of traffic to the victim's IP address.

Historically, almost all DDoS traffic in the US was inbound from other regions. However, during the pandemic, we observed a significant increase in outbound DDoS traffic–originating from the US. This suggests that attackers used US-based enterprise and IoT hosts (IP addresses) as reflectors and amplifiers to create a significant level of attacks destined to hosts located globally.

Catching these types of attacks requires the ability to monitor, track, and correlate massive volumes of data that may contain seemingly unrelated traffic, but which can be a result of a sophisticated or an orchestrated DDoS attack, sometimes using an IoT botnet.

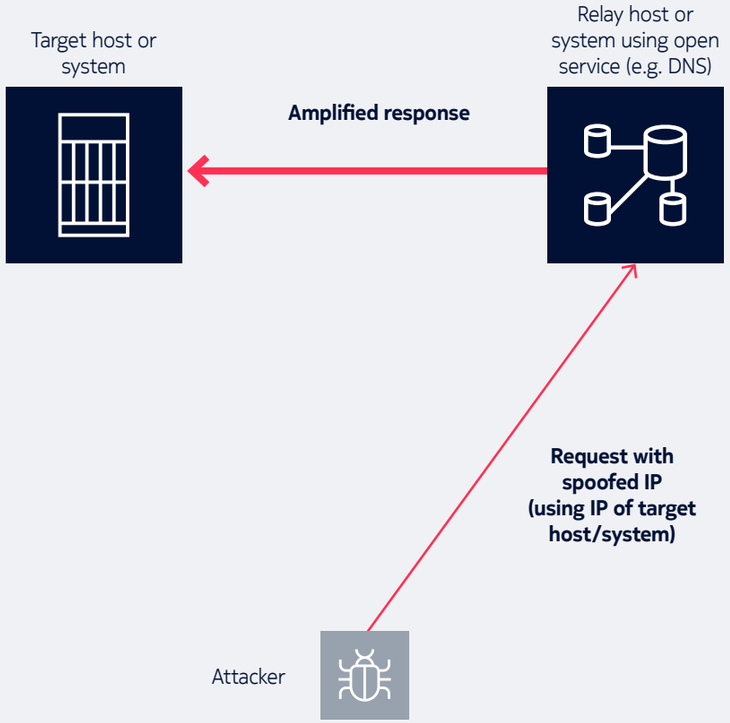


Figure 50. A DDoS amplifier is a server used to send an amplified volume of traffic to the victim's IP address

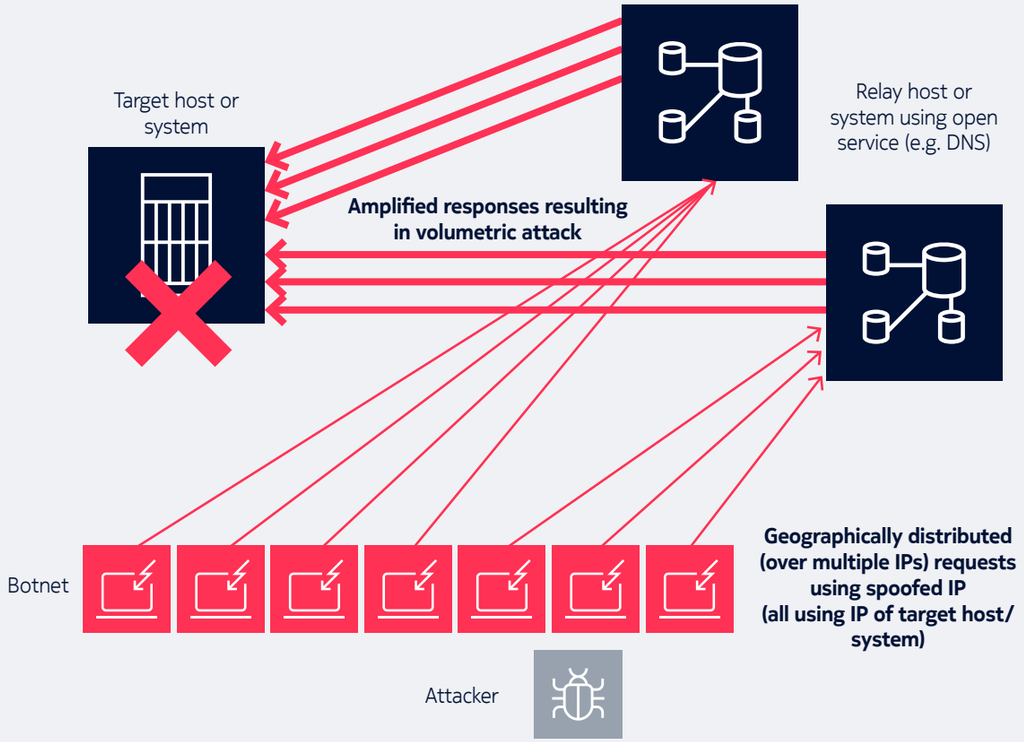


Figure 51. Reflection/amplification DDoS attack using spoofed, geographically distributed requests

Key takeaways for service providers: Security

DDoS attacks are a constant threat for service providers – increasing congestion on the network, and creating downtime and outages that impact the customer experience.

Increases in gaming and the proliferation of IoT-connected devices mean that service providers should expect to see more DDoS attacks, and from more sources. When the world is more reliant than ever on our networks, extra vigilance is required.

Traditional methods of detecting and blocking attacks may no longer be sufficient. Instead, a holistic view of network traffic in real time will be necessary to understand shifting patterns of DDoS traffic, tackle its sources, and mitigate its impact.

Conclusion

Five lessons from 2020 for service providers

The experiences of 2020 were unlike any other year in internet history. Never has so much demand been put on the networks so suddenly and so unpredictably.

For service providers, the events of 2020 have delivered some key lessons that can be used to plan future capacity, and develop and deliver value-added services to subscribers.

Key takeaways

#1 "[Service provider] networks were made for this"*

Despite seeing the equivalent of a year's traffic growth in just a few days, networks were able to take the strain – a testament to the foresight and engineering expertise of both communications service providers and cloud services providers.

While the networks held up during the biggest spikes in demand, data from September 2020 indicates that traffic levels remain elevated even as lockdowns are eased. The big question now for service providers is how much capacity to engineer into the networks now for future eventualities – or how to get the required headroom capacity when needed.

#2 Internet-based content delivery chains are evolving

Demand for streaming video, low-latency cloud gaming and videoconferencing, and fast access to cloud applications and services all placed unprecedented pressure on internet-based content delivery paths. Just as we saw content delivery networks (CDNs) grow in the past decade, we expect the same to happen with edge/far edge cloud in the next decade, bringing content (storage and compute) closer to end-users.

Service providers have an opportunity to develop win-win partnerships with internet applications, content and services providers, and with the content delivery networks (CDNs) that host and deliver their content. To capitalize on this opportunity, service providers must have a full visibility of the internet service delivery chain, not just of their own network.

#3 Residential broadband networks have become critical infrastructure

The COVID-19 pandemic events highlighted the role of our residential broadband connectivity as vital for society. Thanks to service providers' and cloud operators' agility and immediate actions, people in lockdown could use their network connections to work, play, socialize, get help, and provide help to others.

The challenge for service providers is to find ways to improve overall network resilience and offer tailored work/play/connect packages. They must also address dynamically shifting consumer needs – ranging from uninterrupted access to critical communications to soaring demand for high-bandwidth, low-latency content and services. Accelerating the rollout of new technologies – such as 5G and next-gen FTTH – that will improve access and connectivity in rural, remote, and underserved areas would go a long way toward bridging the digital gap in many societies.

#4 Deep insight into network traffic is essential

This analysis of internet traffic in 2020 provides significant insights into the changing patterns of consumption and demand in service provider networks and cloud networks. While the COVID-19 era may prove in many ways to have been exceptional, the likelihood is that it has only accelerated trends in content consumption, production, and delivery that were going to happen anyway. Recent data from September 2020 supports this notion.

By understanding network traffic trends in detail and in real time, service providers can gain more in-depth insight into evolving subscriber needs and preferences. That will allow them to develop partnerships and offers that elevate their role to providers of valuable, differentiated services.

#5 Security has never been more important

In normal circumstances, DDoS attacks can threaten a business's livelihood and reputation. In situations where broadband connectivity is an essential service, protecting network infrastructure and services becomes critical. In particular, the rise of online gaming has led to more and shorter DDoS attacks, often targeted at a single host, creating challenges for service providers in detecting and protecting against attacks.

The need for robust, 360-degree network security DDoS protection is critical. Service providers will need to find better and more cost-effective ways to detect and minimize new forms of DDoS attacks that may go undetected or unmitigated by legacy security tools and approaches.

* Dr Craig Labovitz, CTO, Nokia Deepfield, in ITU/UN webinar on broadband connectivity and digital cooperation in the time of COVID-19, 22 April 2020.

https://www.youtube.com/watch?v=ti7G1dDW7HQ&feature=youtu.be&t=2285

Gain detailed insight into network traffic with Nokia Deepfield

This report's data was gathered using our Nokia Deepfield portfolio of applications, which use big data analytics to monitor, analyze, and understand traffic on service providers' networks.

How Deepfield works

The Deepfield platform ingests data from many different sources within the network, starting with essential IP flow-related data sets (any x-flow type of data), BGP and SNMP. These data sets can be further enhanced with DNS information (from DNSflow) along with other router-, network, and telemetry-related data sets such as RADIUS/AAA, IPFIX and gRPC.

The Deepfield platform can also ingest custom data sets from other network and operational domains, including network management, software-defined networking (SDN) control, operations support systems/business support systems (OSSs/BSSs), customer care, support, and billing[5].

All these data sets are processed and correlated to provide a real-time, multidimensional, un-siloed view of the network, services, and IP flows.

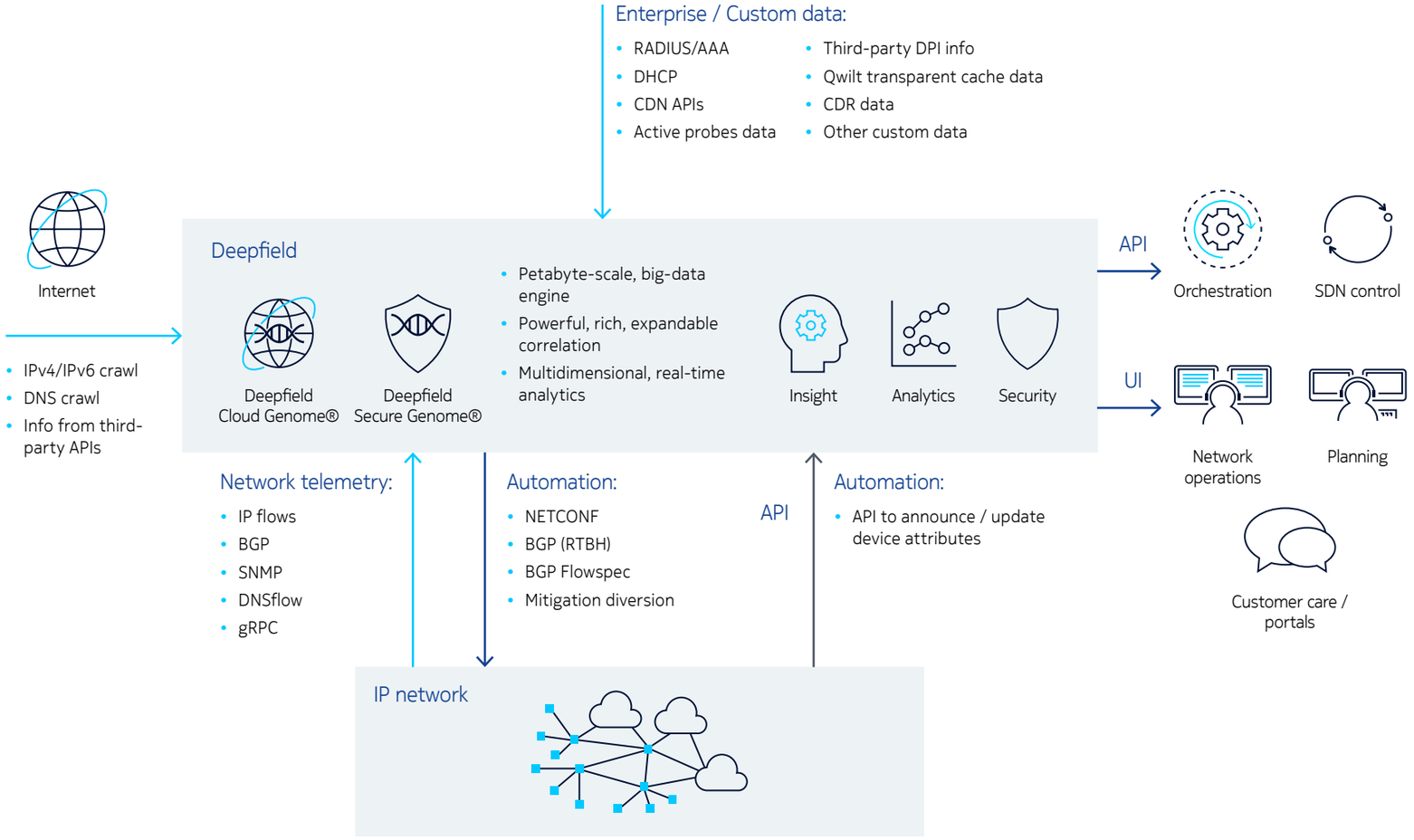
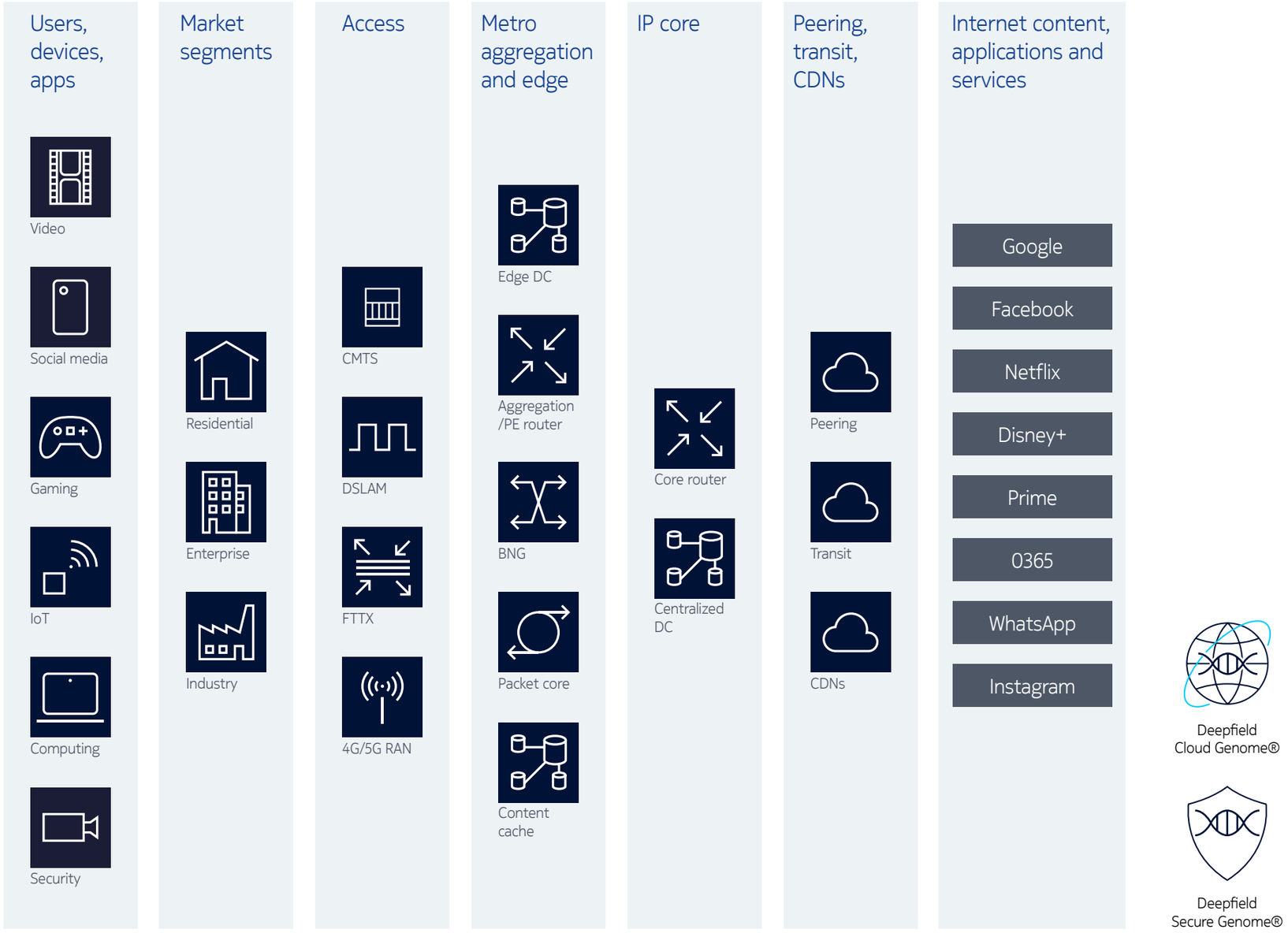


Figure 52. Nokia Deepfield ingests network data from many sources to provide real-time traffic insights

5. May require custom development. Please discuss your requirements with your Nokia sales representative.



Nokia Deepfield Genome

Augment network traffic data with insights into the service delivery chain

A unique aspect of our Deepfield solution is its ability to provide a detailed, global, and real-time view of the internet service delivery chain and security. We do this through our proprietary data feeds, Deepfield Cloud Genome® and Deepfield Secure Genome®, collectively referred to as Deepfield Genome.

Deepfield Genome is a Nokia proprietary, cloud-based data feed that continuously probes and tracks billions of internet IPv4 and IPv6 addresses. Using Genome, we can map, categorize, and track internet service and security-related information for billions of IP hosts and traffic flows. Genome maps IP addresses to more meaningful DNS names and employs advanced ML rules to tag the addresses into service and security-related types and categories.

Deepfield Genome is based on Nokia Deepfield patented technology. It's constructed by cloud-based agents run by Deepfield, which continuously probe and map the internet, scanning hundreds of millions of IP addresses daily, and further analyzing, identifying, and categorizing data.

The resulting Cloud Genome and Secure Genome data feeds are available to Deepfield customers as real-time updates, providing a holistic service and security-related perspective of all internet applications and content.

Combine data sets and create visualizations for unprecedented insights

Deepfield equips service providers with unprecedented levels of visibility and insight into what's happening in their network, without probes or deep packet inspection (DPI) technology.

By overlapping the information from the network with the Genome data sets, the Deepfield solution allows service providers to create correlations between data sets and across many data dimensions, which otherwise are hard or impossible to be made. These correlations provide unique and deep insight into the network, peering and transit services, and how content is consumed.

A single source of traffic intelligence

Deepfield makes it easy to visualize the internet service delivery chain – from cloud providers to end-users and subscribers, delivering insights that can inform network and service planning, modeling, and forecasting. In particular, Deepfield can provide meaningful insights that help with:

Accurate network planning and forecasting: with visibility into which services are being used at which times of day, and how much bandwidth they are consuming.

Quality of Experience (QoE) monitoring: with detailed insights into the performance of individual applications and content services by network area and user profile.

Detecting network anomalies: with configurable alerts for when QoE or other KPIs exceed a certain threshold.

Business development: with insights into how content, application, and services are consumed at the individual subscriber level – to inform service plans, marketing offers, and value-added partnerships.

DDoS protection: with granular insight into where DDoS attacks are originating and their impact on network traffic, and intelligent auto-mitigation against attacks of any scale.

To learn more, visit
https://www.nokia.com/networks/solutions/deepfield/

Nokia OYJ
Karakaari 7
02610 Espoo
Finland

Document code: CID 210130

About Nokia

We create the technology to connect the world. Only Nokia offers a comprehensive portfolio of network equipment, software, services, and licensing opportunities across the globe. With our commitment to innovation, driven by the award-winning Nokia Bell Labs, we are a leader in the development and deployment of 5G networks.

Our communications service provider customers support more than 6.4 billion subscriptions with our radio networks, and our enterprise customers have deployed over 1,300 industrial networks worldwide. Adhering to the highest ethical standards, we transform how people live, work, and communicate. For our latest updates, please visit us online www.nokia.com and follow us on Twitter @nokia.