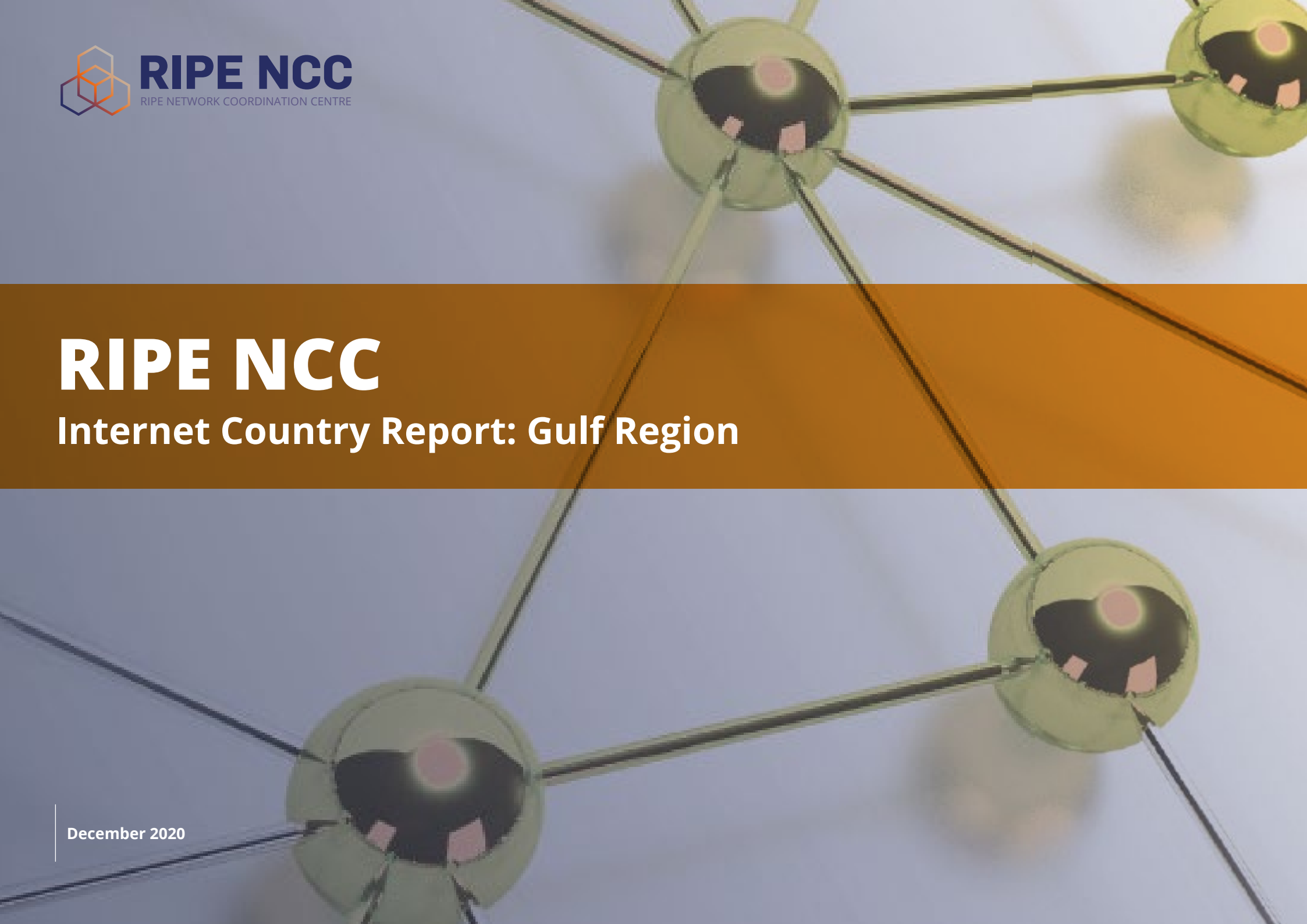


RIPE NCC
RIPE NETWORK COORDINATION CENTRE

RIPE NCC

Internet Country Report: Gulf Region

December 2020

Introduction

The Internet is a global network of networks, yet every country's relationship to it is different. This report provides an outlook on the current state of the Internet in the Gulf region. We offer an analysis of the region's market landscape and its state of development, examine Internet routing within the region, take a close look at how it connects to the global domain name system, and investigate its connections to the global Internet. This analysis is based on what we can observe from the RIPE NCC's measurement tools as well as a few external data sources.

We focus the spotlight on eight different countries in the RIPE NCC's service region – Bahrain, Iraq, Kuwait, Oman, Qatar, Saudi Arabia, the United Arab Emirates and Yemen – which form a sub-region with its own unique opportunities and challenges, and present a comprehensive analysis of its Internet development and potential for future growth in order to inform discussion, provide technical insight, and facilitate the exchange of information and best practices regarding Internet-related developments in this part of the world. This is the sixth such country report that the RIPE NCC has produced as part of an ongoing effort to support Internet development throughout our service region by making our data and insights available to local technical communities and decision makers.

Highlights

- Market development, infrastructure and available Internet address resources all vary widely among the eight countries included in this report
- Even in the more mature access markets, state-owned incumbents are still the dominant players
- IPv4 scarcity may pose less of a challenge than in other parts of the world, given the region's high mobile penetration, but further IPv6 deployment is still needed to support future growth
- Domestic connectivity within the countries shows bottlenecks and potential single points of failure
- International connectivity in many of the Gulf countries is not very diverse, with the majority dependent on a small number of providers
- Regional connectivity is far from optimised in the region as a whole, with traffic being sent across distant locations rather than making use of local exchange points
- Routing security could be greatly improved in the region

Digital Trends, the Gulf Market and Opportunities for Growth

Data Sovereignty, Cloud Strategies and Building Internet Ecosystems

As more and more of the world's business transactions, government services, education models and our private lives move online, several themes have emerged in recent years in policy discussions around the digital landscape.

One of these is that governments are increasingly concerned with the idea of digital sovereignty, extending their need to protect their citizens and physical resources to the online world. Suddenly, the route that Internet packets take from point A to point B has gone from being a technical argument to a matter of national security. Several countries in the Gulf region have already enacted laws and regulations to protect citizens' personal data.[1] Governments in the region, as elsewhere in the world, are becoming increasingly aware of and concerned with the idea of this data leaving their countries' borders.

Governments are also looking to protect their national infrastructure, which increasingly includes ICTs. Many nations have a vested interest in ensuring their digital independence and are looking at ways of reducing existing dependencies on foreign infrastructure or resources. With so much of our economies and societies relying on the Internet today, there's simply too much at stake.

Another major trend taking place today is the shift to cloud providers. Building physical infrastructure is expensive, and many different types of businesses, organisations and governments are now looking to the cloud to provide the services they need, making this relatively new type of service provider a major player in the digital sphere. Indeed, many of the Gulf countries have cloud computing strategies in place as a key component of their digital transformation efforts. However, governments in some parts of the world are also becoming increasingly wary of relying on the biggest cloud providers (Google, Amazon Web Services, Alibaba, etc.) for these services, as they are concentrated in the US and China and create yet another foreign dependency. As a result, many governments are now looking to develop their own local cloud platforms.

A shift has also taken place in that the Internet is no longer the sole domain of the Internet service and telecommunications providers. Advances like IoT coupled with a greater overall dependency on ICTs have caught the attention of other industries that have now become active in the digital sphere.

For all these reasons, regulating and governing this space has become considerably more complex, as measures taken towards the Internet or telecommunications industry can quickly spill over or cause unintended consequences for a wide range of industries that, at first glance, seem to be totally unrelated.

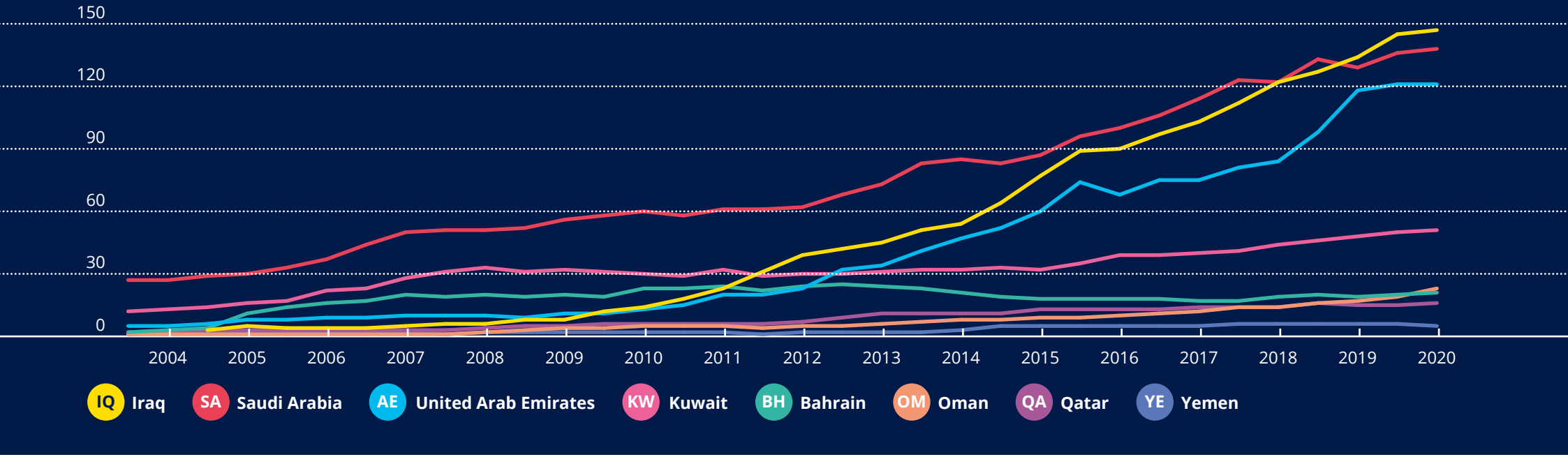
In order to develop healthy, local Internet ecosystems – those that support local content development and hosting, data exchange, cloud and other services – governments need to create an enabling environment that encourages open, diverse markets that allow for greater connectivity, multiple access points and increased choice in service providers both nationally and internationally. In this report, we look at a number of different indicators in order to assess the region's ability to support this kind of local Internet development, including: resource availability, diversification in domestic and international access, regional connectivity and routing security.

The Market Landscape

The countries included in this report vary greatly in terms of geographical size and location, population and GDP. As a result, their digital landscapes – including market development, infrastructure, and national ICT priorities – also span a wide range. The focus in many of the region's nations is on digital transformation, including smart cities, e-government and e-health services. These countries all have national ICT strategies in place that aim to position them as regional or world leaders, placing a great deal of attention on such aspects as infrastructure initiatives, ICT skills and cloud access.

1 *Data Protection Laws of the World: https://www.dlapiperdataprotection.com/index.html?t=law&c=BH&c2=*

Figure 1:
Number of Local Internet Registries over time



Number of Providers and Other Organisations Running Their Own Networks

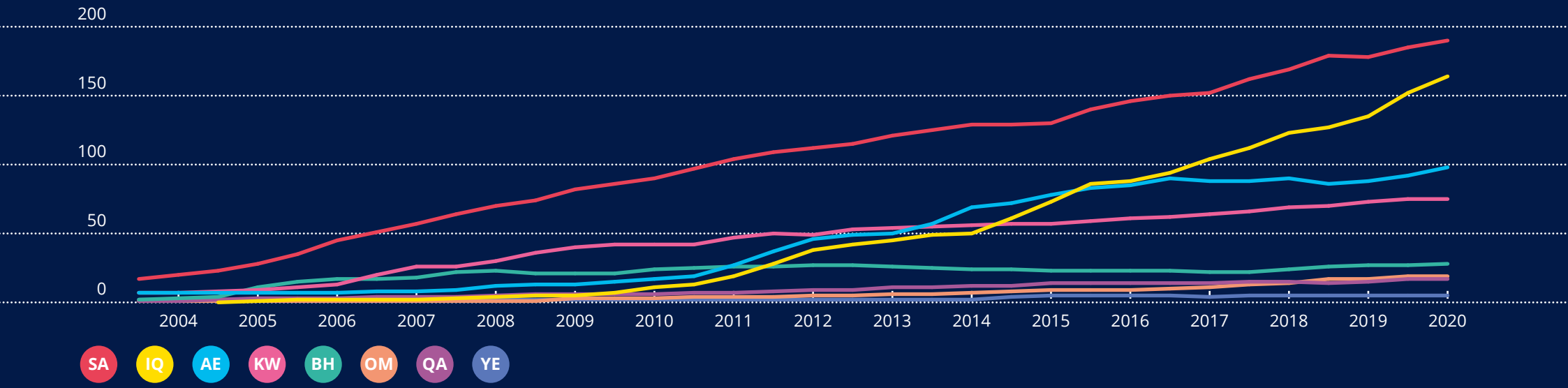
As the Regional Internet Registry for the Gulf region, the RIPE NCC can track the development of the local Internet through the increase in RIPE NCC members and Local Internet Registries (LIRs) over time. As illustrated in figure 1, there is a clear split in the region in terms of LIR growth over time. While Iraq, Saudi Arabia, the United Arab Emirates and, to a lesser extent, Kuwait all show significant growth over the past decade, Bahrain, Oman, Qatar and Yemen have experienced far less growth, with some plateauing or even decreasing their number of LIRs.

RIPE NCC Members and Local Internet Registries (LIRs)

RIPE NCC members include Internet service providers, content hosting providers, government agencies, academic institutions and other organisations that run their own networks in the RIPE NCC's service region of Europe, the Middle East and Central Asia. The RIPE NCC distributes Internet address space to these members, who may further assign IP addresses to their own end users. It is possible for members to open more than one account, called a Local Internet Registry (LIR).

For a long time, the majority of RIPE NCC members were large, incumbent Internet service providers. More recently, however, we've seen a significant increase in other types of organisations requesting IP addresses to run their own networks, including banks, government agencies, academic institutions and enterprises. This gives these organisations greater control over their Internet number resources, routing policies, and access to other providers, including the cloud and big data providers that play a significant role in today's Internet ecosystem. An increase in diversity, combined with an ability to select from different connectivity providers, generally creates a more competitive environment and helps drive down costs.

Figure 2:
Number of networks over time



As a result of this change, an increase in the number of LIRs doesn't necessarily mean there are more Internet service providers. In addition, it's possible for the same organisation to hold several LIRs, although we don't see this in practice much in the Gulf region except in the United Arab Emirates, where 87 organisations hold 121 LIRs.

As seen in figure 1, there's been steep growth in the number of LIRs in Iraq, which overtook Saudi Arabia in 2019 to become the Gulf country with the most LIRs. From 1 January 2019 until 1 November 2020, 36 new Iraqi LIRs were established, all of which are still active. There appears to have been a large surge of small to medium Internet service and solutions providers, some with a national and others with a more regional focus. This should help diversify the domestic market, as more players can offer unique solutions for their customers, drive down costs and increase innovation – all of which support the long-term health of the local Internet ecosystem.

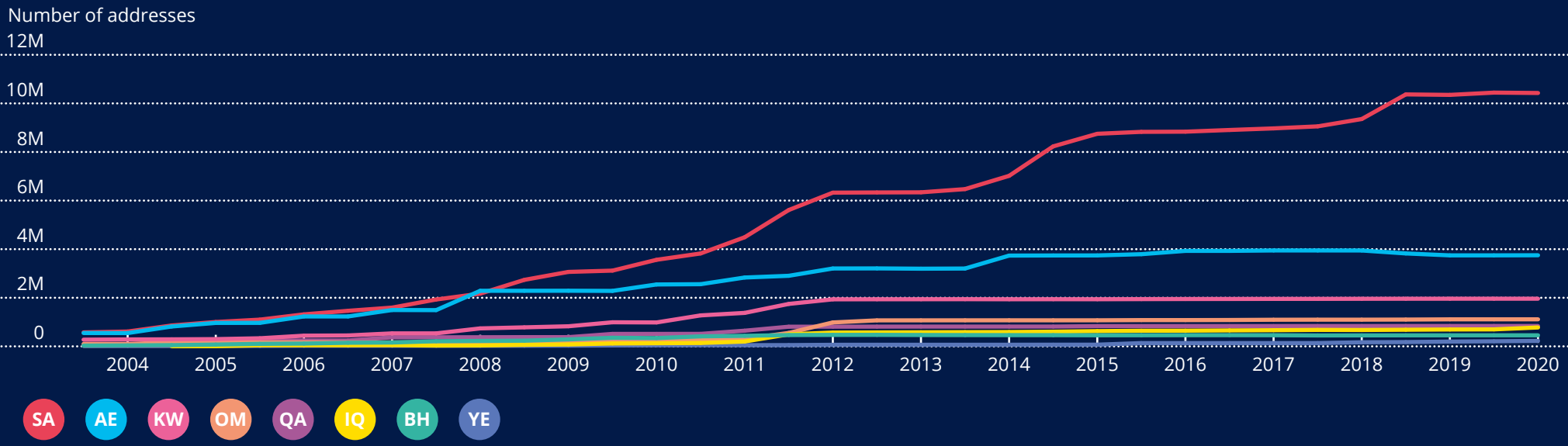
Network Growth and Diversity

A larger number of Local Internet Registries generally corresponds to a larger number of independently operated networks called Autonomous Systems, each of which is represented by an Autonomous System Number, or ASN. (An Autonomous System is a group of IP networks that are run with a single, clearly defined routing policy. There are currently about 70,000 active ASNs on the Internet today.) The RIPE NCC is responsible for the allocation of ASNs in the Gulf region as part of its mandate as the Regional Internet Registry. This provides us unique insight into the distribution and deployment of these networks across the Internet.

In figure 2, we again see a divide among the Gulf countries, with significant growth in Saudi Arabia, Iraq, the United Arab Emirates and Kuwait, and little to none in Bahrain, Oman, Qatar and Yemen.

The number of networks in a given country is one indication of market maturity. The greater the diversification, the more opportunity exists for interconnection among networks, increasing resiliency.

Figure 3:
IPv4 holdings over time



IPv4 Address Space in the Gulf Region

Until 2012, RIPE NCC members could receive larger amounts of IPv4 address space based on demonstrated need. When the RIPE NCC reached the last /8 of IPv4 address space in 2012, the RIPE community developed a policy allowing LIRs to receive a small, final allocation of IPv4 (1,024 addresses) in order to help them make the transition to IPv6, the next generation protocol that includes enough IP addresses for the foreseeable future. In November 2019, the RIPE NCC made the last of these allocations and a system now exists whereby organisations who have never received IPv4 from the RIPE NCC can receive an even smaller allocation from a pool of recovered address space as long as there is space available in the pool (occasionally member accounts are closed and address space is returned to the RIPE NCC).

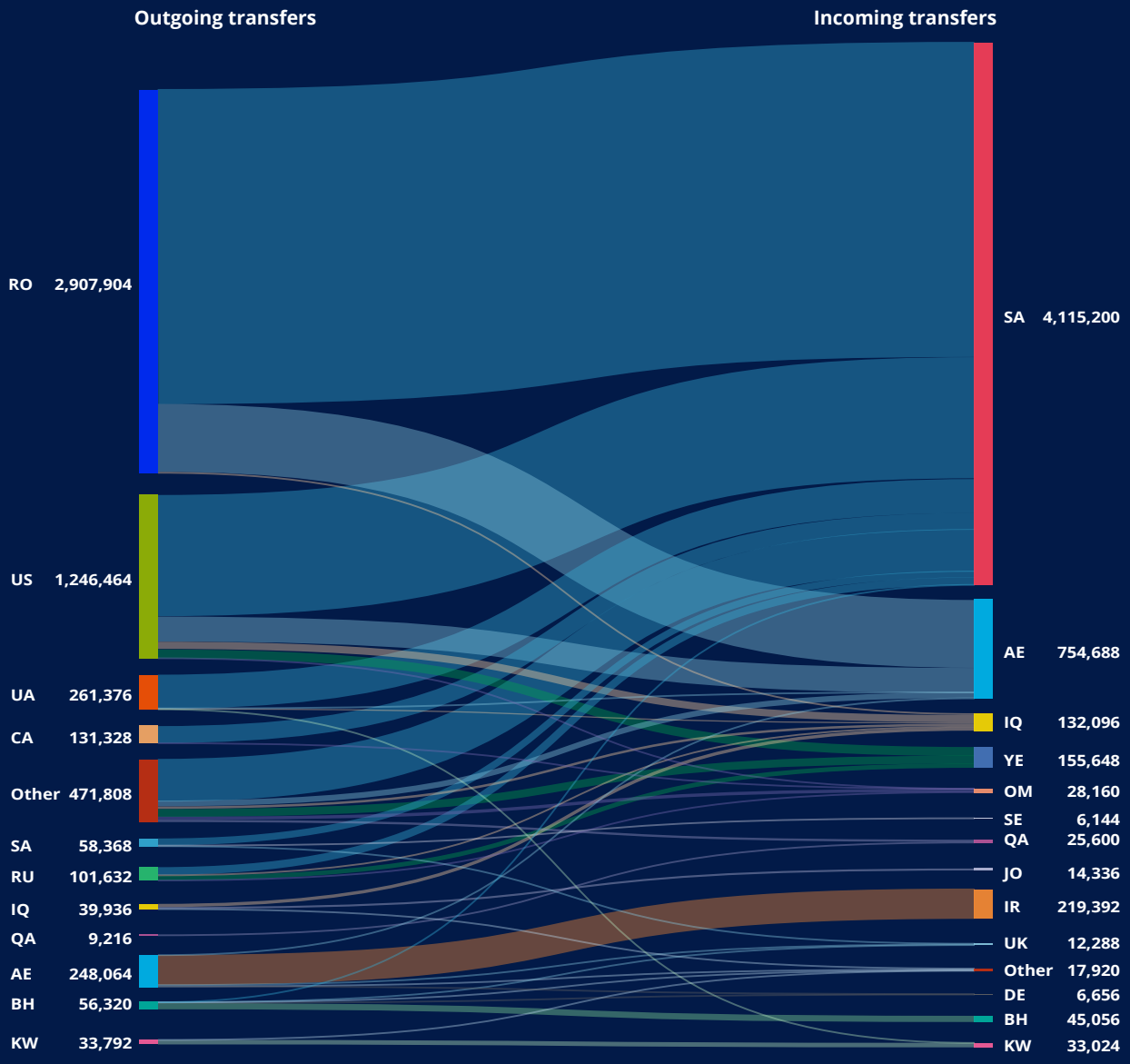
Indeed, 2012 does seem to be a turning point for many of the Gulf countries – including Kuwait, Oman, Qatar, Iraq, Bahrain and Yemen – after which we see IPv4 acquisition plateau. In fact, we only see modest growth even before 2012, signaling a later start to Internet development than in parts of Europe, for example. We see Saudi Arabia and the United Arab Emirates acquired more IPv4 in the years leading up to 2012, and moderate growth continued even after this point in the United Arab Emirates for a number of years before tapering off.

Interestingly, Saudi Arabia continued to acquire millions of IPv4 addresses even after the policy change in 2012. The final IPv4 allocations made to new LIRs after 2012 were so small (1,024 addresses each) that this doesn't increase a country's IPv4 holdings by much. Instead, this growth was almost exclusively the result of IPv4 transfers.

IPv4 Secondary Market

To fill the demand for more IPv4 address space, a secondary market has arisen in recent years, with IPv4 being bought and sold between different organisations. The RIPE NCC plays no role in these financial transactions, ensuring only that the RIPE Registry – the record of which address space has been registered to which RIPE NCC members – remains as accurate as possible.

Figure 4:
IPv4 transfers within, into and out of the Gulf region between January 2014 and November 2020



As IPv4 has become more scarce, many providers and other organisations have turned to the secondary market. Figure 4 shows the IPv4 transfers that have taken place within, into and out of each country in the region since the market became active.

Given its larger number of LIRs, networks and IPv4 holdings, it's no surprise to see Saudi Arabia as the most dominant of the Gulf countries in the transfer market. More than four million IPv4 addresses were transferred into the country over the past seven years, while a little more than 8,000 were transferred out of the country and another 50,000 or so were transferred between entities within the country. These imported addresses account for about 40% of the country's total IPv4 holdings. Romania supplied nearly three million of these addresses and more than a million came from the United States.

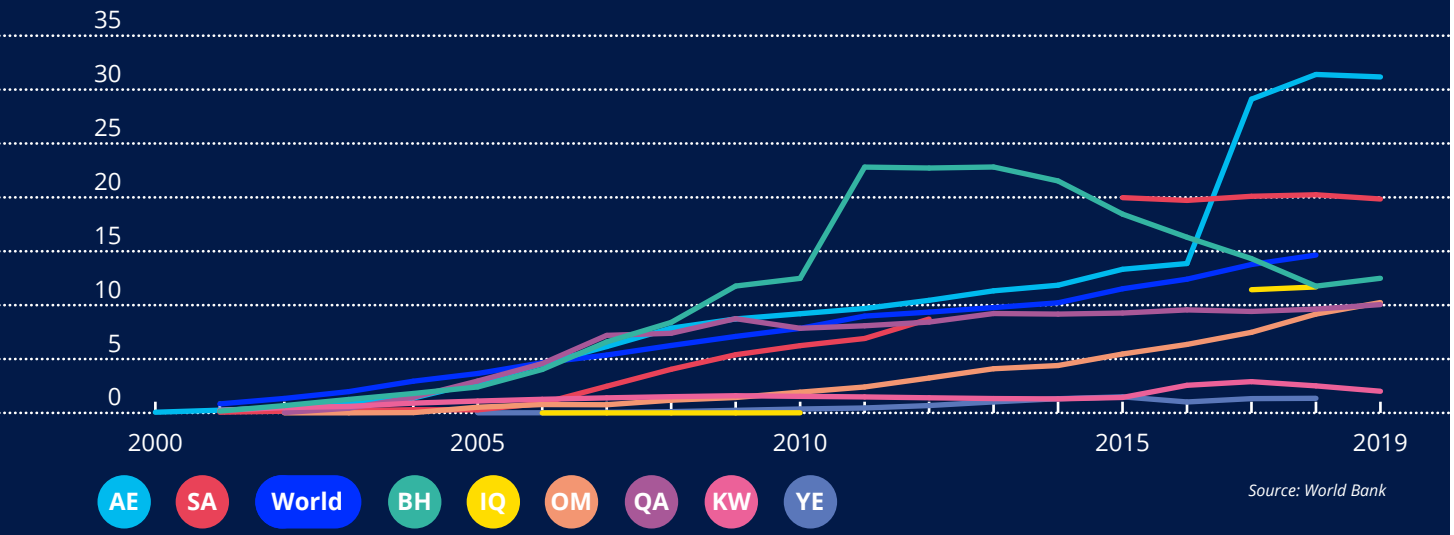
Romania is also the main source for IPv4 addresses transferred to the United Arab Emirates, the other main player in the secondary market. The United Arab Emirates has imported more than 750,000 addresses in total but has also exported nearly 250,000, the vast majority of which were transferred to Iran. Of the eight countries included, Bahrain and Kuwait were the only to have exported more IPv4 addresses than they imported, albeit by a small margin.

It's interesting to note that we see far fewer domestic transfers (between organisations in the same country) in the Gulf region than we do in other parts of the RIPE NCC's service region, including Europe and Central Asia. This is likely the result of having few online service providers in the region's markets.

Internet Penetration and Potential for Future Growth

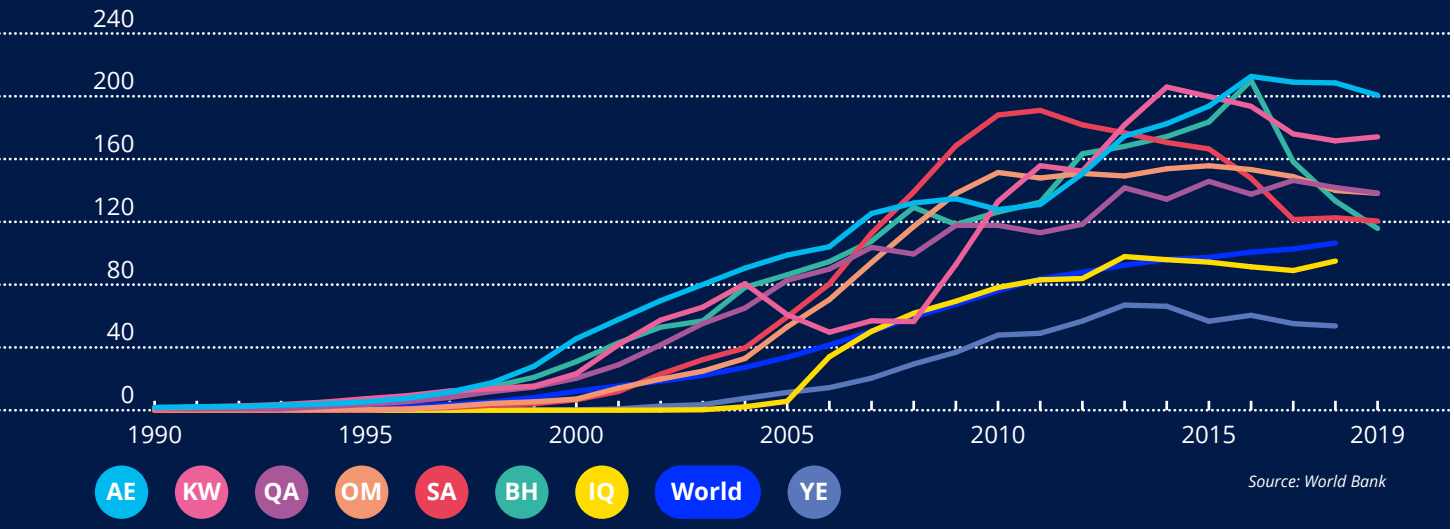
Despite Saudi Arabia's large IPv4 holdings, it still has only one IPv4 address for every three citizens. Most of the countries in the region are in a similar position, with one address for every two to five people. The exceptions are

Figure 5:
Fixed broadband subscriptions per 100 people over time



Source: World Bank

Figure 6:
Mobile subscriptions per 100 people over time



Source: World Bank

Iraq, with one address for every 50 people, and Yemen, with one address for every 136 people.

It's important to note that having a low address-to-population ratio doesn't necessarily mean that it will be impossible for a country to provide connectivity to all its citizens. Because the markets in the Gulf region were late to develop compared to much of Europe and North America, there was much faster growth in the mobile rather than the fixed broadband market.

As a result, we see some of the highest mobile subscriptions per capita in the world in many of the Gulf countries, with six of the eight countries averaging more than one mobile subscription per person. Indeed, mobile subscriptions in the wealthier Gulf countries are much higher than the average for the European Union (123), East Asia and the Pacific (122) and the world (107)[2], and although we see growth slowing in the more saturated markets in recent years, the number of mobile Internet users continues to grow, due in large part to the migration of 2G subscribers to mobile broadband networks.[3]

Technical workarounds exist that allow multiple users to share a single IP address, such as carrier-grade network address translation (CGN), and such technologies are in widespread use in mobile broadband connectivity. Given the region's high reliance on mobile access, there may still be enough IPv4 to accommodate short-term growth if mobile operators employ these technical workarounds to share IPv4 addresses among their users. However, there are well-documented drawbacks to address-sharing technologies, and in order to fully unlock the potential societal and economic benefits of further digitisation, deploying IPv6 is the only sustainable strategy for accommodating future growth and supporting the region's Internet development goals.

2 Source: World Bank
3 GSMA report, The Mobile Economy Middle East & North Africa 2019: https://data.gsmaintelligence.com/research/research/research-2019/the-mobile-economy-middle-east-north-africa-2019

Figure 7:
IPv6 holdings over time

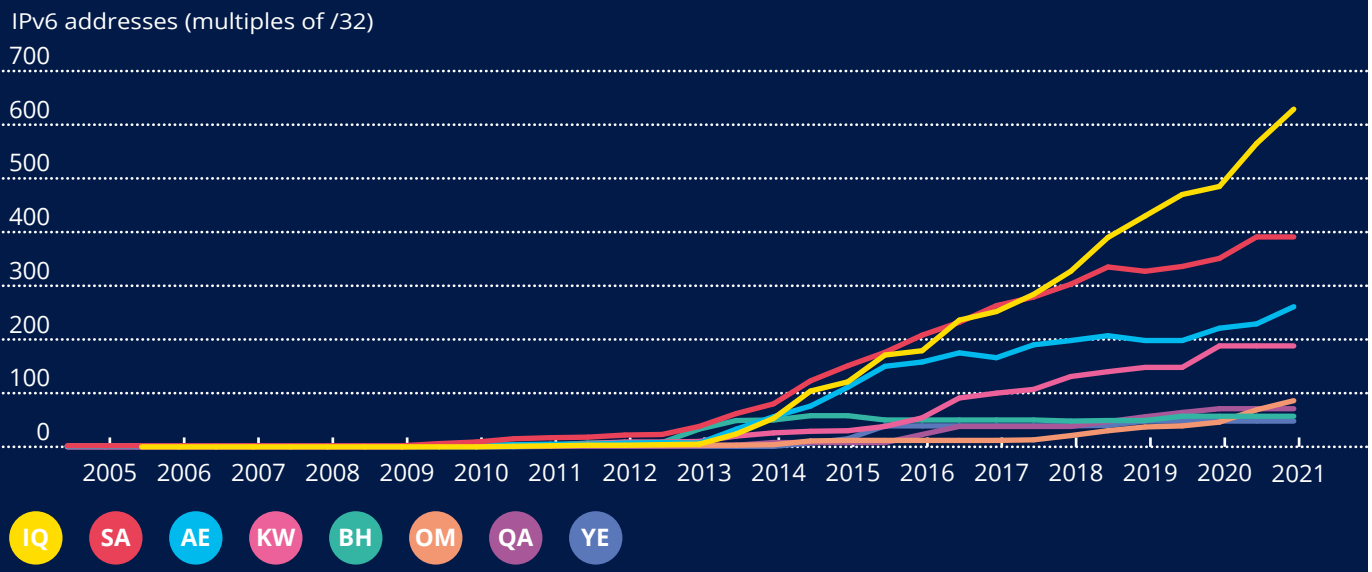


Figure 8:
IPv6 deployment rates

Country	Akamai	APNIC	Facebook	Google
United Arab Emirates	34.1%	31.5%	35.8%	31.9%
Saudi Arabia	25.5%	23.0%	21.6%	23.9%
Oman	10.6%	9.6%	11.8%	11.7%
Kuwait	5.4%	6.9%	7.6%	3.2%
Iraq	0.0%	0.0%	0.2%	0.0%
Qatar	0.0%	0.0%	0.2%	0.2%
Yemen	0.0%	0.1%	0.1%	0.1%
Bahrain	N/A	0.0%	0.0%	0.0%
World	N/A	27.2%	28.9%	32.2%

Sources:
Akamai: https://www.akamai.com/us/en/resources/our-thinking/state-of-the-internet-report/state-of-the-internet-ipv6-adoption-visualization.jsp, APNIC: https://stats.labs.apnic.net/ipv6, Facebook: https://www.facebook.com/ipv6, Google: https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption

IPv6 in the Gulf Region

Despite IPv4's dwindling availability and its increasing cost on the secondary market, many countries in the Gulf region continue to struggle with IPv6 deployment. Although Iraq, Saudi Arabia, the United Arab Emirates and Kuwait have substantially increased their IPv6 holdings in recent years, there are vast differences between them when it comes to actual deployment rates. In Iraq, for example, we see organisations opening LIRs and requesting an IPv6 allocation simply because there is no additional cost in doing so, and the country has few IPv4 addresses; however, this doesn't translate into actual use.

Data gathered by APNIC, Akamai, Facebook and Google show that Iraq, Bahrain, Qatar and Yemen have virtually no users connecting over IPv6. The United Arab Emirates leads the region, with between 31% and 36% deployment, depending on the measurement source.

In trying to make sense of these generally low figures, we can look to the RIPE NCC Survey 2019[4], which polled more than 4,000 network operators and other members of the technical community. Only 38% of survey respondents from the Gulf countries said that their organisations will require more IPv4 address space in the next two to three years, compared to a 53% average across all respondents. Indeed, 21% of respondents state that IPv4 scarcity isn't an obstacle for their organisation, with the top reason (at 27%) being that they have enough IPv4 addresses.

Of those who do find IPv4 scarcity an obstacle, 27% state that their biggest challenge is IPv6 deployment. Indeed, it appears that many organisations are aware of the need to transition to IPv6, as this was the top choice for how organisations planned to obtain more address space (24%) and other options, including buying IPv4 on the secondary

4 RIPE NCC Survey 2019: https://www.ripe.net/survey

market (19%) and using NAT (15%), were far less popular in the Gulf countries than the average across all regions (61% and 41%, respectively).

Despite awareness around IPv6, many organisations have not yet managed to fully deploy it. Indeed, only 5% of respondents from the Gulf countries answered that IPv6 was fully deployed on their networks compared to the total average across all respondents of 22%. However, 48% of respondents said they had either started deployment, were testing deployment, or were working on a deployment plan, so perhaps we will see an increase in IPv6 rates in the region over the coming years.

IPv6 deployment extending all the way to the end user and enterprise networks is key to supporting the digital transformation goals that the Gulf countries have set for themselves. Although current levels of IPv4 may be enough to maintain the status quo via address sharing and other workarounds, deploying IPv6 is the only sustainable strategy for accommodating future growth and supporting the region's Internet development as it continues to offer more and more services online, from e-government and e-health services to cloud services to online banking to smart cities.

2. Domestic and International Connectivity

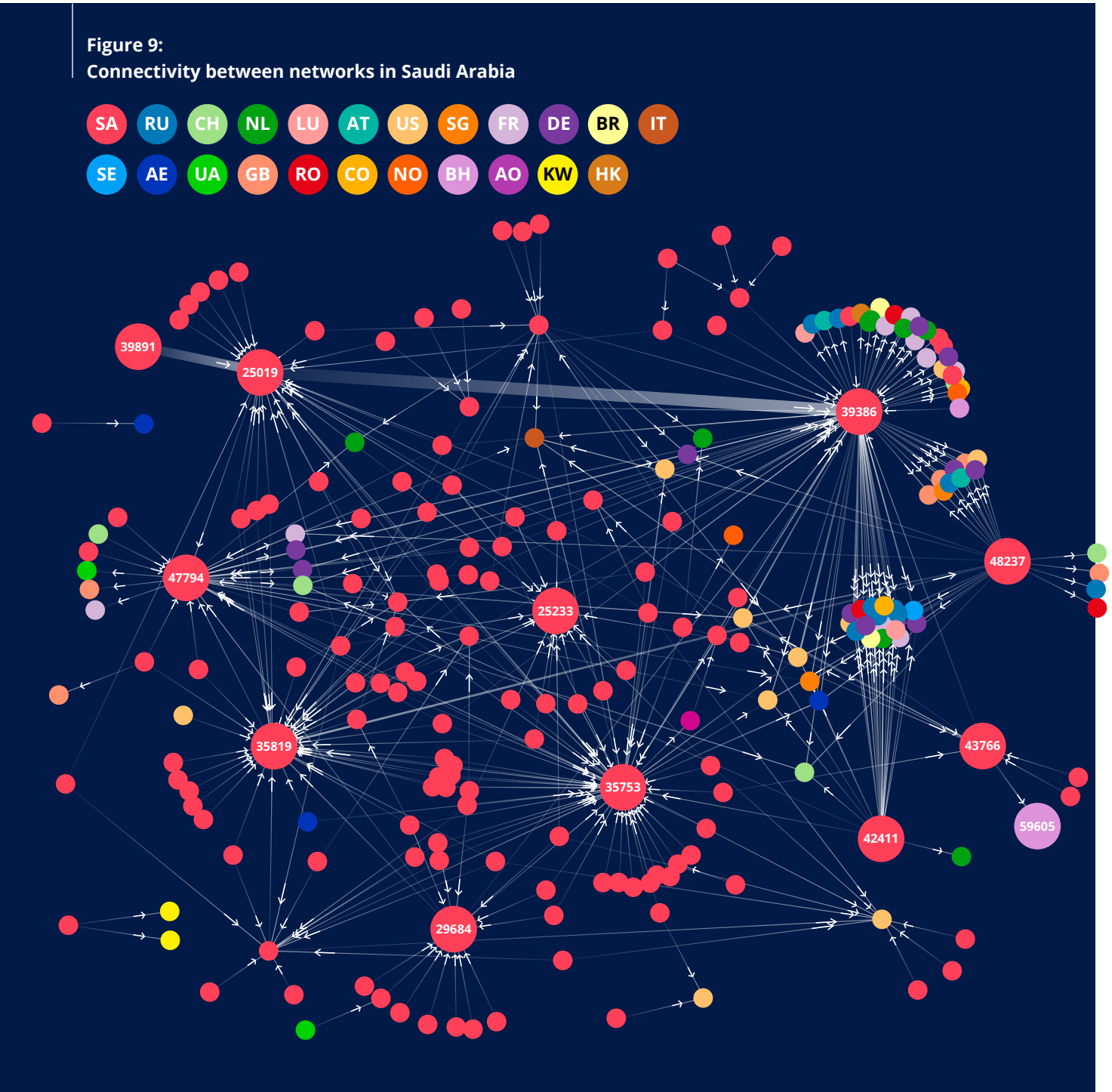
Domestic Connectivity Between Networks

To understand the relationships that exist between different networks, we can investigate the interconnections within each of the countries using data from the RIPE NCC's Routing Information Service (RIS), which employs a globally distributed set of route collectors to collect and store Internet routing data. This shows us the available paths that exist between networks (as opposed to actual paths taken).

For each country, we plot how the routes propagate from one network to another (indicated by arrows) up to the point where the path reaches a foreign network. The nodes in each figure are colour-coded according to the country in which the network (ASN) is registered, and the width of the lines is determined by the number of paths in which we see the connection between the different ASNs. Note that we only label the ASNs that we specifically mention in the text, and that the position of the different networks doesn't correspond to any kind of geographical layout; instead, these figures are merely a visual representation of the interconnections between the networks in each country.

Due to the nature of Border Gateway Protocol (BGP) and the RIS route collection processes, our view is limited to the routes followed by international traffic. We will only observe peering relationships between two ISPs in a country when one or both partners announce the other's routes to a third party which propagates the route further. Most notably, we will not see peerings at regional IXPs, where the intention is to keep local traffic within the country or region. Nevertheless, graphing the connections that we are able to see provides valuable insight into domestic connectivity.

Figure 9:
Connectivity between networks in Saudi Arabia



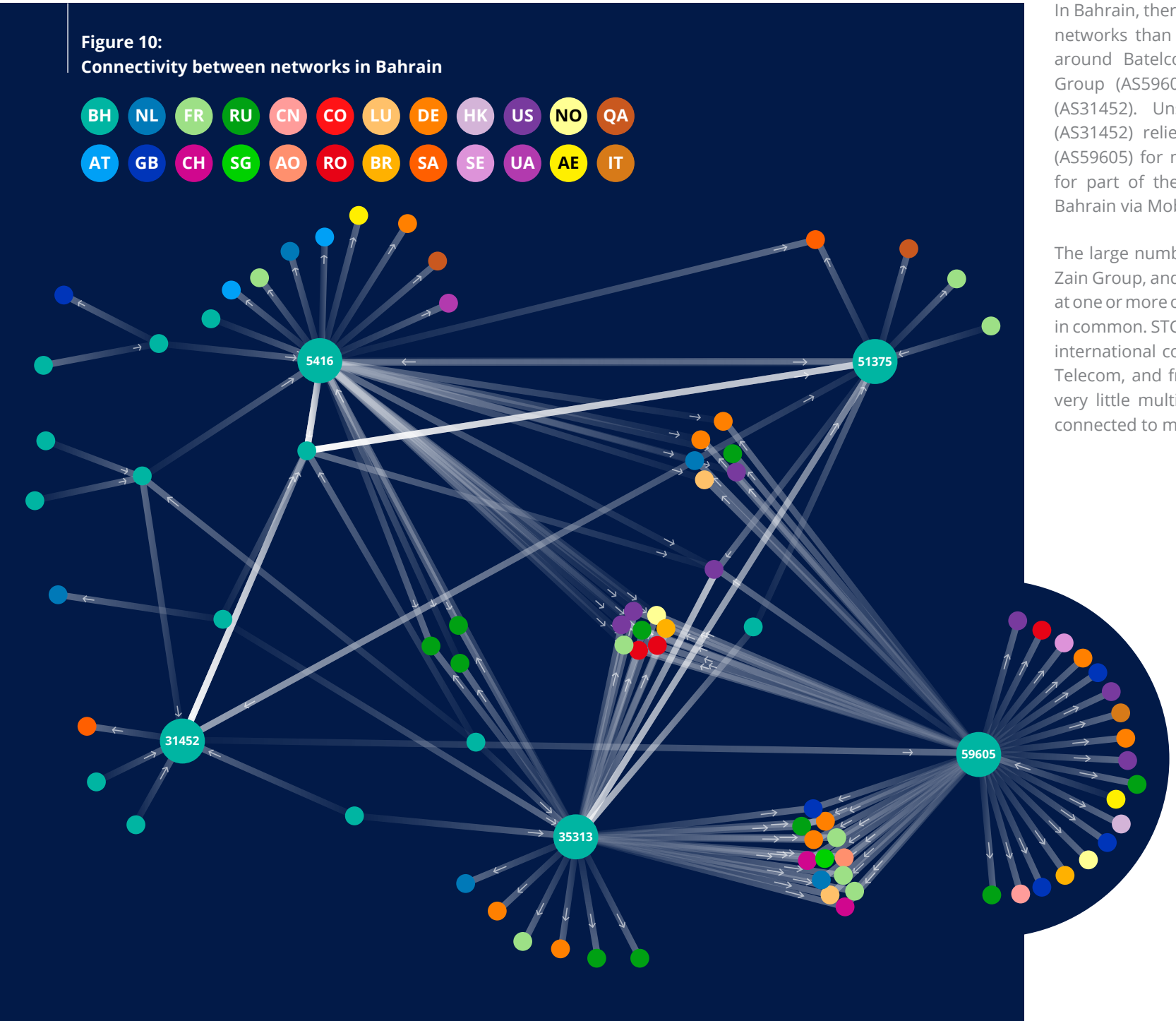
In Saudi Arabia, there is a density of networks that goes far beyond the country's number of service providers. Banks, enterprises, universities, hospitals and others are all running their own networks, resulting in a more diverse and resilient local Internet landscape.

We observe seven networks with significant clusterings around them: Saudinet (AS25019), held by Saudi Telecom (STC); STC's international gateway (AS39386); Go Telecom (AS47794); Mobily (AS35819); Arabian Internet and Communications Services (AS25233); Integrated Telecom Company (AS35753); and Nour Communication (AS29684). Many of them are multihomed to two or more providers (which generally increases resiliency or performance).

The dominant position of STC is reflected by the thick line between AS25019 and AS39386; many of the routes to Saudi IP networks in RIS follow this path. The connection between AS25019 and AS39891, which is the ASN used for STC's Mobile Network, also stands out.

In terms of external connectivity, next to Go (AS47794) and STC's gateway, there are a variety of international peers for Mobily (AS48237, connecting their AS35819 network to the rest of the world) and for TAQNIA Space Co. (AS42411). From the main providers, Zain KSA (AS43766) appears to have only one connection to the rest of the Internet. However, this one upstream, AS59605, is held by Zain KSA's parent company, Zain Group, which operates throughout the region. As we will see below for Bahrain (where Zain Group's headquarters are located), the AS59605 network is well connected via major IXPs. This set up is similar to that of Mobily and STC: one ASN for local connectivity and another to use at foreign IXPs.

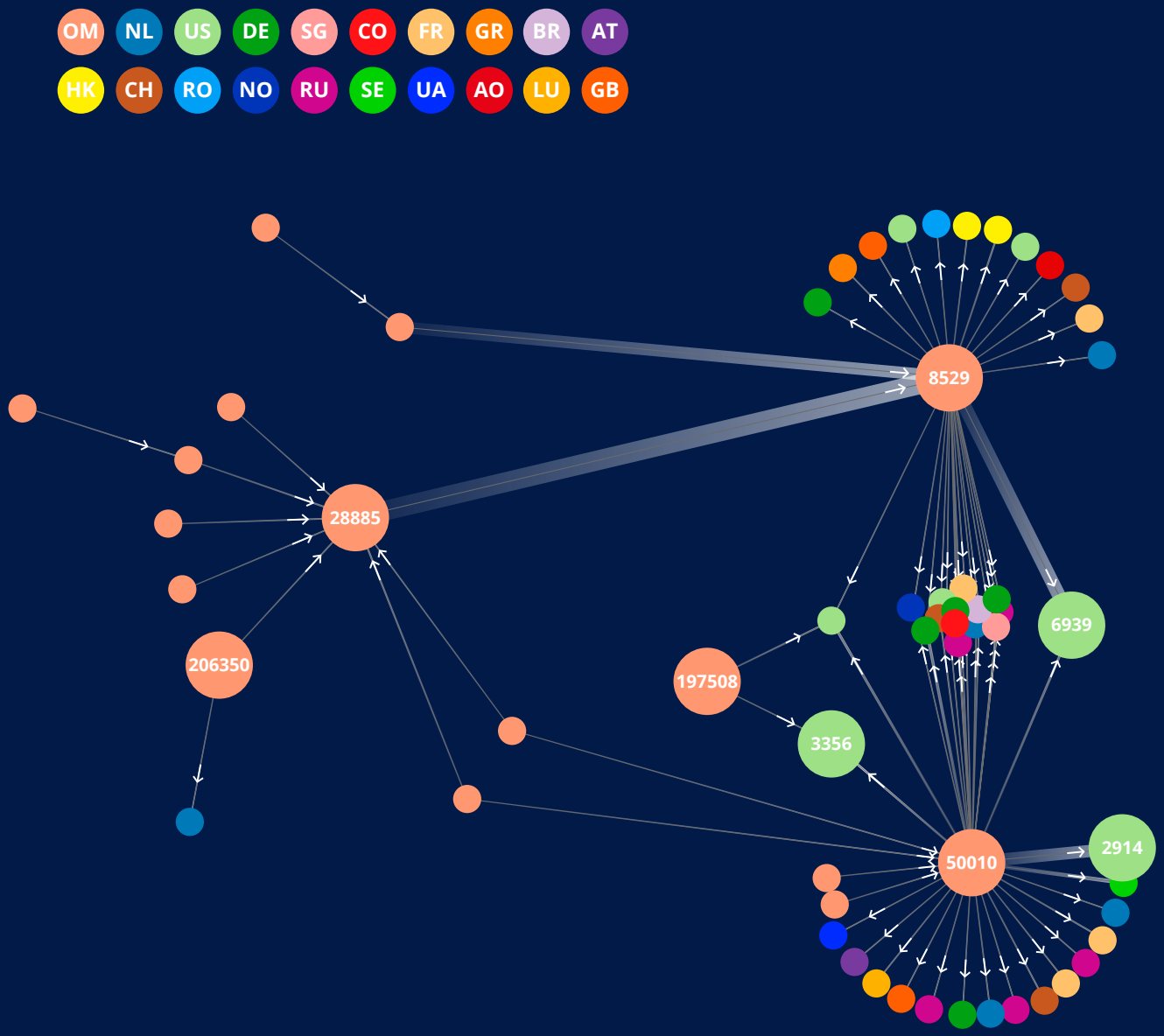
Figure 10:
Connectivity between networks in Bahrain



In Bahrain, there are fewer connections between individual networks than in Saudi Arabia. We observe five clusters around Batelco (AS5416), STC Bahrain (AS51375), Zain Group (AS59605), Infonas (AS35313) and Zain Bahrain (AS31452). Unsurprisingly, the Zain Bahrain network (AS31452) relies on Zain Group's international network (AS59605) for most of its external connectivity. However, for part of the prefixes we also observe paths to Zain Bahrain via Mobily, based in Saudi Arabia.

The large number of international connections to Batelco, Zain Group, and Infonas indicates these all have a presence at one or more of the major exchanges and have many peers in common. STC Bahrain, on the other hand, gets most of its international connectivity from its parent company, Saudi Telecom, and from Gulf Bridge International. We observe very little multihoming, with only a handful of networks connected to more than one other Bahraini network.

Figure 11:
Connectivity between networks in Oman



In Oman, we see even fewer interconnections, with three main clusters: two around networks held by Oman Telecommunications Company (Omantel) (AS28885 and AS8529) and one around Omani Qatari Telecommunications Company, operating under the name Ooredoo Oman (AS50010). The latter two networks provide almost all external connectivity in the country. Only OMREN (Oman Research and Education Network) (AS206350) and Integrated Telecommunications Oman (AS197508) do not get their external connectivity from those two main providers. We observe little to no multihoming; only two networks are seen connected to both Omantel and Oooredoo.

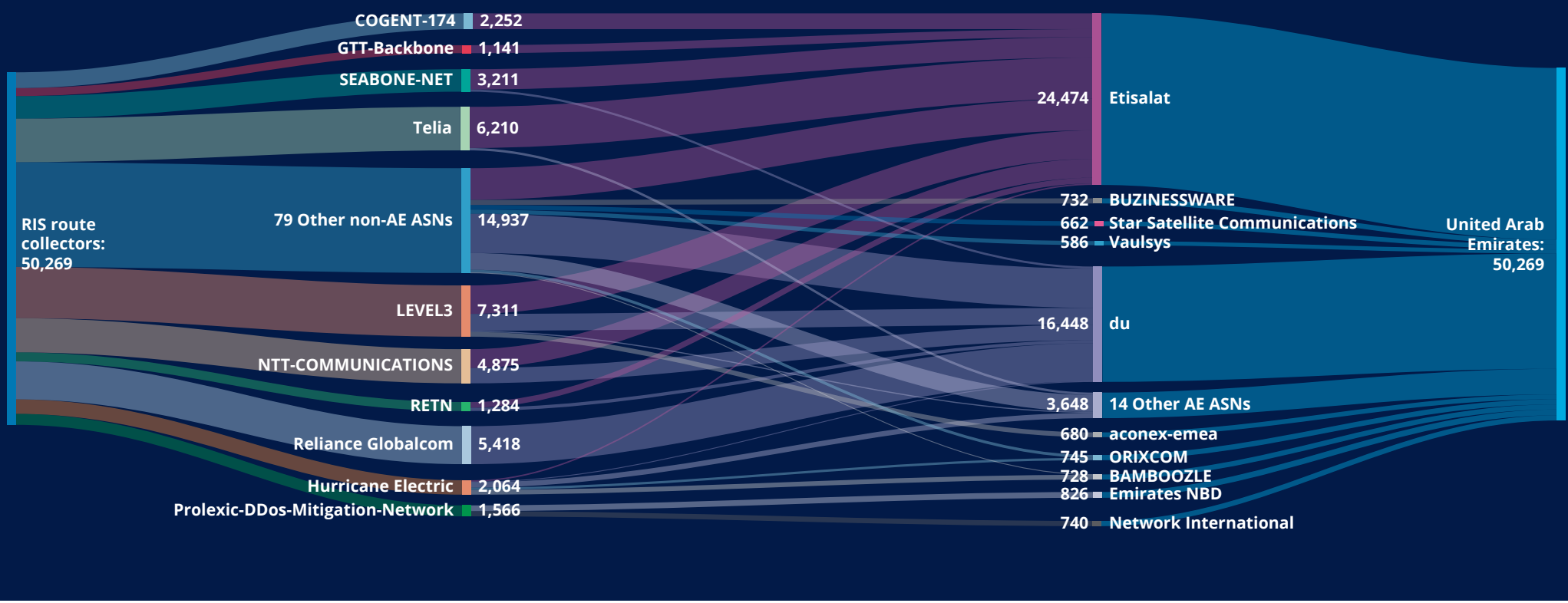
In terms of connections to the rest of the Internet, the thickness of the lines shows how Omantel was mostly seen in paths with Hurricane Electric (AS6939) as its transit provider. For Ooredoo Oman, on the other hand, NTT communications (AS2914) and Level3 (AS3356) were more important.

We included these three countries in the report as examples that span a range of different configurations and development levels; however, the corresponding figures for all eight countries are available online and include labels for all the ASNs.[5]

Overall, we see big differences in resilience between these countries. A visualisation of Internet connectivity should resemble a deeply interconnected web, with a large distribution of paths and without clear choke points or bottlenecks. Relying on a handful of networks for local and international connectivity diminishes the stability of the local Internet by creating potential single points of failure. Without more alternative paths in place, any kind of disruption with one of these networks can create a critical situation for a large number of users and services.

5 See RIPE Labs article: https://labs.ripe.net/Members/suzanne_taylor_muzzin/ripe-ncc-internet-country-report-gulf-region

Figure 12:
The United Arab Emirates' international connectivity



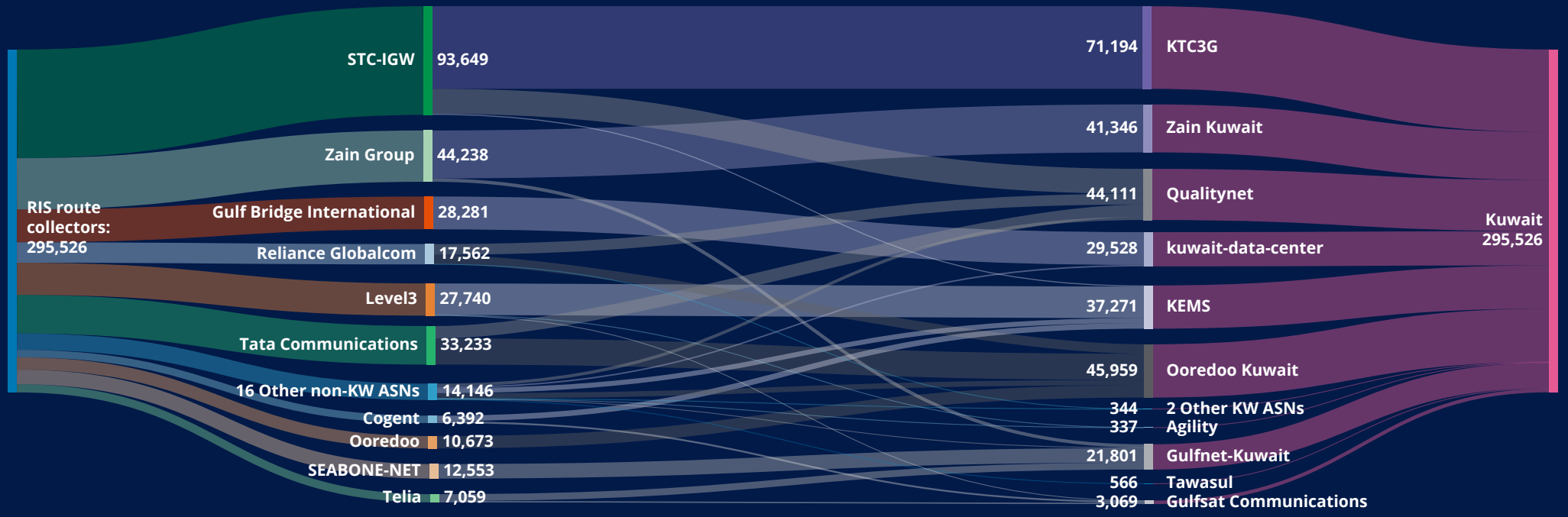
International Connectivity

Extending our view, we now look beyond domestic connectivity to examine how the Gulf countries connect to the rest of the world. To investigate this, we again turn to the RIPE NCC's Routing Information Service (RIS). We look at the routes collected by RIS for IP networks in each country and identify the last foreign and first domestic network encountered in these paths. This gives us an overview of which operators provide international connectivity into each country.

In the United Arab Emirates, Etisalat and du account for most of the country's external connectivity, and both are multihomed to large transit providers. Most Etisalat routes are provided by Telia, Level3 and NTT Communications, while Du's top three providers include Level3, NTT Communications and Reliance Globalcom. The most striking observation, however, is each provider's relatively large share of routes that pass through other external networks. This hints at a strong presence at exchange points where peers pick up announcements from du and Etisalat and pass the routes on to the RIS route collectors.

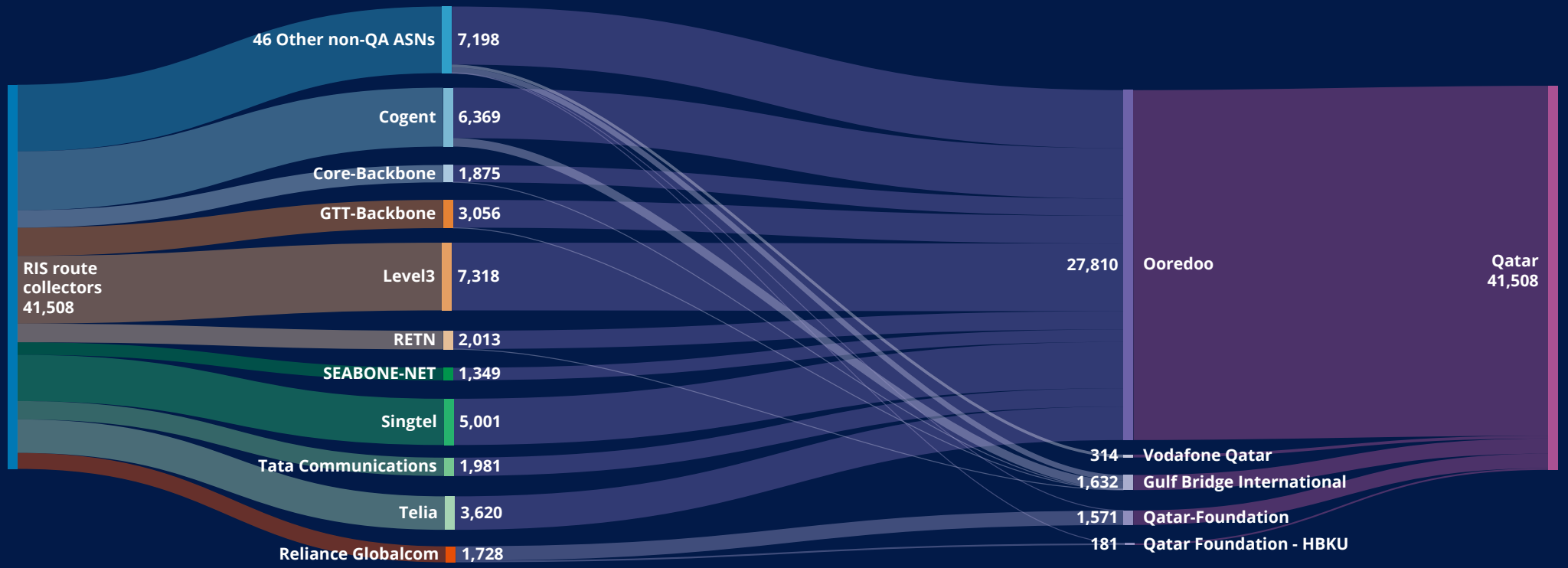
It's worth noting that, although a significant number of networks receive transit from both Etisalat and EITC, no connection is seen in the global routing data between the two providers. It's possible that the two organisations peer with each other at an IXP or other exchange, but neither are seen providing transit to the other. If they do peer with one another directly, it is only to transfer traffic between their respective customers.

Figure 13:
Kuwait's international connectivity



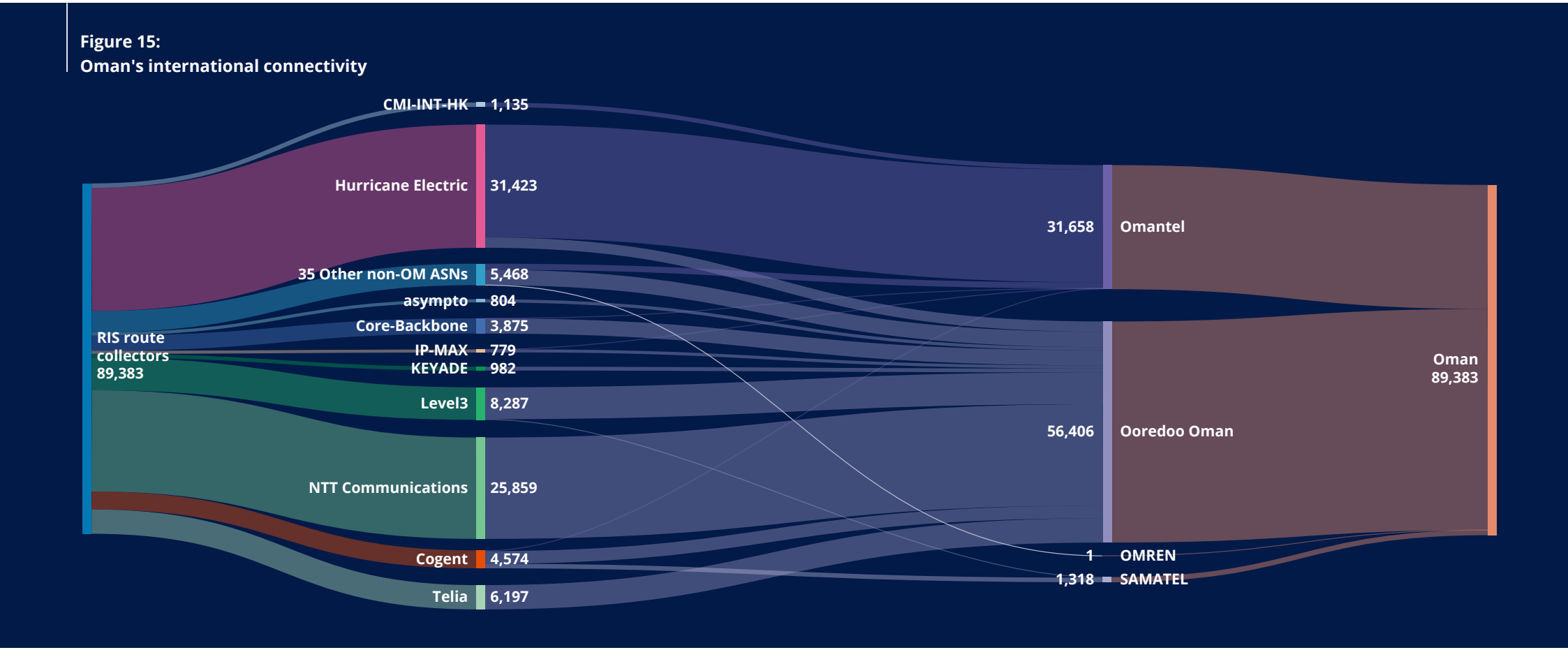
In Kuwait, we see comparable shares of routes reaching the country via Kuwait Telecom Company, Zain Kuwait, Qualitynet, Ooredoo Kuwait and KEMS. As is the case elsewhere, Reliance Globalcom, Level3 and Tata Communications are the major transit providers. But KTC, Ooredoo Kuwait and Zain Kuwait also receive transit via their respective parent companies. In fact, Zain Kuwait relies completely on the Zain Group network for external connectivity.

Figure 14:
Qatar's international connectivity



In Qatar, we see a relatively simple system with Ooredoo accounting for the vast majority of the country's external connectivity. It connects to well-known transit providers such as Cogent, Level3 and Tata Communications, and with its presence at major IXPs, it also has connections to dozens of other providers. Qatar Foundation, Gulf Bridge International and Vodafone Qatar are much smaller entry points for some of the IP networks in the country.

Figure 15:
Oman's international connectivity



In Oman, Omantel and Ooredoo Oman are responsible for almost all of the country's international connectivity. Omantel receives transit primarily from Hurricane Electric, while Ooredoo Oman relies on NTT Communications as its dominant transit provider. Both are present at major IXPs in Europe, which adds over 35 other networks that, in routing terms, are just one hop away from Oman.

Again, we included figures for the above countries as examples that span a range of different international connectivity environments, and the corresponding figures for the other Gulf countries are available online.[6]

Overall, just as with domestic connectivity, we see large differences in the resiliency of the connections that exist from the different Gulf countries to the rest of the global Internet. Relying on a small number of large, local incumbents to provide the vast majority of the connections into and out of a country creates the potential for bottlenecks and single points of failure, negatively impacting that country's Internet stability, regardless of how many upstream connections they have.

6 See RIPE Labs article: https://labs.ripe.net/Members/suzanne_taylor_muzzin/ripe-ncc-internet-country-report-gulf-region

3. Traffic Paths and Routing Security

Domain Name System Queries in the Gulf Region

Turning now to investigate how traffic is routed to, from and within the region, we first examine which local instances of K-root are queried from requests originating in the different countries.

K-root and DNS

K-root is one of the world's 13 root name servers that form the backbone of the domain name system (DNS), which translates human-readable URLs (such as https://www.ripe.net) into IP addresses. The RIPE NCC operates the K-root name server. A globally distributed constellation of these root name servers consists of local "instances" that are exact replicas. This set-up adds resiliency and results in faster response times for DNS clients and, ultimately, end users.

These measurements are based on the RIPE NCC's RIPE Atlas measurement platform, which employs a global network of probes to measure Internet connectivity and reachability. Many of the countries covered in this report have only a few RIPE Atlas probes connected. Having more volunteers who connect RIPE Atlas probes throughout the region could possibly give different results and, in any case, would provide a more detailed picture (see the section on RIPE Atlas at the end of the report for more information about how to get involved).

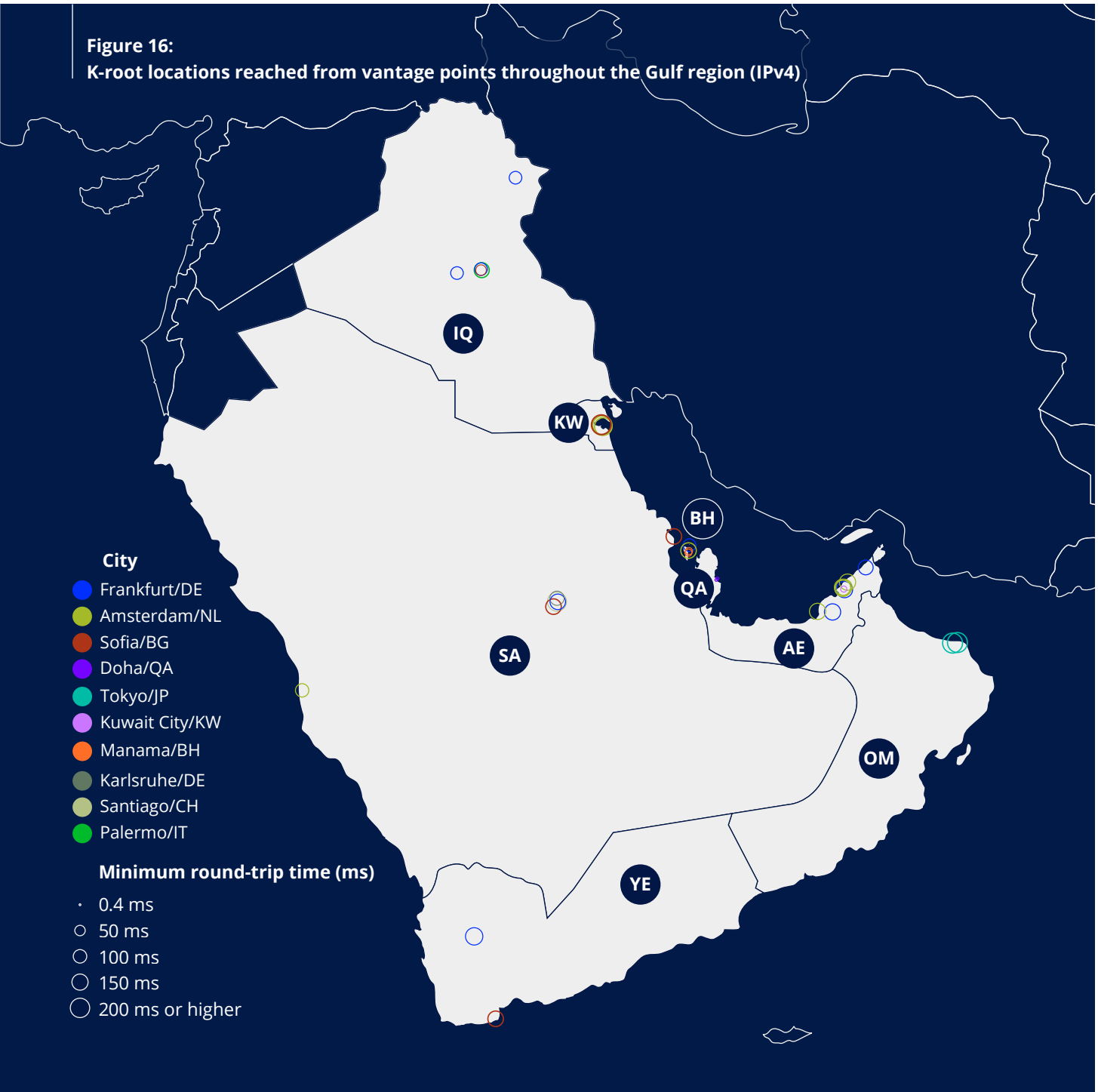
Regardless, we include the data that we were able to collect here. Examining the choices that different RIPE Atlas probes in the region make about which K-root instance to query provides some insight into how the routing system considers the various options and decides which networks and locations will provide the best results when the Internet is left to itself to make such decisions. This in turn offers some insight into what small to medium networks could expect in providing regional services, while bigger, more established players often work out direct peering and caching arrangements to optimise their routing.

Border Gateway Protocol and Anycast

The K-root name server, like many other DNS servers, uses a technique called anycast whereby each individual instance of K-root is independently connected to the Internet via a local Internet exchange point or any number of upstream networks available at its location. Each instance communicates using the Border Gateway Protocol (BGP), which is designed to select the best path out of all the available options. Initially, the most important criterion is path length, and the system will choose the path with the lowest number of intermediary networks. However, network operators can override the BGP decision-making process, often for reasons relating to costs or ownership. It is not uncommon for networks to prefer routes that may be longer but are less expensive due to peering arrangements via an Internet exchange point or a parent company.

Although the region hosts five K-root instances (two in Kuwait and one each in Doha, Manama and Riyadh), we can see that the vast majority of queries originating in the Gulf region are sent instead to instances in Frankfurt, Amsterdam and London. This could be the result of suboptimal routing as well as the policy of the organisation hosting the K-root instance, which may not be announcing the route widely to their peers or upstream providers.

Figure 16:
K-root locations reached from vantage points throughout the Gulf region (IPv4)



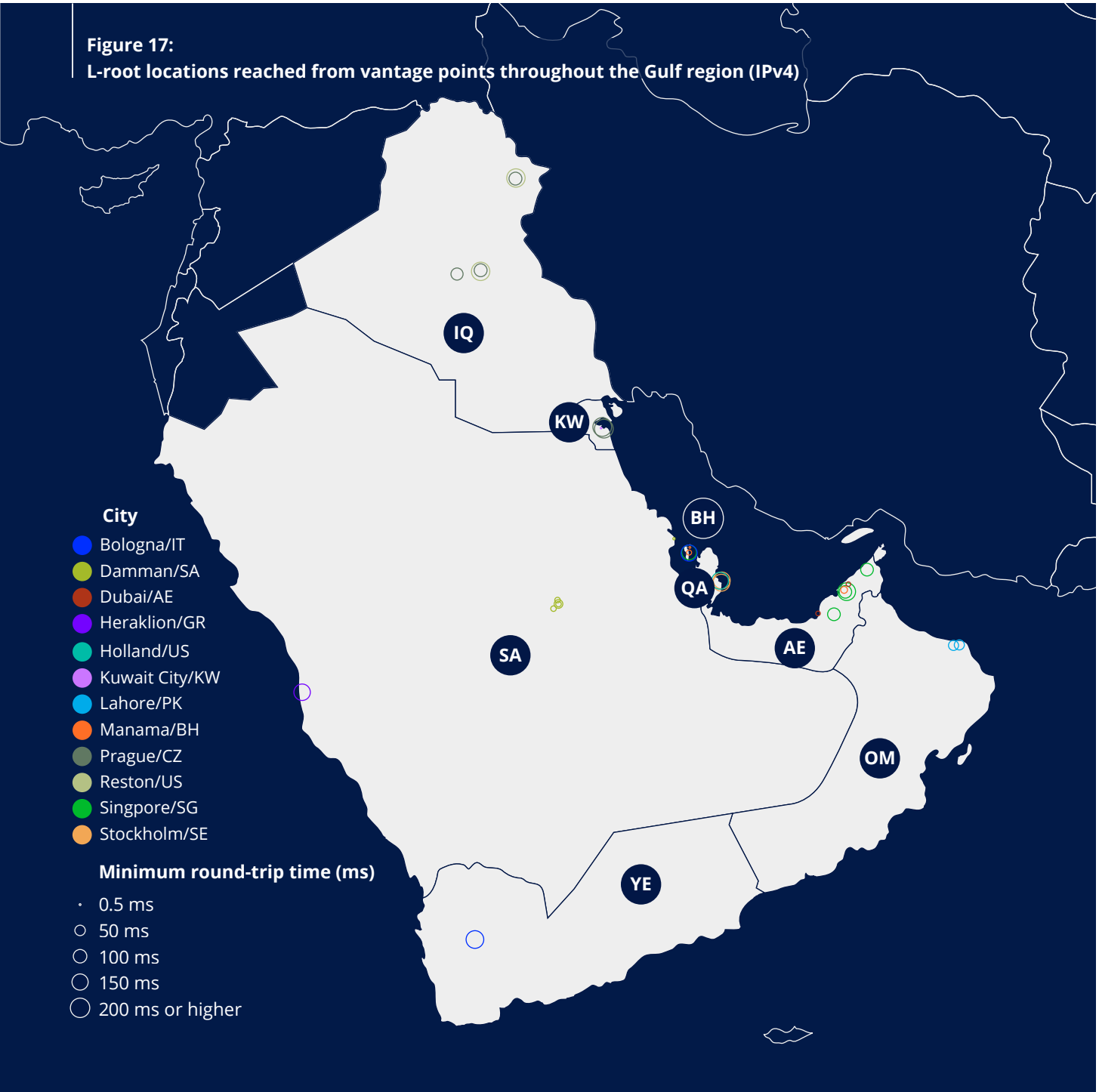
Looking at individual RIPE Atlas probes in the different countries, we see the different K-root instances queried by the probes, along with the resulting round-trip times, in figure 16. (Note that we performed many measurements per probe, and the round-trip times shown are the lowest that we observed across all measurements.)

Almost all the probes in the United Arab Emirates preferred to query K-root instances in Amsterdam and Frankfurt rather than those in Kuwait, Manama, Doha or Riyadh. Similarly, probes in Saudi Arabia predominantly queried instances outside of the region – with quite a few reaching Sofia in addition to Amsterdam, Frankfurt, Karlsruhe in Germany, and even Santiago – compared to the number that reached the instance in Kuwait. Interestingly, on the day of our measurements, none of the queries originating in Saudi Arabia were sent to the instance in Riyadh.

Only one of the five probes in Kuwait reached the instance in the country while the others were sent to Amsterdam and Sofia. Kuwait is a good example of how much faster response times are when querying the local instance rather than those farther afield. Probes in Oman relied exclusively on an instance in Tokyo, resulting in a round-trip time of over 200ms. Only in Qatar do we see all queries being sent to the local instance in Doha.

As stated previously, K-root is just one of the world's 13 root name servers, and every domain name system (DNS) client will make its own decisions about which particular root name server to use. In cases where response times to K-root would be relatively slow, it is highly likely that clients would opt for faster alternatives among the other root name servers. We therefore also looked at how probes in the Gulf region reached L-root, another of the world's 13 root name servers, which is operated by ICANN.

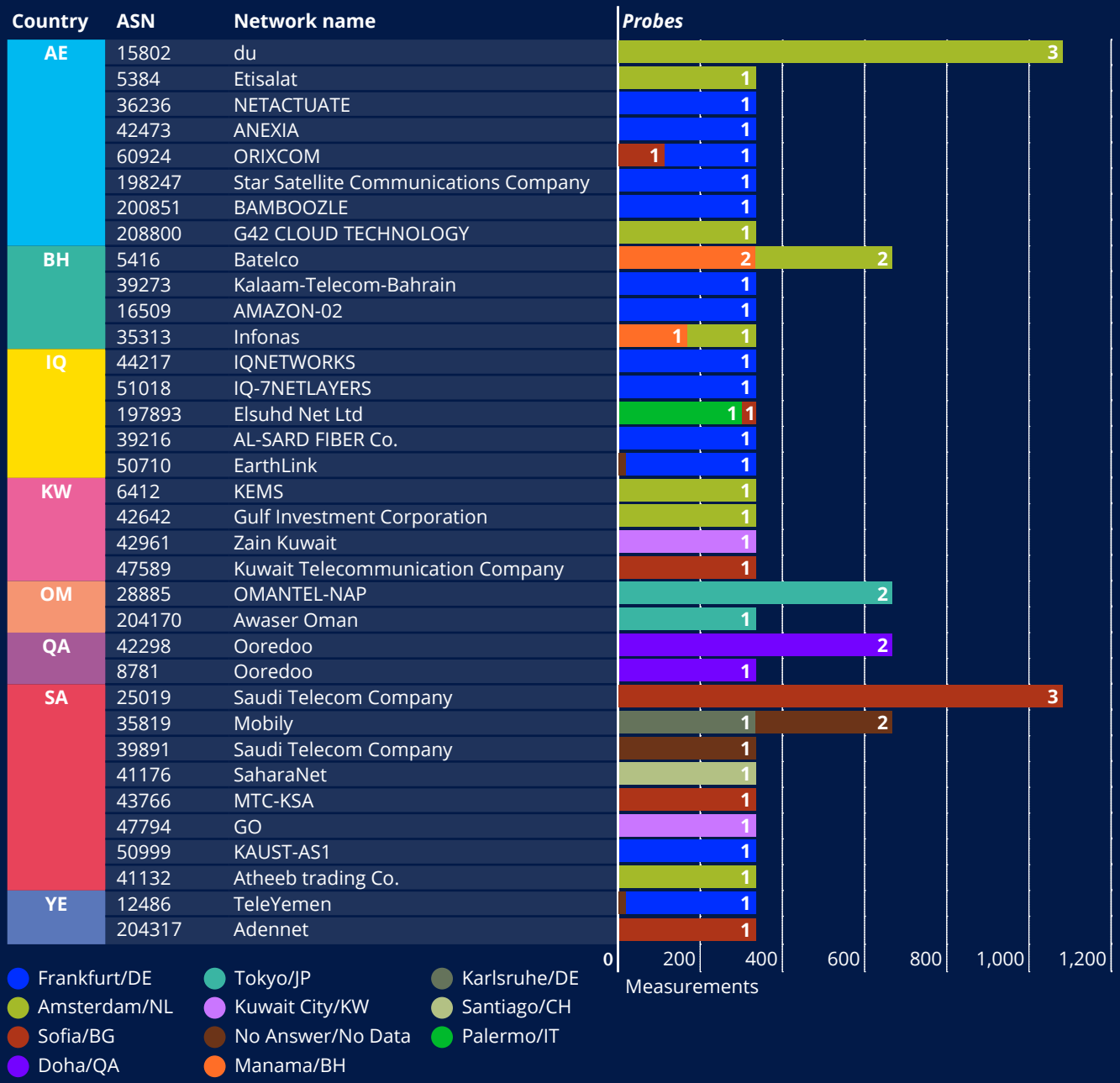
Figure 17:
L-root locations reached from vantage points throughout the Gulf region (IPv4)



With L-root, we see more probes reaching the instances that exist in the region. A high volume of requests are consistently sent to those in Manama, Damman and Dubai, although we also see a large number of queries being sent to Prague.

When looking at the results in each country, nearly half of the queries in Iraq were sent to the US, with the remainder querying instances in Prague. All queries originating in Oman were sent to Lahore rather than a regional instance, while queries in Qatar reached the US and Stockholm. Far fewer queries in the United Arab Emirates were sent to the instance in Dubai than those in Manama and Singapore. In Bahrain, quite a few queries were sent to the local instance in Manama, although just as many were sent to Bologna and others to Singapore. Also of note is that, in September 2020, one probe in Bahrain queried the L-root instance in Manama, but with a rather high round-trip time of 110ms, suggesting that packets left the country and took a detour to Europe before returning.

Figure 18:
K-root locations reached from different networks throughout the Gulf region (IPv4)



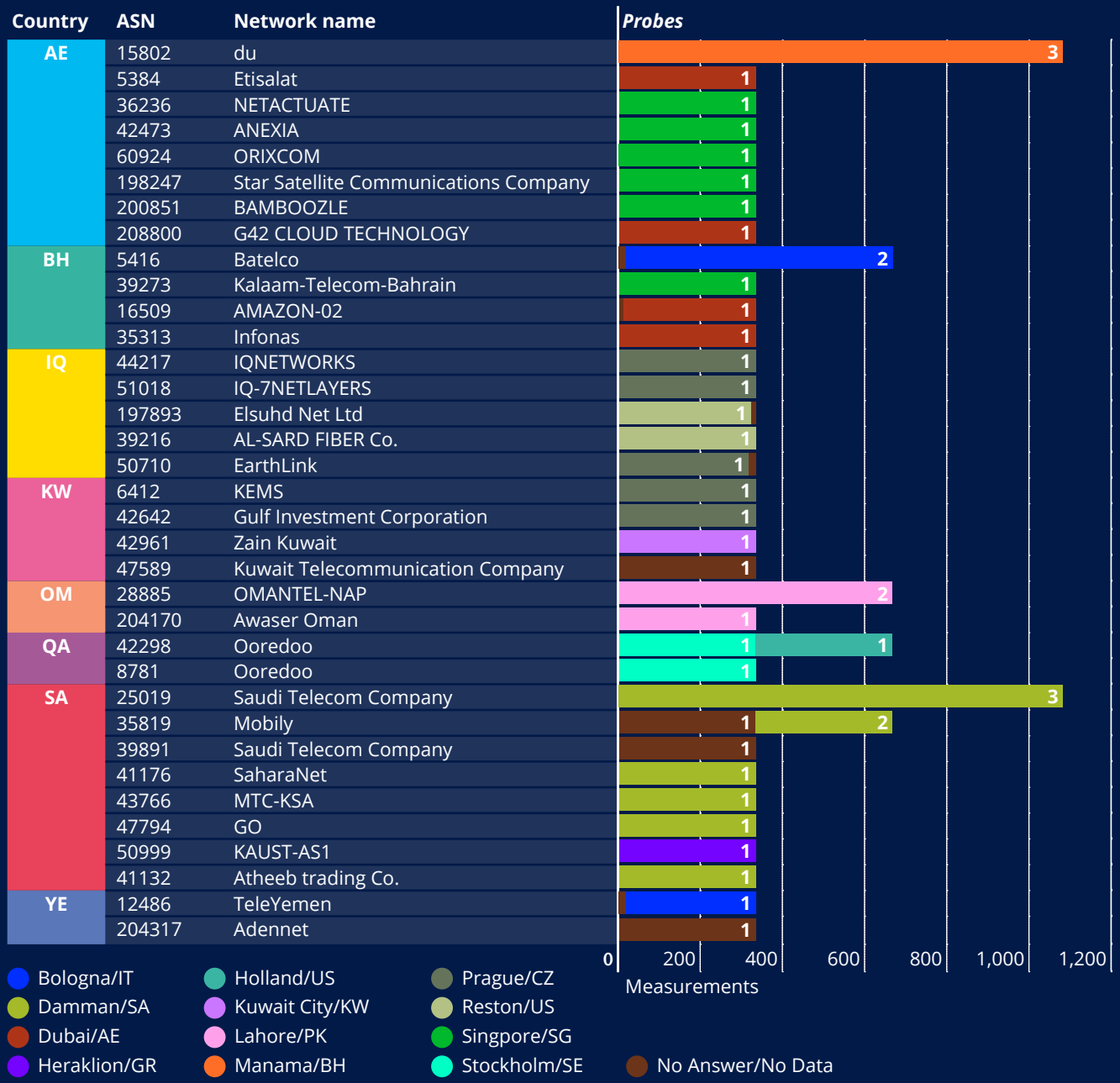
We can also look at which K-root and L-root instances are queried by probes in different networks, as opposed to different countries. Traditionally, the Border Gateway Protocol (BGP) decision-making process would ensure that once a particular path has been identified as being the best option, there is consistency across all the routers that are part of that particular network. Indeed, this is very much what we see in figures 18 and 19, where almost all the probes in a given network end up querying the same K-root and L-root instances.

A few exceptions include a network in the United Arab Emirates (Orixcom) that reached K-root instances in both Kuwait and Frankfurt. Another is the two probes in Batelco in Bahrain, both of which queried the local K-root instance in Manama and an instance much farther away in Amsterdam. Kalaam-Telecom in Bahrain also reached these two instances on the day of our measurements, possibly indicating that it went through Batelco to reach K-root. Finally, a network in Iraq (Elsuhd Net Ltd.) reached an instance in both Palermo and Sofia.

Comparing overall access to K-root versus L-root for the 38 probes, we found that 18 of them had shortest round-trip times to K-root and 19 of them had shortest round-trip times to L-root. (One probe had mixed results.)

It's worth noting that the shortest path (from a routing perspective) for a network in the Gulf region to a root name server might well be through Amsterdam or Frankfurt, if the network operator peers at one of the exchanges in those locations (and we know that many Gulf operators are present at those exchanges). Smaller operators generally have less control over their routing and will be more affected by the routing policies of their upstream providers, unless they make their own peering arrangements and individual routing decisions.

Figure 19:
L-root locations reached from different networks throughout the Gulf region (IPv4)



We should also note that these results, while considered generally representative, offer only a snapshot of measurements made on a single day in November 2020. Given BGP's dynamic nature, results can change constantly due to subtle changes in routing.

Regional Traffic Exchange

The Gulf region has seen an increase in the number of Internet exchange points (IXPs) in recent years. Bahrain, Kuwait, Saudi Arabia and the United Arab Emirates each have at least one operational IXP, while Iraq, Oman and Yemen are developing peering and interconnection frameworks.

These IXPs are governed and financed according to different models, with some being state-led and operated, such as Saudi-IX (SAIX) and Kuwait-IX (ix.kw), while others are operator-driven, such as Batelco's Manama-IX (MN-IX), STC's Jeddah exchange (JEDIX), and Etisalat's SmartHub IX, all of which are owned and operated by those providers.

Some have more of a commercial approach and have partnered with European IXPs for their operations, such as Dubai's UAE-IX partnering with DE-CIX in Germany, MN-IX partnering with AMS-IX in the Netherlands, and JEDIX partnering with LINX in the UK. Still others operate as non-profits, including ix.kw and the Qatar Internet Exchange (QIX.qa).

Again using data from the RIPE Atlas measurement network, we can investigate how some of the networks in the region exchange traffic with each other, and get some indication of where those exchanges take place and what role the local IXPs play in the region. For this experiment, we performed traceroutes from each RIPE Atlas probe to every other probe in the region. Because those measurements disclose the IP addresses of the routers involved, we then used RIPE IPmap to geolocate those network resources. This gives some insight into the paths available to traffic, although it does not directly measure traffic.

Figure 20:
In-region traffic paths

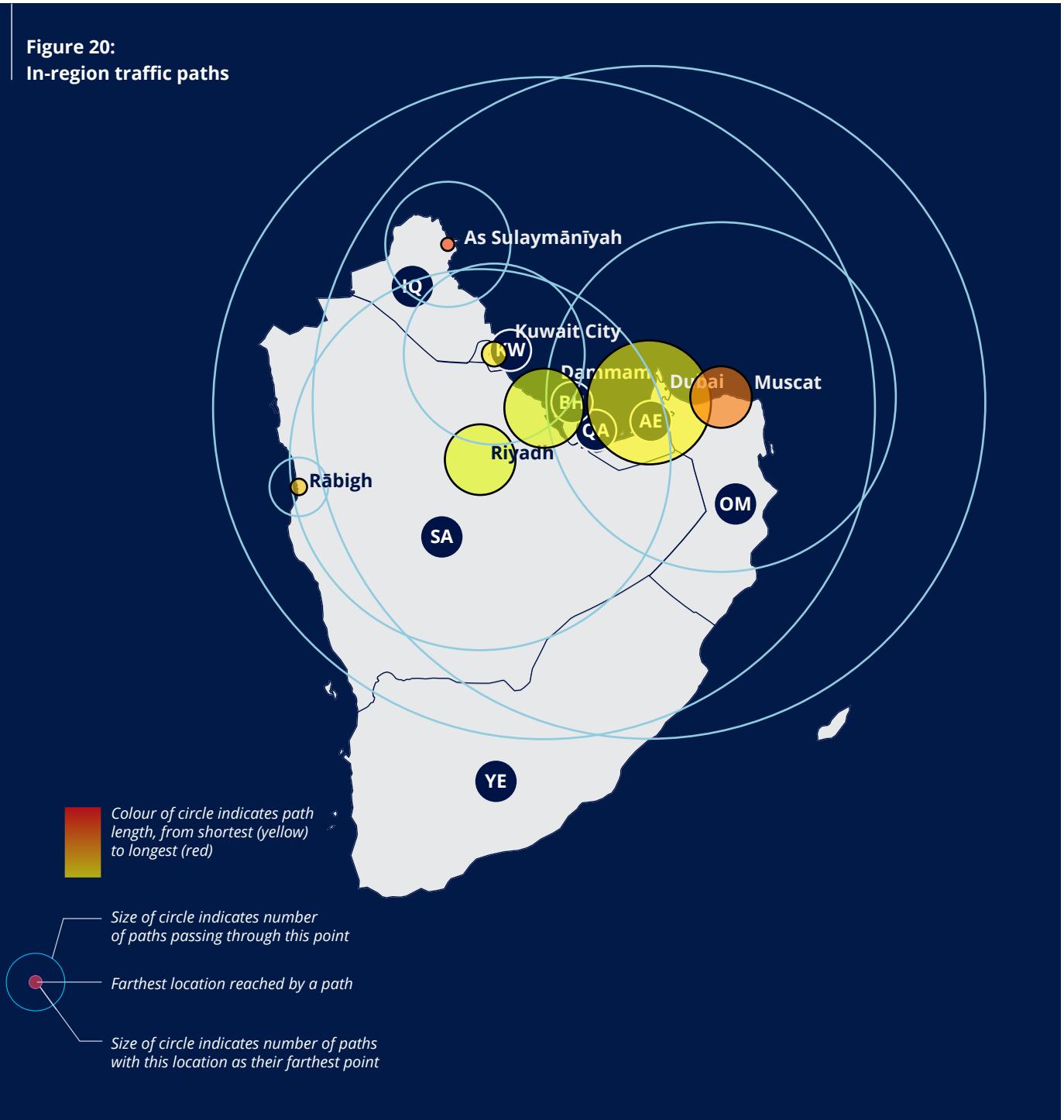


Figure 20 shows the results of these measurements only for the paths that stayed within the Gulf region, with the size of the outer circles representing the number of paths passing through the points at their centres.

We can see a large number of paths centred around Dammam and Dubai, indicating that a high volume of traffic is likely being exchanged there. Riyadh and Muscat also seem to act as lesser exchange points. As indicated by the colour of the inner circles, we can see that the different points all offer comparable path lengths (and, by extension, response times), with paths via Muscat being slightly longer.

Figure 21:
Out-of-region traffic paths

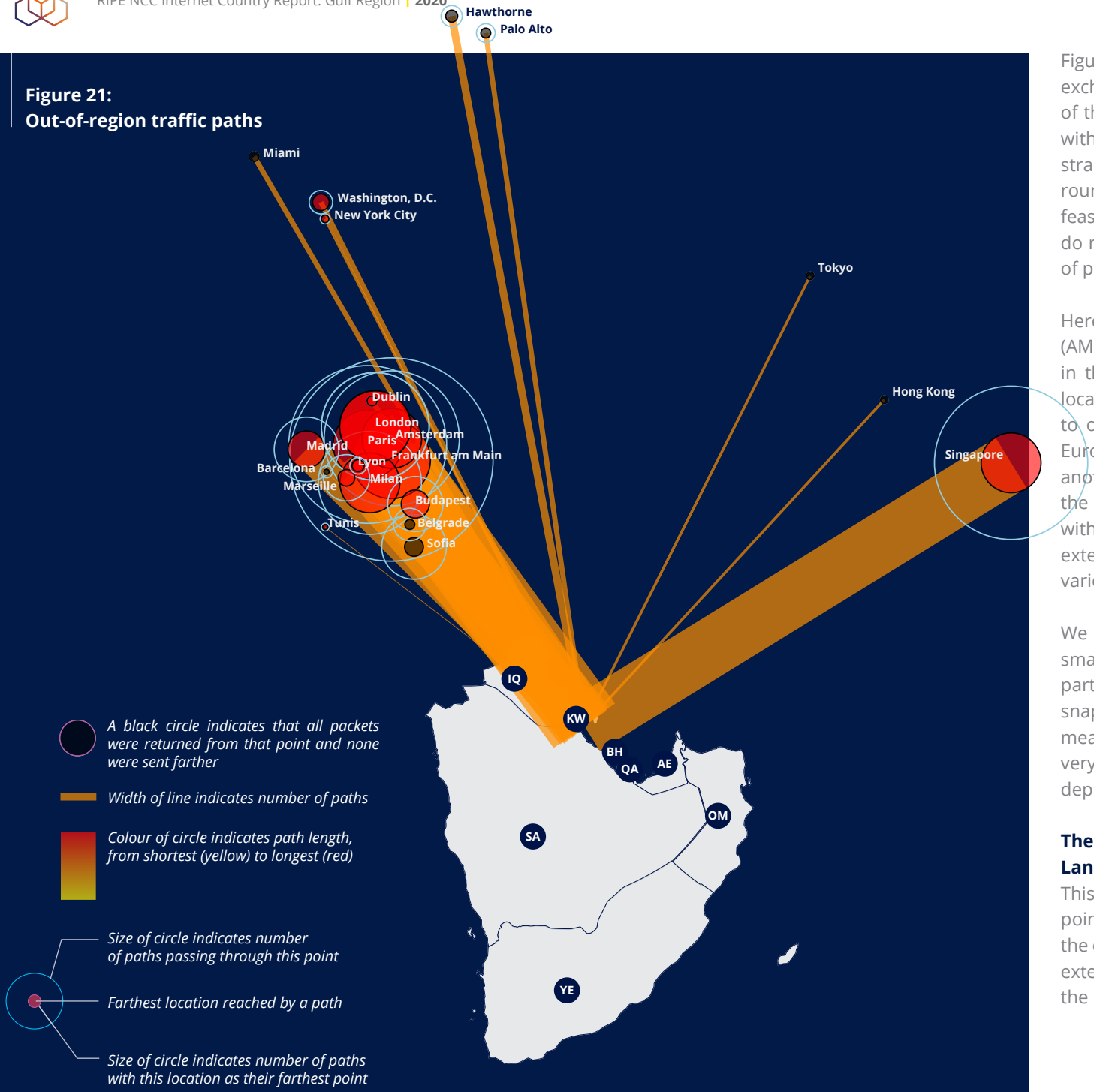


Figure 21 extends the view to look at where traffic might be exchanged outside of the region (note that the placement of the paths' origin is simply meant to represent an origin within the Gulf region). Ideally, paths should travel in a straight line from end user to end user, in order to reduce round-trip times. In reality, however, this is almost never feasible. Although figure 20 showed that some traffic paths do remain within the region, there is a significant number of paths extending to much more distant locations.

Here we see the influence of foreign IXPs in Amsterdam (AMS-IX) and Frankfurt (DE-CIX), but we also see networks in the Gulf region using tier-1 transit networks in these locations, as well as in London and Paris. It's interesting to observe providers in the Gulf region preferring these European exchanges, or preferring to peer with one another via transit in these locations, rather than using the exchanges that exist within the Gulf region or peering with one another directly. We can also see that some paths extend all the way to Tokyo, Hong Kong, Singapore and various exchange points in the US.

We should note that these figures are based on a small number of measurements that were taken at a particular point in time and therefore offer only a limited snapshot of the situation. However, we would expect that measurements taken at any other time would likely offer very similar results. Again, having more RIPE Atlas probes deployed in the region would produce more robust results.

The Effect of Routing Behaviour on the Internet Landscape

This behaviour of routing packets a long way to an exchange point, only to have them travel back to a destination close to the origin, is referred to as "tromboning". The farther a path extends from the origin/destination, the more inefficient the path is. In this particular case, delays from detours as

distant as the US and Asia will not be minimal, although how noticeable this is to an end user would depend on their activity.

These detours generally increase costs for the network operator and, more importantly, the additional distance travelled unnecessarily increases the risk of disruptions. It also creates additional dependencies on external suppliers – many of which reside in foreign jurisdictions that may not have legal frameworks that are compatible or compliant with local regulations – potentially causing issues with data sovereignty.

While some Gulf countries lead the world in indicators such as mobile penetration[7] and Internet speeds[8], the region's peering landscape lags far behind, with most traffic being sent far outside the region rather than making use of the several exchange points that have been established in recent years.

The approach to Internet peering and interconnection throughout the Gulf region clearly remains national, rather than regional, in scope. With few exceptions, it's rare to find operators from multiple countries peering at most of the region's IXPs, unless there is a local licensed subsidiary in the country through which they peer. This continues despite the well-documented benefits to the entire Internet ecosystem when traffic is exchanged across local or regional IXPs, including the economic benefits of much wider market exposure, lower costs for end users, faster connections, better user experience, and improved resiliency.

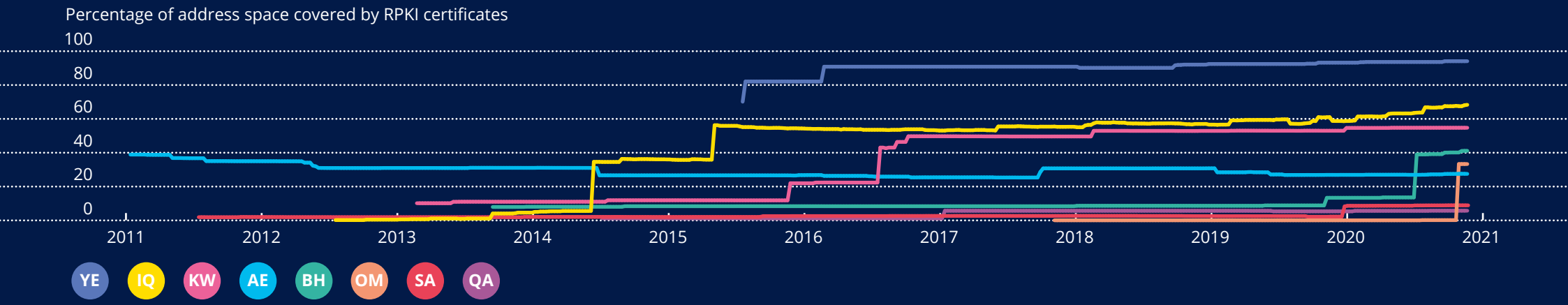
Routing Security

Beyond looking into the different routes available to traffic originating in the region, we can also investigate routing security in the Gulf countries by looking at how effectively IP address space is protected by Resource Public Key Infrastructure (RPKI), a security framework that helps network operators make more secure routing decisions.

RPKI uses digital certificates to prove a resource holder's right to announce IP prefixes (i.e. certifying that the resources were allocated or assigned to the resource holder by a Regional Internet Registry). This helps avoid the most common routing error on the Internet: the accidental announcement of an IP prefix by someone who is not the legitimate holder of that address space. Using the RIPE NCC's RIPEstat tool – which provides all available information about IP address space, ASNs, and related information for hostnames and countries – we can see what percentage of a country's IPv4 address space is covered by RPKI certificates.

7 See figure 6 in this report
8 The United Arab Emirates, Qatar and Saudi Arabia are among the top 10 countries in mobile speeds: https://www.speedtest.net/global-index

Figure 22:
IPv4 address space covered by RPKI



Again, the numbers vary significantly from country to country, with more than 50% of the address space in Yemen, Iraq and Kuwait covered. For the address space in other countries, including Saudi Arabia and Qatar, there's almost no coverage, while operators in Bahrain and Oman have started using RPKI only recently. (It's worth noting that having fewer IP prefixes and LIRs makes it easier to achieve higher percentages, as fewer certificates need to be created to cover the address space.)

Creating certificates is an important first step in protecting against accidental incorrect route announcements and intentional hijacks. However, for this to be effective, networks around the world also have to reject routes with invalid origins so that the bad announcement isn't propagated through the routing system. In 2019, the RIPE NCC launched RPKI Test[9], a web-based tool that lets users verify whether their network can reach a destination that is announced with an invalid origin Autonomous System in BGP (which, ideally, should not be possible).

We conducted several tests using RIPE Atlas probes to determine whether we could reach prefixes with invalid origins, and which should therefore theoretically be unreachable. (We also safeguarded against the possibility of the prefixes not being reachable because of wide-scale network problems by including a measurement to an address in the same network that is covered by a valid certificate to ensure it could be reached.)

In the first test, we targeted the two prefixes that are also measured in the RIPE NCC's RPKI Test (which are provided by NTT Communications). We saw six networks for which, almost every time we measured, the destination with the invalid certificate was unreachable, as desired. However, given that the destinations are located far away in the US, we cannot determine whether it is the local network hosting the probe that is filtering prefixes with invalid certificates, or whether the network's transit provider is responsible for the filtering.

To check this, we also ran measurements against two targets that Cloudflare has made available. As these are anycasted (i.e. announced from various geographical locations at the same time), transit providers shouldn't have as much influence. The results showed that the networks that were not able to reach the destination prefix with an invalid certificate *could* reach the Cloudflare targets covered by invalid certificates. The only one for which some doubt remains is MTC KSA (AS43766), for which about 50% of the measurements could not reach the invalid prefix. These results suggest that the filtering we saw taking place in the first test was likely the result of the transit providers, and that the networks we measured (those with RIPE Atlas probes) are not using RPKI validation.

Governments in the region, along with the larger service providers, could help encourage smaller players to certify their Internet number resources and share best current operational practices around routing security in general in order to better safeguard the Internet and reduce the opportunity for bad actors to hijack resources and attack the routing system.

9 https://labs.ripe.net/Members/nathalie_nathalie/rpki-webtest

Conclusion

The Internet landscape in the Gulf region has experienced tremendous growth in a relatively short period of time. Although markets were later to develop than in parts of the world like Europe and North America, the region has prioritised digitisation and made huge strides in achieving its digital transformation goals. Governments and service providers have each had a role to play. Removing regulatory barriers has made it easier to establish Internet exchange points and deploy IPv6. A more diverse field of service providers are acquiring Internet address resources and running their own networks.

However, the full potential of a healthy, competitive digital landscape cannot be fully realised until a number of further developments take place. It's important for players of all sizes to obtain Internet number resources that fulfill their needs and to protect those resources using best practices in routing security, to understand the importance of deploying IPv6 on their networks to accommodate future growth into new types of online services, to strengthen both their domestic and international connectivity and to build a healthy interconnection environment that includes peering at the IXPs in the region.

A significant number of paths extend far outside of the region and access to the domain name system does not take advantage of local root name server instances. Improving routing policies would result in decreased latency, lower costs, better user experience, and less dependency on foreign infrastructure.

Countries within the Gulf region vary in terms of their access to the rest of the global Internet, although this generally relies on a handful of operators providing connectivity for entire countries. Again, more interconnections would improve diversification, giving players more options and access points, while bolstering redundancy and resiliency.

It's worth noting that all of the observations in this report are based on active paths, and we cannot know what "hidden" world of backups exists that would automatically take over in the case of any disruptions. Whatever redundancy does exist would provide the system with more resiliency.

Many of the findings in this report are based on data that the RIPE NCC has collected through its RIPE Atlas measurement platform, which is significantly limited in many of the countries in the Gulf region. Having more volunteers install RIPE Atlas probes in the region would allow for substantially more robust data and analysis.

We encourage governments and operators in the region to take a more collaborative approach to improve overall interconnectivity, and make use of the regional resources in place, such as root name instances and Internet exchange points. At the same time, we would encourage operators to focus not just on routing optimisation, but routing security, as RPKI uptake could also be improved in the region. As we've seen throughout this report, the digital landscape is changing and is no longer the sole domain of large incumbent service providers. We rely on Internet connectivity more than ever before to keep our economies and societies thriving. Governments need to adapt to this changing environment through open and flexible regulation that supports growth.

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.

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 https://www.ripe.net

RIPE Atlas

RIPE Atlas is the RIPE NCC's main Internet measurement platform. It is a global network of thousands of probes that actively measure Internet connectivity. 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) has been collecting and storing Internet routing data from locations around the globe since 2001.
https://www.ripe.net/ris

The data obtained through RIPE Atlas and RIS 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. Please see the RIPE Atlas and RIS websites to learn more.

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