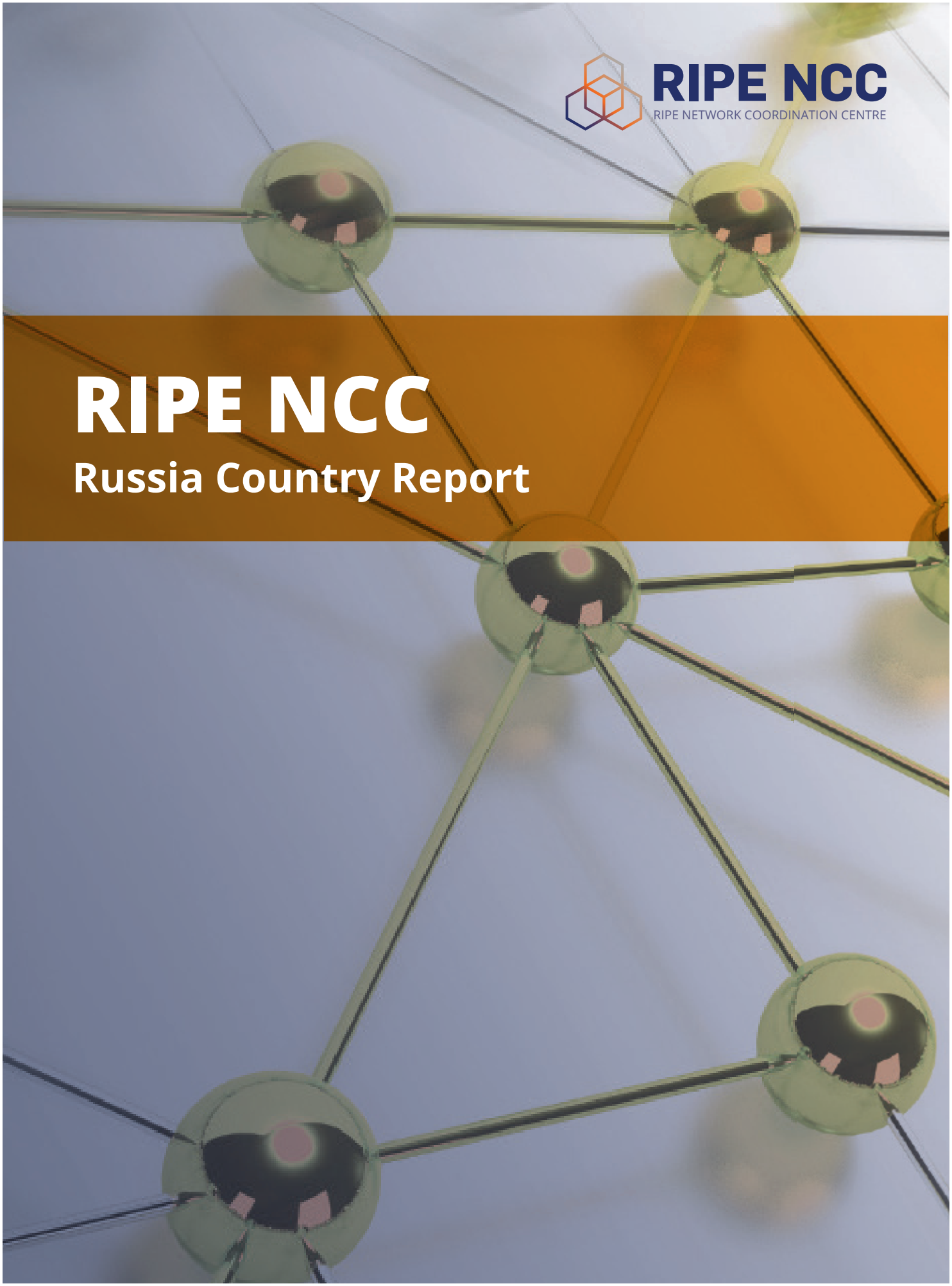


RIPE NCC
RIPE NETWORK COORDINATION CENTRE

RIPE NCC
Russia Country Report

Date: April 2019

Introduction

The Internet is a global network of networks, yet every country's relationship to it is different. Russia's place in the Internet landscape has been shaped by its own unique history and development in ways that are often still visible today, and which may continue to influence its development into the future.

This report provides an outlook on the current state of Internet development in Russia. It offers an analysis of growth trends and Internet routing in the country, as well as an evaluation of Russia's efficiency in accessing the global Domain Name System (DNS), based on what we can observe from the RIPE NCC's measurement tools and infrastructure.

We present these findings in conjunction with the RIPE NCC Day in Moscow in the hopes that they will inform discussion, provide technical insight, and facilitate the exchange of information regarding Internet-related developments in Russia. This is the second such country report that the RIPE NCC has produced as part of a new, ongoing effort to support Internet development throughout our service region by making our data and insights available to local technical communities and decision makers alike.

Growing Internet Use in Russia

After a decade of intensive growth, the past five years have seen a slower yet steady rise in the number of Internet users in Russia. Internet penetration increased from 67% to 75% between 2014 and 2019, suggesting that there are more than 71.5 million Internet users in Russia today.

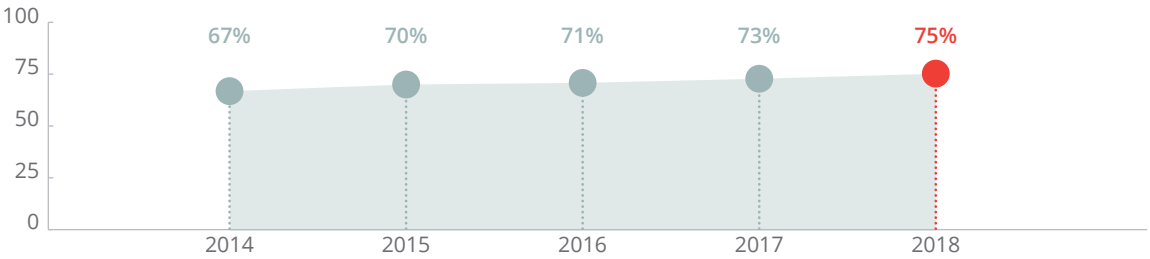


Figure 1: Growth of the Internet between 2014 and 2019. Source: Omnibus GfK-Rus.

While growth has recently levelled out, particularly as certain sectors have become saturated, Internet penetration is likely to keep rising in the coming years. This will continue to drive the need for Internet number resources and the further development of existing Internet infrastructure to accommodate new users and devices coming online.

As millions of new devices connect to the Internet, many of them will require an IP address - a unique identifier that allows any device to connect to other devices on the Internet. Globally,

there are five Regional Internet Registries (RIRs) that are responsible for the allocation and administration of IP addresses to Internet Service Providers and other network operators. The RIPE NCC fulfills this role for Europe, the Middle East and parts of Central Asia.

Figure 2: The five RIRs and their respective service regions.

IPv4 Exhaustion

Background

Much of the existing Internet is built using IPv4 addresses, a standard developed early in the Internet's history that allows for around four billion unique addresses. It was not anticipated that there would be a need for more than this. However, the Internet has since grown beyond what anyone could have imagined and available IPv4 addresses are now running out. A next generation IP address type, called IPv6, was developed in the 1990s to address this need. But network operators have been slow to make the switch because there was, until recently, still plenty of IPv4 address space available.

IPv4 exhaustion is now in its final phases. Of the five RIRs, three have only small amounts of IPv4 address space left to allocate (RIPE NCC, LACNIC, APNIC) and one has none (ARIN). In fact, the RIPE NCC ran out of "new" address space nearly a year ago, and has since been allocating address blocks that were previously in use and have been returned to us.

RIPE

The RIPE community is an open forum in which anyone interested can participate and which develops policy around the management of Internet number resources for the RIPE NCC region, which the RIPE NCC then implements.

IPv4 exhaustion presents a defining challenge for the ongoing growth of the Internet. Anticipating this situation, the RIPE community developed a policy in 2010 to set aside a final block of IPv4 address space for new entrants. The intention was to allow new companies requiring address space to obtain a small block of IPv4 addresses to connect their IPv6 networks with the IPv4 Internet. Based on current demand and allocation policy, we expect the RIPE NCC will have IPv4 address space to distribute for approximately another 12 months.

The Effects of IPv4 Exhaustion

This approach of preserving IPv4 for new entrants has produced some unexpected developments in the community of network operators. A significant number of companies have opened multiple accounts with the RIPE NCC (each of which is called a Local Internet Registry, or LIR) to access more IPv4 addresses, occasionally resorting to dishonest or fraudulent means to do so. The worst of this activity has been addressed through a combination of policies created by the RIPE community, changes to RIPE NCC procedures, and greater investment in due diligence and verification of supporting documents when processing new applications. Still, these issues illustrate how seriously network operators view IPv4 exhaustion and the value they place on IPv4 addresses.

At the same time, many network operators find that they are able to get more out of the limited addresses available to them through the use of address-sharing technologies, which allow multiple devices to connect to the Internet via a single IP address. This is complemented by a substantial IPv4 transfer market that has emerged in recent years, involving financial transactions between individuals or companies for the use of IPv4 address space. However, the consensus is that these measures can only be short- to mid-term solutions. The inevitable conclusion is that, with several billion people still unconnected, the number of connected devices per person increasing, and the rapid growth of the Internet of Things, IPv6 deployment is needed to allow for the future growth of the Internet.

Russia's Internet Address Space

Organisations Receiving Internet Number Resources

In 1995, RosNIIROS, RADIO-MSU and RoSprint became the first Russian organisations to receive Internet number resources from the RIPE NCC. Since that time, we have seen phenomenal growth in the number of Local Internet Registries (LIRs) in Russia. Figure 3 illustrates the last five years of growth. For comparison, we've included the three countries with the largest number of LIRs in the RIPE NCC service region (Russia, the United Kingdom and Germany), along with two other countries (Poland and Turkey) that are comparable to Russia in terms of GDP per capita and/or Internet market size.

> **Local Internet Registries (LIRs)**
> **Any company or organisation that receives Internet address space from the RIPE NCC becomes an LIR. Most LIRs are Internet Service Providers or other organisations operating their own networks, such as governments, universities, banks, or large corporations.**

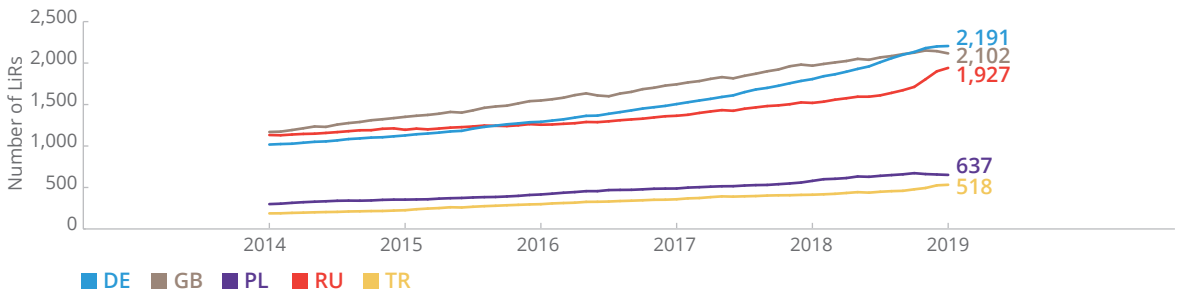


Figure 3: Growth in the number of LIR accounts registered in Russia and other selected countries from January 2014 to January 2019.

Highlights:

- As of 1 January 2019, a total of 1,927 LIRs are active in Russia, the third highest number of LIR accounts registered to any country in the RIPE NCC service region
- Over the past five years, there has been a 72% increase (from 1,118 LIRs) in the number of Russian LIRs
- While the rate of growth has been quite steady during this period (an average of about 8% per year), there was a sharp rise of 28% in 2018

Given the impending IPv4 exhaustion, it is likely that some of the recent LIR growth is speculative, driven by members that open multiple LIR accounts to obtain more IPv4 address space. We therefore expect to see a reduction in the number of LIR accounts in the coming years as these members no longer see the need to maintain multiple LIRs and consolidate the registration of their IP address holdings under a single LIR.

However, this anticipated drop in LIR growth is likely to be replicated across the RIPE NCC service region, and should not be taken to indicate slowing Internet growth. Indeed, the high number of new and long-term LIRs registered indicates a highly active Internet ecosystem in Russia.

IPv4 Resources

With more than 45.5 million IPv4 addresses, Russia holds the sixth largest number of any country in the RIPE NCC service region. Those with more address space, such as Germany and the UK, tend to have been early Internet adopters and as such, they obtained large blocks of address space prior to the introduction of the current Internet registry system and the establishment of the RIPE NCC (often referred to as "legacy" address space).

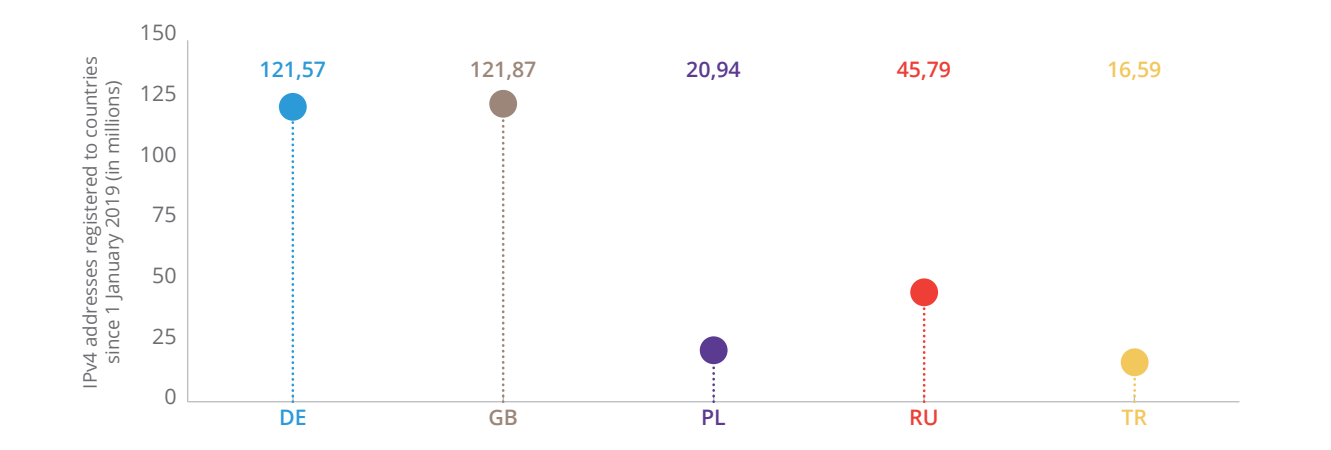


Figure 4: Number of IPv4 addresses registered to Russia and other countries as of 2019.

Despite the growth in the number of LIR accounts over the past five years, the amount of IPv4 address space in Russia has remained fairly steady during that time. In large part this is because Russian LIRs have been quite active in transferring their Internet number resources on the IPv4 transfer market, as explained in the section below.

IPv4 Address Transfers

With IPv4 exhaustion on the horizon, an IPv4 transfer market emerged in the ARIN, APNIC and RIPE NCC service regions several years ago. Policies developed by the respective communities now allow for the transfer of IP addresses between operators in these three service regions. This is particularly relevant as North America appears to have the most unused IPv4 addresses available for transfer - the large amounts of IPv4 space allocated to US organisations in the early days of the Internet and the fact that the US industry today is relatively advanced in IPv6 deployment may account for this.

Not all transfers involve a financial transaction. The RIPE community has asked the RIPE NCC to report on all resource transfers, whether they are the result of mergers or acquisitions, the movement of resources between subsidiaries and affiliates, or a market transfer.

Taking all of this into consideration and to improve the estimate of Russia's market size, we analysed the largest transactions and excluded those that occurred between related companies. With that correction, we see 5.5 million IPv4 addresses transferred between what the RIPE NCC sees as unrelated organisations in the past six years, 3.3 million of which stayed within Russia.

Figure 5: Number of IPv4 addresses transferred from countries to Russia (left) and from Russia to countries (right). The thick line in the middle represents the 3.3 million IPv4 addresses transferred between LIRs in Russia.

Setting all this in the wider context of global transfer flows, Russia is the third largest source of IPv4 transfers (after Romania and the US) and the second largest receiver of IPv4 transfers (after Iran and just ahead of Saudi Arabia and Germany). It is also striking that 66% of these resources were transferred between LIRs within Russia, which means they never left the country. This is indicative of Russia's low dependence on imports despite its high involvement in the transfer market.

Like Russia, countries such as Germany also see a large proportion of internal transfers. What is notable with Germany is that the country's high involvement in the IPv4 transfer market does not seem to conflict with a relatively high percentage of IPv6 adoption. This is mainly due to the fact that, although the efforts of larger access providers have driven Germany's IPv6 capability rates to approximately 40%, there is still a need for IPv4 among hosting providers looking to grow their businesses. With this in mind, it's interesting to consider what IPv6 adoption can tell us about the state of affairs in Russia.

IPv6: Necessary for Future Growth

Although IPv6 was released in 1998, it was not until early 2013 that Google saw the global percentage of users accessing its services over IPv6 pass the 1% threshold. Today, this figure stands at around 26%.

In one sense, the slow uptake of IPv6 by network operators can be viewed as completely rational behaviour; there was no real benefit in moving to IPv6 until enough networks had deployed it that a critical mass was reached. It took time before vendors started selling IPv6-capable network equipment, and many key services were not IPv6-enabled. Most network engineers were unfamiliar with IPv6 and required training to get up to speed with the new protocol. And for a long time after IPv6 was developed, there were still plenty of IPv4 addresses available.

This began to change when the RIRs started allocating address space from their final blocks of unused IPv4 addresses. To get around the growing scarcity of IPv4 addresses, network operators started sharing IPv4 addresses among multiple end users. However, it is increasingly clear that IPv6 deployment is the more cost-effective solution.

In the meantime, practically all network equipment sold today is IPv6-capable and many key services are now IPv6-enabled. And with the massive degree of concentration in terms of content and services that has taken place in recent years, ISPs around the world that switch on IPv6 typically report that as much as 70–75% of the traffic on their network immediately travels across IPv6, because the bulk of their users are connecting to services like Facebook, Google and YouTube – all of which are IPv6 enabled.

IPv6 Penetration in Russia

IPv6 is gradually gaining ground in Russia, although penetration is still significantly behind the worldwide average of 26%.

Approximately 74% of LIRs active in Russia have received IPv6 allocations from the RIPE NCC. However, many of these would have been allocated by default when receiving their final IPv4 allocations, and they may not be actively using their IPv6 resources.

IPv6 can be supported both by upstream service providers or by content delivery services (the largest being Cloudflare) which provide IPv6 support by default for their customers' IP addresses. We have therefore calculated these cases separately when looking at IPv6 penetration according to the most popular independent IPv6 counters that exist for Russia.

Counter	Hotlog	LiveInternet	Mail.ru	Rambler	SimilarWeb (top50)
IPv6	10.8%	8.3%	7.7%	10%	26%
IPv6 without Cloudflare	8%	3.3%	3%	3.3%	26%

The significantly higher percentages for SimilarWeb is explained by the fact that it provides a small number of websites, including Google, YouTube, Facebook, Wikipedia, etc. that are all accessible over IPv6, which the other counters do not include in their analyses. This means that Russian Internet users can access more resources over IPv6 than it may at first seem.

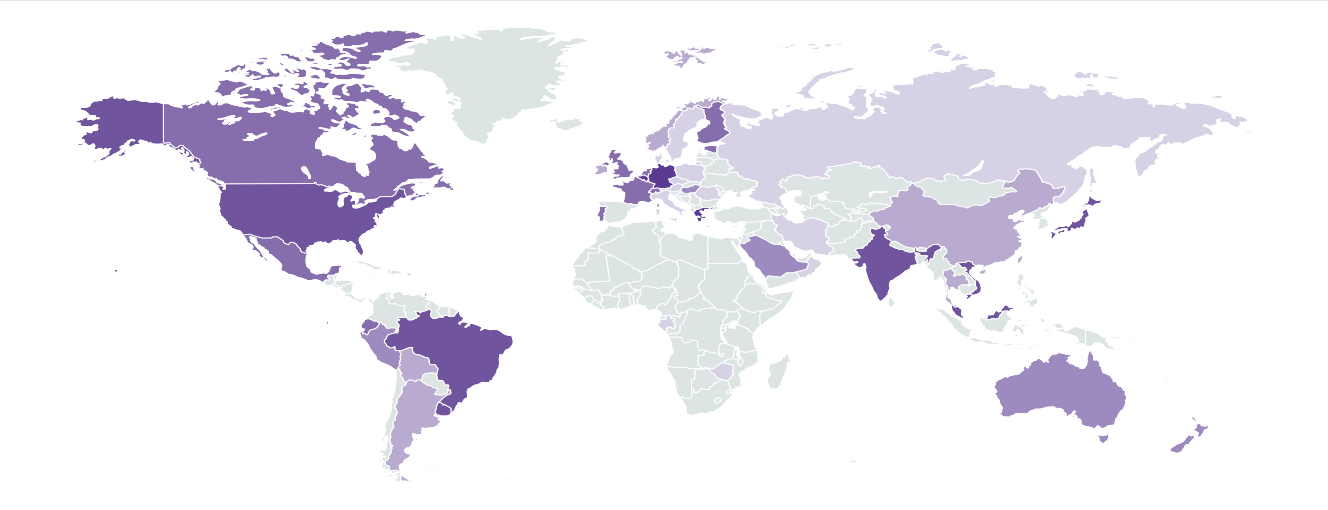


Figure 6: Relative global IPv6 accessibility according to Google.

Perhaps surprisingly, the most popular websites (in terms of traffic) do not lead the way in IPv6 deployment, which is likely a result of larger websites using their own content delivery networks while the smaller ones rely on Cloudflare, which, in fact, provides the IPv6 support.

The main factors driving IPv6 deployment appear to be:

- A desire to reach not only Russian, but also Western audiences and content
- Protection using Cloudflare services (which include IPv6 support for free by default) as protection against DDoS attacks
- A desire on the part of companies (particularly large companies like Yandex, Mail.RU and Google) to target potential customers more precisely (which is much more difficult when end users are sharing IPv4 addresses)

IPv6 in Mobile Networks

Deployment of IPv6 on mobile device networks has proved to be a significant driver of IPv6 adoption rates in parts of the world.

Mobile adoption of IPv6 has only happened recently in Russia. In 2017, MTS (one of the largest national operators in Russia) started an IPv6 pilot project in their mobile network, and in 2018 this project started being rolled out in production, region by region. Initially they allowed enthusiasts on Android devices to opt in to IPv6. In mid-2018, Apple supported the initiative and IPv6 also became accessible to users with newer Apple devices. After that, MTS switched to an opt-out model for Apple users. MTS then started negotiations with other vendors about out-of-the-box IPv6 support on their new devices.

Although the overall percentage of mobile users accessing content over IPv6 remains relatively low in Russia for the time being, we can expect this number to increase as other national providers make their own agreements with vendors and begin making IPv6 available to their customers.

Russia's Networks

Another way to view the Internet landscape is by looking at Autonomous Systems. An Autonomous System (AS) is a network or group of networks run by one or more operator(s) with a single, clearly defined routing policy. AS Numbers (ASNs) are used to identify networks in a similar way that IP addresses are used to identify specific devices. An LIR that is a traditional Internet service provider will typically operate a single AS, though it may have more depending on the nature of its business and network requirements. There are around 80,000 independent networks, or Autonomous Systems, on the Internet today, making up the global "network of networks".

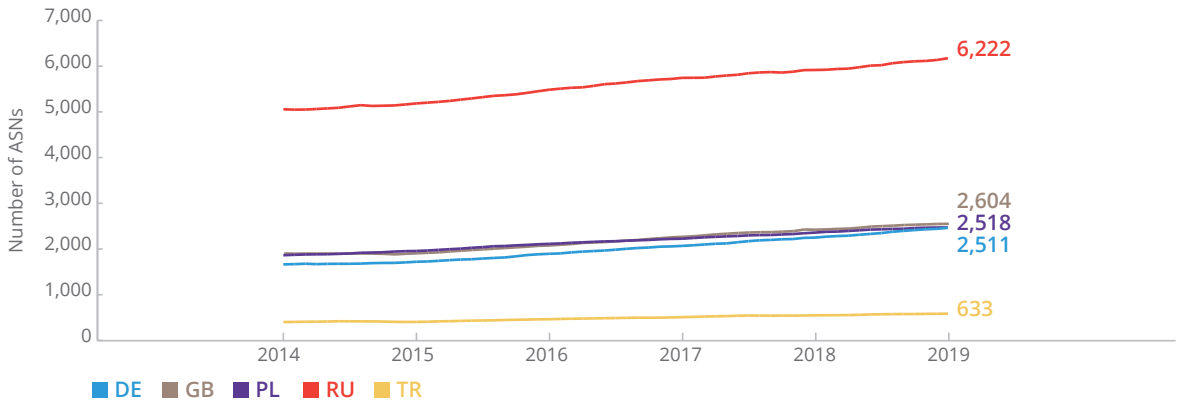


Figure 7: AS Number growth in the last five years.

Compared to other countries in the RIPE NCC service region, the number of ASNs registered to Russian entities is substantially higher, at 6,228. This may be due in part to the large geographical size of the country.

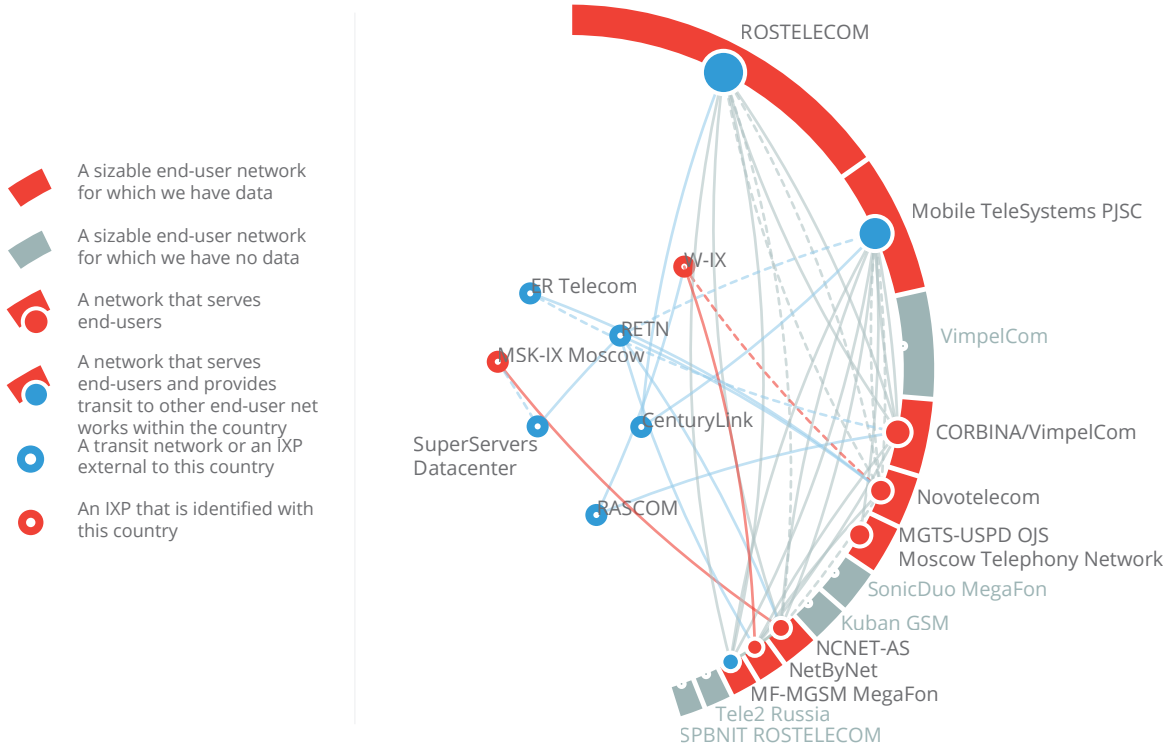


Figure 8: A snapshot of Russian ASNs and the interconnections between them during January 2019. ASNs that are not visible are those that cover less than 1% of Internet users in Russia.

Another reason could be that, historically, many organisations in Russia and Eastern Europe didn't register with the RIPE NCC as an LIR themselves but still wanted their own address space, which meant obtaining address space from an existing LIR. As part of that process, such organisations often obtained an AS Number, in order to be able to define their own routing policies and be more independent.

Russia's Internet market has also historically been large, diverse and open, supporting many different Internet Service Providers. Even as larger companies have acquired smaller ones more recently, the ASNs are still in use.

This kind of network diversity has contributed to Russia's robust internal connectivity; with many different paths for traffic to be able to flow through, there is less potential for disruption.

How Internet Traffic is Routed

The Internet is a dynamic ecosystem where independent, autonomously operating parties connect and exchange traffic at a multitude of places. The RIPE NCC cannot see how much traffic flows over each link, or know all possible routes between Russian service providers. However, several RIPE NCC tools allow us a glimpse into how traffic is routed through Russian address space.

International Traffic: How Traffic Reaches Russia

When international Internet connectivity in a country is heavily regulated, we expect a relatively small number of entry points into the country, provided by a few dominant organisations. These organisations provide connectivity on the national level, either to locally operating ISPs or directly to end users. When policies are more liberal, smaller ISPs may also provide connectivity via international players, a foreign Internet exchange point (IXP), or with foreign organisations at a local IXP. In those cases, we would expect to see more diversity in the paths available to traffic entering the country.

Figure 9 presents views for Russian IPv4 space from an IXP in Frankfurt, Germany and another in São Paulo, Brazil. For all of the approximately 32,000 Russian IPv4 prefixes (each of which contains many individual IP addresses) available to the global Internet, they show the first Russian network(s) observed and the number of prefixes passing through them. We can see there is quite some diversity. Five to ten networks act as an entry point for most traffic entering Russia, but about 1,000 other networks also provide some international connectivity. There is even greater diversity in the paths available to IPv6 traffic.

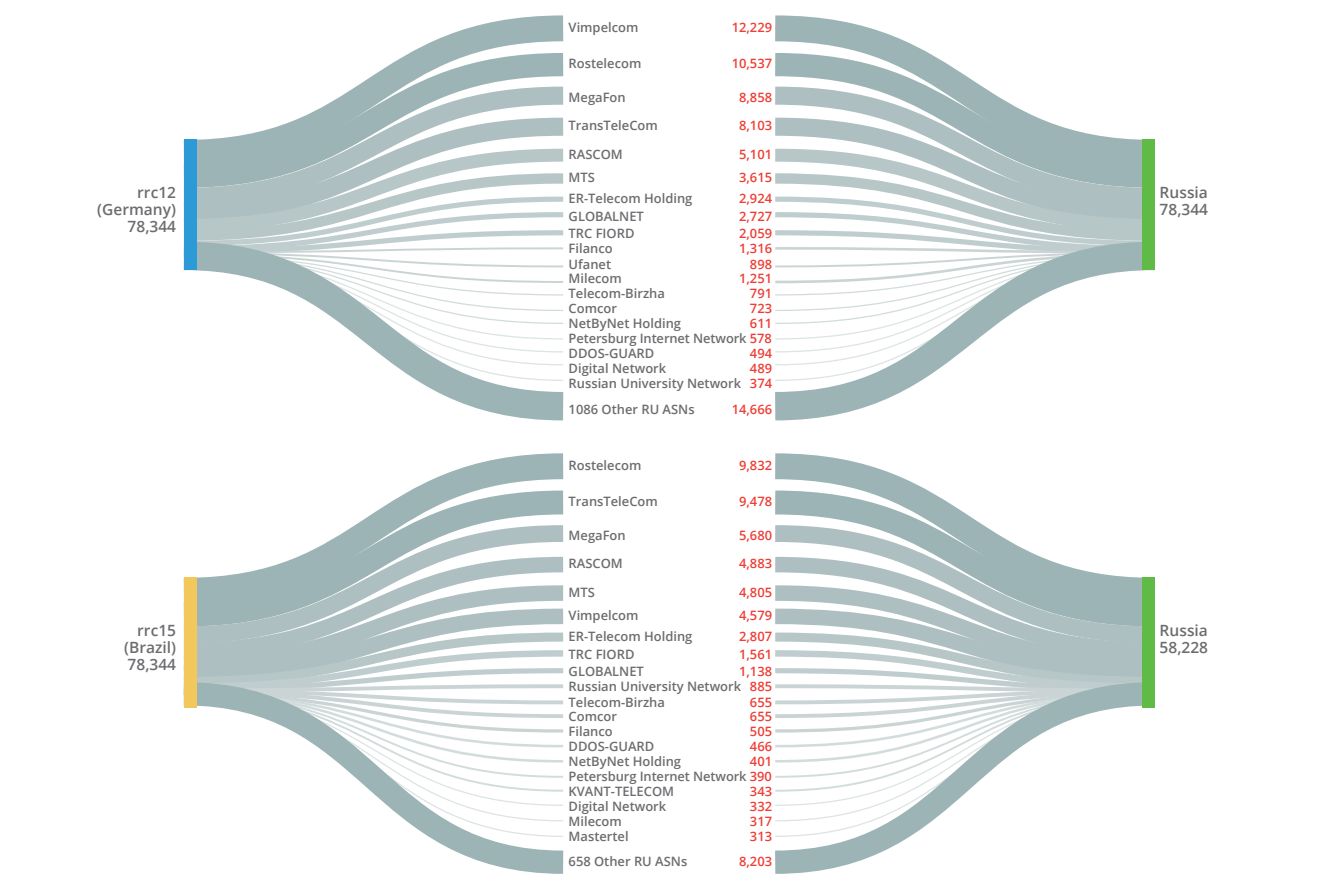


Figure 9: First Russian ASNs observed from Germany (top) and Brazil (bottom), with the number of prefixes passing through each ASN labelled.

It's important to note that the RIPE NCC cannot see all possible paths available to traffic being routed; our view is based on the approximately 170 locations where we collect data. Similarly, we cannot say whether these paths are actually used to route traffic – only that they are available.

What we can determine is that no single party holds the monopoly on international IP connectivity to Russia, and that even from a location as distant as São Paulo, providers have different paths to reach Russia. Having many paths and connections is important to the health of the Internet, because if one path becomes unavailable for whatever reason, traffic is simply rerouted via another available path. The many available paths into Russia, coupled with its many independent networks, therefore means that it benefits from a stable and resilient Internet.

Traffic Within Russia: Does Local Traffic Leave the Country?

Given Russia's large number of available traffic paths, one would expect traffic with a Russian origin and destination to stay within the country. Generally, this is the case – but not always. One exception occurs when traffic is routed via a provider present in Russia but with alternative routes outside of the country that may sometimes also be taken. However, we also see cases where, after reaching Russian networks, traffic takes a detour to one or more foreign networks before returning to its final destination in Russia.

We can look at the different paths that traffic could take from two different perspectives: the paths that are available between different networks (i.e. Internet service providers) according to what network operators include in their routing tables, and the paths that we see traffic take between two points. These two perspectives are based on different RIPE NCC measurement tools.

Available Network Paths

In a snapshot taken in March 2019, the RIPE NCC's data collectors found about 350,000 different available routes for the approximately 32,000 IP prefixes announced by Russian networks. Six percent of these routes appear to take a detour, meaning they traverse one or more foreign networks when sending traffic between two Russian networks.

The presence of a foreign network in the path could happen for any of three reasons:

1. The foreign network has infrastructure in a Russian data centre
2. The Russian prefix is used abroad, in foreign infrastructure
3. The Russian and foreign networks exchange traffic abroad, so traffic sent over these routes does in fact leave the country

Looking at the data, we find that 85% of the cases in which traffic appears to leave the country involve a single foreign network. In a large majority of our observations, that network is RETN, an internationally operating provider with a strong presence in Russia and Eastern Europe. As such, traffic over these paths very likely stays within Russia. A similar situation may apply to other cases where a single foreign network is seen; traffic over those paths does not necessarily leave Russia either. The remaining 15% of the cases in which traffic appears to leave the country are more complex, which involving more than one foreign network in the path. There is a greater likelihood of traffic leaving the country, but these cases only affect about 2,300 prefixes.

However, we also see cases where routes do seem to indicate that traffic would leave Russia. One Russian network peering at the Moscow Internet Exchange has paths to Rostelecom via RETN and the British Vodafone Group for 1,600 of the 32,000 Russian IP prefixes. The impact of such detours for Russian Internet users depends on the services offered by the destination networks as well as the market share held by the provider with the suboptimal paths.

It's interesting to know which paths exist between different networks - but just because these

routes exist, that does not mean that traffic is actually traversing them. It's possible, for example, that the majority of traffic traverses a relatively small number of the available paths, and that the majority of traffic actually stays inside the country (even though external routes are also available).

Paths Between Two Points

To assess whether traffic actually left the country while travelling from one Russian location to another, we look to measurements that record the IP addresses of the routers that are traversed between the two points (across all the different "hops" that Internet traffic takes along its journey).

For IPv4 traffic, we see that about 3% of paths have a non-Russian IP address. The top three countries where Russian traffic is routed before it reaches its final destination are Sweden (1.6%), Germany (0.7%) and Ukraine (0.4%). Sometimes the detour involves only one city, such as Stockholm, where different Internet Service Providers exchange traffic; other times, the route is more complex and we see packets go from Stockholm to Hamburg to Amsterdam before returning to Russia.

For IPv6 traffic, we see a much larger dependency on foreign exchange points, with 33% traversing another country.

Figure 10: Some of the paths taken by IPv6 traffic that left the country, despite having both a Russian origin and destination.

The View from K-root

Apart from IP address space, another major factor in looking at the broader Internet landscape is the Domain Name System (DNS), one of the main components of the Internet's global infrastructure. The root server system contains information on how to reach the authoritative servers for the DNS top-level domains (TLDs), such as .com, .org, .net, and the country-code TLDs, including .ru. When an Internet user types in "google.com", for example, their computer generally sends a query to their provider's DNS server. If it does not yet know how to reach ".com", it will ask a root name server for directions.

The RIPE NCC operates K-root, one of the 13 Internet root name servers. The K-root service consists of a set of distributed servers that use IPv4 and IPv6 anycast: by announcing the same IP prefixes from multiple locations around the world, service providers can choose which of the available locations is best suited for their DNS query traffic. Three of these K-root instances are located in Russia, hosted by Selectel in Saint Petersburg, MultiHOST LLC in Moscow and JSC MSK-IX in Novosibirsk.

Investigating which K-root instances are used from within Russia provides insight into how these resources are reached and shared within the country. The results give an indication of how the Internet service providers connect with one another.

The maps below illustrate how 450 of our measurement probes in Russia reach K-root servers.

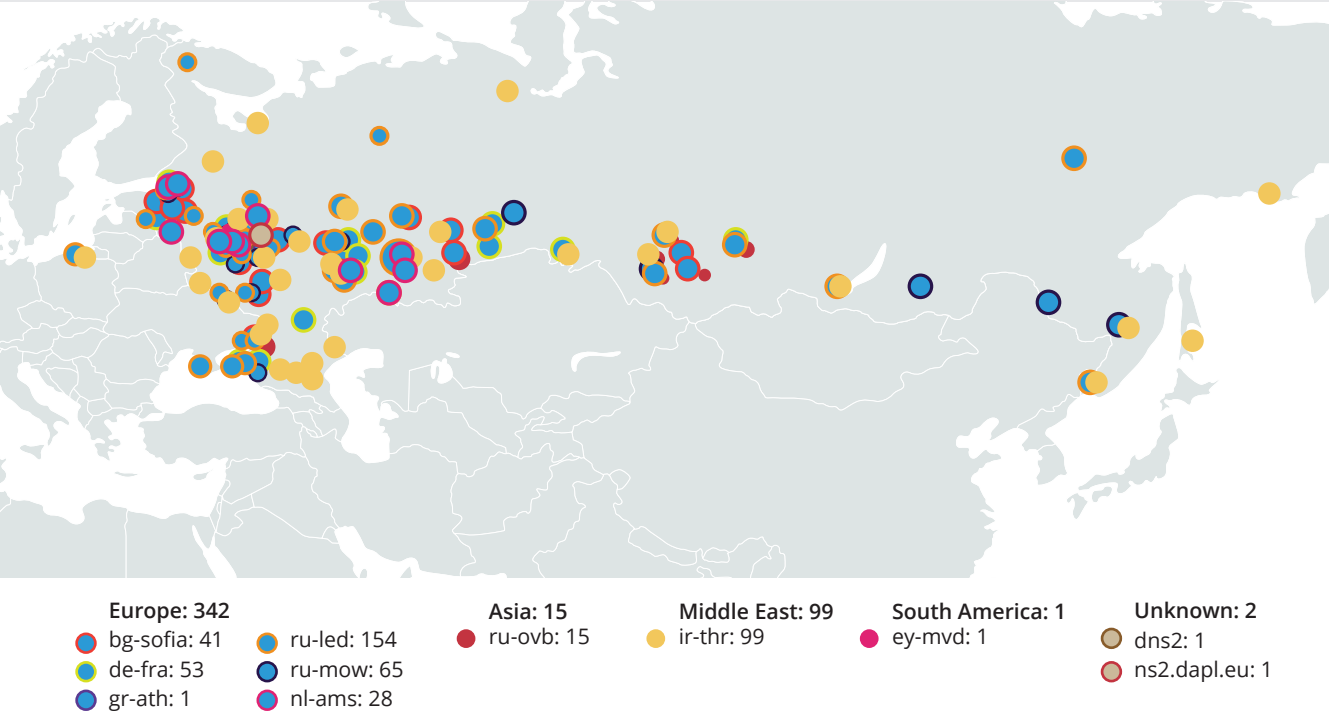


Figure 11: A view of which K-root server answers queries from locations within Russia and Moscow. Different colours represent the continent on which the K-root server is located: blue indicates locations in Europe, yellow the Middle East, and red Asia. The size of each data point reflects the time it took the server to answer the query.

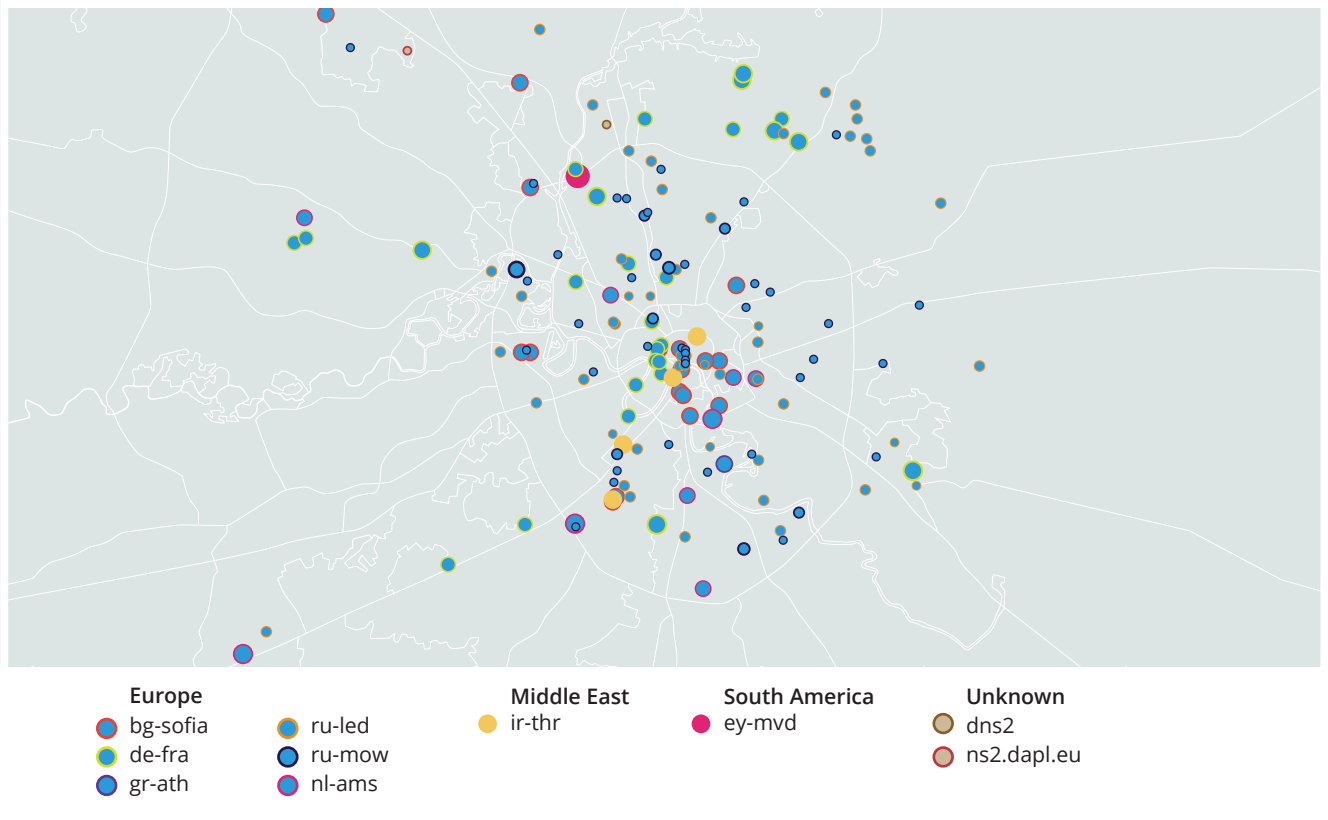


Figure 12: A view of which K-root server answers queries from locations within Russia and Moscow. Different colours represent the continent on which the K-root server is located: blue indicates locations in Europe, yellow the Middle East, and red Asia. The size of each data point reflects the time it took the server to answer the query.

On the country level, we see a split between servers in Europe and the Middle East (specifically Iran), with similarly sized circles, indicating comparable response times. If we zoom in to the Moscow region, only a few queries were sent to the server in Iran and, as indicated by the smaller sized circles, a good number use a local (Moscow or Saint Petersburg) server, resulting in a short response time.

K-root instance	Number of measurement probes answered by indicated K-root instance	K-root instance	Number of measurement probes answered by indicated K-root instance
Saint Petersburg	149	Sofia	41
Tehran	101	Amsterdam	29
Moscow	64	Novosibirsk	14
Frankfurt	53	Montevideo	1

The limited number and location of RIPE NCC measurement probes mean that these results are not necessarily representative for the country as a whole. But they do illustrate that at least some service providers rely on a K-root server outside of Russia. This has little impact on the performance of the Internet; most queries are answered from a local cache, and these are often hosted by service providers. Additionally, when response times from a specific network to the K-root server are high, it is likely those queries will be answered by an instance of one of the other root name servers which, in the topology of the Internet (not necessarily geographical distance), happens to be closer.

Conclusions

While the Russian Internet's development may have intensified later than some the other big Internet economies like Germany and the UK, it has developed quickly over recent years, with millions of users coming online.

In the RIPE NCC service region, Russia holds the sixth largest amount of IPv4 address space and has the third largest number of LIRs. The number of LIRs has grown substantially in recent years, due in part to true growth and in part to the increasing scarcity of available IPv4 address space, with some operators opening multiple RIPE NCC accounts in order to obtain additional IPv4 allocations.

There is a healthy IPv4 transfer market in Russia. IPv4 address space is being transferred both into and out of the country, but two thirds of transfers are taking place between Russian entities, as those organisations with unused space help to fill the needs of those that require more.

The small amounts of IPv4 address space the RIPE NCC is still allocating to support new entrants to the market cannot meet long-term demand, and should only be seen as a way to facilitate IPv6 deployment. As more and more aspects of citizens' everyday lives migrate to the online world, it's more important than ever to ensure that the required technical infrastructure is in place to support this evolution.

Russia's IPv6 adoption is still in its early stages and is currently lower than the worldwide average; however, many of the barriers that have historically held back network operators and decision makers from making the switch to IPv6 having now been overcome, and the country is well equipped to support the rapid adoption of this next generation protocol to ensure it can meet the needs of its increasingly connected population.

Russia benefits from a robust national Internet infrastructure, including good access to the Domain Name System (DNS). Although some service providers rely on DNS root name servers located outside of the country, this has little impact on Internet performance. While hosting more local instances of the K-root name server would do little to improve response times or resiliency, any organisation willing to meet the technical requirements of hosting a K-root instance is able to do so by applying, for free, with the RIPE NCC.

In addition, the vast majority of local IPv4 traffic is routed within the country and does not rely on foreign exchange points, although this percentage is higher for IPv6 traffic. In some cases, even traffic that appears to travel outside the country may involve an international provider that is operating in Russia, meaning that traffic actually remains within the country.

The diverse number of paths available to traffic entering Russia from the global Internet, coupled with the large number of independent networks operating within the country, means that Russia enjoys a stable Internet resistant to disruption, while contributing to the resiliency of the global Internet.

About the RIPE NCC

The RIPE NCC serves as the Regional Internet Registry for Europe, the Middle East and parts of Central Asia. As such, we allocate and register blocks of Internet number resources to Internet service providers (ISPs) and other organisations.

The RIPE NCC is a not-for-profit organisation that works to support the open RIPE community and the development of the Internet in general.

Although based in Amsterdam, the RIPE NCC has staff based across our service region and an office in Dubai to better understand and serve the needs of members and other stakeholders in this part of our service region.

Data Sources

The information presented in this report and the analysis provided is drawn from several key resources:

RIPE Registry

This is the record of all Internet number resources (IP addresses and AS Numbers) and resource holders that the RIPE NCC has registered. The public-facing record of this information is contained in the RIPE Database, which can be accessed from **www.ripe.net**.

RIPE Atlas

RIPE Atlas is the RIPE NCC's main Internet data collection system. It is a global network of hardware devices, called probes and anchors, that actively measure Internet connectivity. Volunteers around the world connect these devices to their home networks or data centres. Anyone can access this data via Internet traffic maps, streaming data visualisations, and an API. RIPE Atlas users can also perform customised measurements to gain valuable information about their own networks. **https://atlas.ripe.net**

Routing Information Service (RIS)

The Routing Information Service (RIS) collects and stores Internet routing data from locations around the globe. It was established in 2001. More information is available at:
https://www.ripe.net/ris

The data obtained through RIPE Atlas and the Routing Information Service is the foundation for many of the tools that we offer. We are always looking at ways to get more RIPE Atlas probes connected and to find network operators willing to host RIS collectors.

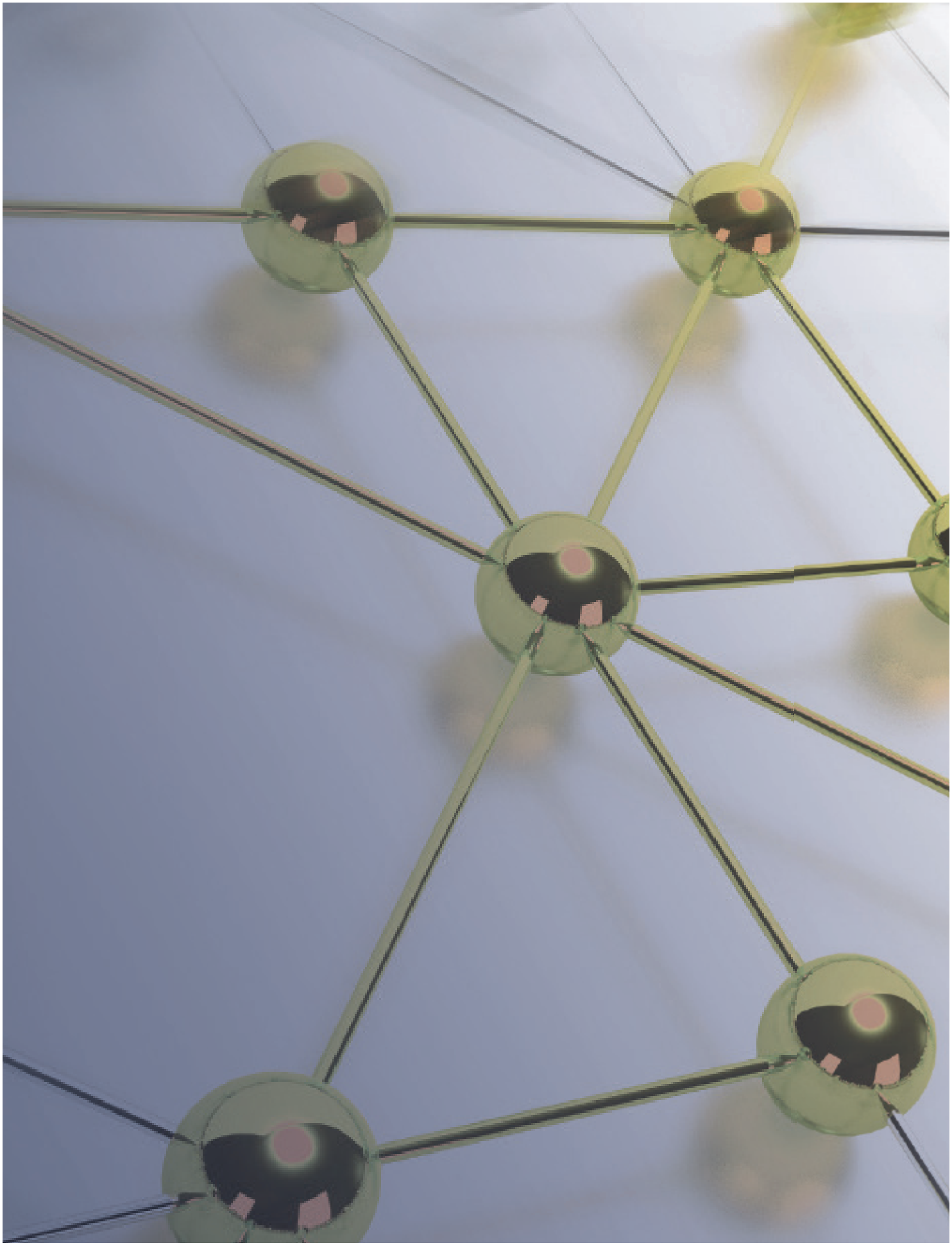
For more information on how you can contribute or be a part of this important work, see:
https://atlas.ripe.net/get-involved/

Other RIPE NCC tools and services:

- RIPEstat: https://stat.ripe.net/
- RIPE IPmap: https://ipmap.ripe.net/
- K-root: https://www.ripe.net/analyse/dns/k-root

External Source:

- Omnibus GfK - independent organisation providing global figures for Internet penetration



RIPE NCC
RIPE NETWORK COORDINATION CENTRE