

Unlocking Digital Growth: **The role of Internet Exchange** **Points (IXPs) in South East Europe**



Table of Contents

Executive Summary	2
Background	3
1. Keeping local traffic local	7
1.1 Connecting service providers for seamless traffic exchange	7
1.2 Content localisation	13
2. Fostering local interconnection for developing a digital economy	15
2.1 Open and inclusive membership policies	15
2.2 Who should connect at the IXP?	16
2.3 Cultivating a collaborative knowledge ecosystem	18
3. Attracting global hyperscalers and content providers	20
4. Becoming a hub for exchanging regional traffic	24
4.1 Enhancing regional and global digital connectivity	24
5. Summary and future outlooks	29
5.1 Looking ahead	29
5.2 Recommendations from the field	29
Appendix 1 - Operator matrix (March 2025)	31
Appendix 2 - Content matrix (March 2025)	32

Executive Summary

This report focuses on the Internet Exchange Point (IXP) landscape in South East Europe (SEE). We examine the role IXPs play in the peering and interconnection ecosystem and apply our four established criteria for assessing IXP success:

1. Keeping local traffic local
2. Fostering local interconnection to support the digital economy
3. Attracting global cloud and content players
4. Becoming hubs for regional traffic exchange

IXPs in the SEE region vary significantly in both maturity and scope. While IXPs have been widely deployed across SEE, their stages of development differ widely: the oldest was established three decades ago and many started in the last decade. Their functional roles also diverge, ranging from exchanges that focus on their “core” function of facilitating local traffic exchange to larger hubs serving as regional interconnection points.

Their development is also shaped by diverse governance models. Some exchanges operate as small-scale initiatives led by research centres and universities, while others have grown into successful commercial businesses reflecting differing perspectives on the role and purpose of an IXP.

Since IXPs in the region serve varied purposes, no single exchange is expected – while possible – to meet all of these objectives. Nonetheless, this report provides a practical benchmarking framework to help policymakers, decision makers and operators assess IXPs not just as technical facilities, but as critical assets in the region’s digital economy.



Background

For the purpose of this report, we chose the geographical definition of South East Europe that includes: Slovenia, Croatia, Bosnia and Herzegovina, Serbia, Montenegro, Albania, North Macedonia, Kosovo*, Bulgaria, Romania and Greece.

While the region shares many commonalities, it is important to acknowledge that it is not homogeneous. Emerging differences include EU and non-EU membership, population size and distribution, terrain (such as access to the sea versus landlocked status), market size and concentration.

Across this diverse region, digital transformation and the expansion of digital infrastructure are often set as the top priorities in the national digital strategies. At the same time, there is a common challenge: emerging technologies such as cloud computing, artificial intelligence (AI), and virtual reality are driving growing demand for fast, reliable, data-intensive connectivity. Despite this growing demand, one element of critical Internet infrastructure that is often overlooked is Internet Exchange Points (IXPs).

IXPs are physical facilities that allow networks

such as Internet Service Providers (ISPs), content providers, enterprises, and academic institutions to exchange traffic directly. By keeping local traffic within national borders, IXPs reduce costs, improve performance, enhance resilience, and strengthen the overall security of Internet ecosystems.

The trajectory of Internet Exchange Points (IXPs) in the SEE region has been closely linked to the area's economic and social transitions over the past three decades. In the early 2000s, most of the region relied heavily on international transit through Western Europe, which resulted in high connectivity costs and increased latency for local traffic. Contributing factors included limited national and regional backbone infrastructure, the dominant role of incumbent operators, and high market concentration. Early efforts to address these inefficiencies were the IXPs established in Slovenia and Croatia, operated by research and computing centers – a distinctive model for the region.

Over the following decades, markets were liberalised and competition increased through open access regulation. However, recent trends indicate a new wave of market consolidation across the region, with many local ISPs acquired by large, foreign-

owned telecom groups such as Deutsche Telekom, United Group, A1, Vodafone, and Yettel. These new dynamics are reflected in the way traffic flows within and beyond the region, where operators' peering policies can determine whether data stays local or continues to rely on distant hubs.

*This designation is without prejudice to positions on status, and is in line with UNSCR 1244/1999 and the ICJ Opinion on the Kosovo declaration of independence.

Figure 1:
IXP Landscape in South East Europe



Source: PeeringDB

Today, the SEE region hosts more than twenty active IXPs, improving regional connectivity and reducing reliance on costly international transit routes (Figure 1). Larger markets such as in Romania, Bulgaria and Greece have seen the emergence of multiple IXPs, while smaller markets typically operate a single exchange.

The establishment of these IXPs was rarely straightforward or uniform. Most required an initial push, whether through equipment donations, introductions to potential members, guidance on governance best practices or all combined. Examining the governance models reveals both the opportunities and the limitations of different approaches.

NREN-led governance

As previously mentioned, the first IXPs in the SEE region were initiated and operated by university computer centres or national research and education networks (NRENs), providing neutral platforms at a time when commercial ISPs had limited incentive to establish local peering. The Slovenian Internet Exchange (SIX), founded in 1994 and operated by ARNES - the national research and education network - is the oldest example in the region. Similar models were later adopted across the region, with notable cases including



the Croatian Internet Exchange (CIX), Montenegro Internet Exchange Point (MIXP), Macedonia Internet Exchange Point (IXP.mk), Greek Internet Exchange (GR-IX), Bosnia and Herzegovina Neutral Internet Exchange (BHNIX), and the Albanian Neutral Internet Exchange (ANIX).

These IXPs share a number of key organisational features that shaped their development and operation:

- **Financial model:** In most cases, these exchanges operate as non-profit organisations and rely on the collection of port fees from its members for the purpose of covering operational costs, equipment and capacity upgrades, while other costs like co-location and personnel expenses are covered by the research centre or university. In certain cases though, the IXP is fully funded by the operating institution and connecting to the IXP is completely free of charge.
- **Governance model:** Members often exhibit limited interest or lack the requisite capacity to engage in most day-to-day operational decision-making. Although they typically do not possess formal voting rights, as seen in member-led IXPs, the larger peers still retain significant influence. This is especially true in smaller, more concentrated markets, where they can shape the strategic direction of the

IX, including its expansion initiatives. In some cases, larger operators at certain IXPs have expressed concerns about potential revenue loss if networks they consider customers join the exchange.

- **Technical setup:** On the technical side, these IXPs are typically operated and hosted by the research centres and universities themselves, which are crucial for ensuring their independence from commercial providers. This neutrality helps maintain trust among participants, as no single operator could have undue influence over the exchange's operations or the data flowing through it.

This model brings significant advantages, including high trust among participants due to its neutrality, availability of hosting locations within universities and research centres, and long-term institutional stability independent of market fluctuations. At the same time, these IXPs face constraints such as limited funding for scaling infrastructure, a small number of dedicated personnel managing operations, and slower responsiveness to rapidly changing peering landscape. There is also a risk of becoming insular if the exchange does not engage with broader community stakeholders.

Member-led governance

As markets matured, some ISPs formed

associations to create IXPs collectively, sharing costs and governance responsibilities. The largest Romanian IXP, InterLAN, was established in 2001 as an association of small local ISPs and exemplifies this approach. The member-driven model fosters a strong sense of ownership and inclusiveness, encouraging collaboration and even the smallest ISPs can participate without prohibitive costs.

In some cases, this approach created a critical mass of connected networks, making the IXP itself an attractive destination for content providers seeking to reach smaller, harder-to-reach ISPs. Similarly, the peering needs of one small network were amplified by the association, as the presence of many other smaller networks at the exchange increased the value of connecting there.

While consensus-based decision making can sometimes slow responses to emerging needs, the association model has proven effective in markets with many independent ISPs. The approach balances shared participation with professional management, ensuring long-term sustainability and growth, even in the face of resource limitations compared to larger commercial operators. Diverging member interests, though, remains a challenge and could lead to fragmentation if not managed carefully.



Commercial governance

Privately owned, commercial IXPs represent another model in SEE. Exchanges such as the Serbian Open Exchange (SOX) and the Bulgarian Internet eXchange (BIX.BG) illustrate how professionalised, for-profit management can accelerate growth and infrastructure scaling. This model allows rapid investment in technology, the diversification of services including co-location and value-added interconnection, and especially in the case of BIX.BG; the creation of a regional hub that attracts international peers.

The commercial model also carries challenges. Participants may perceive a risk of bias towards profit over neutrality, while growth can be sensitive to market conditions and financial performance. Maintaining long-term trust and neutrality is therefore essential to ensure that commercial IXPs contribute positively to the broader ecosystem.

Regulator-driven governance

Governments or regulators sometimes step in directly to establish IXPs. While there have been several instances of government ministries or regulatory agencies attempting to either build or take control of IXPs, only one such model currently exists in the region: the Kosovo Internet Exchange

(KOSIX), which is operated by ARKEP, the National Regulatory Authority.

One of the perceived advantages of this governance model is that the regulatory involvement aligns the IXP activities and plans with broader state-led telecommunication strategies, providing credibility where trust among ISPs may be low.

That said, there are drawbacks to this model. Governmental processes may introduce delays in innovation, while limited autonomy could affect the IXP's ability to adapt quickly to evolving market needs. Additionally, funding constraints often hinder growth, limiting the IXP's ability to scale effectively. Similar to NREN-operated IXPs, KOSIX faces significant challenges in attracting and retaining skilled personnel, as well as in building an active and engaged community around the exchange.

Despite these limitations, regulator-driven governance can be effective for kick-starting IXPs in small markets, though long-term success requires greater independence and active community engagement.

This diverse array of IXPs all face similar challenges that influence the trajectory of development in

the region. National backbone infrastructure is underdeveloped in several countries, restricting IXPs to capital cities and limiting their geographical reach. Some IXPs also face strategic dilemmas, wary of being perceived as competitors by their own members.

Reluctance from incumbents to join local exchanges further constrains peering, keeping operational costs high for smaller ISPs and stifling the growth of more efficient, localised ecosystems.

Awareness of IXP benefits also remains limited, especially outside of “traditional” networks. E-government, fintech, and enterprise IT networks often overlook how IXPs can enhance the resilience and security of their own networks as well as the whole national Internet infrastructure.



1. Keeping local traffic local

1.1 Connecting service providers for seamless traffic exchange

When looking at the traffic exchanged within the same country, it might be intuitive to expect that local traffic remains, well, local. This means that the traffic originating from a network in the country will not be routed through circuits that would cross borders, traverse a set of foreign networks/hops, only for it to return to the country of origin towards its final destination. The reality is that this is not always the case.

One of the main reasons behind starting an IXP - some might even argue that this is the “primary” role of an IXP - is to connect all service providers in a way that would facilitate the exchange of local traffic between them. In essence, if network A needs to send traffic to network B, it can do so by handing the traffic over at the IXP, especially if there are no direct peering or interconnections between both networks elsewhere.

But before we delve more into this, to understand how traffic is exchanged within countries, we need to take a look at the interconnection landscape and the way the connectivity industry is running in those countries. When we started analysing the market dynamics, we quickly identified several patterns.

It is often the case that there is a small oligopoly that tightly controls the connectivity market within countries. According to data from the Internet Health Report, just three ASNs in Serbia (AS8400, AS31042 and AS5958) cover 81% of the population. The situation is similar in Slovenia where the top three ASNs (AS3212, AS5603 and AS21283) cover 82.1% of the population; should we add AS34779 to them, the coverage becomes 96%. Some other markets, like the Bulgarian one, witnesses less concentration in the sense that the top three ASNs (AS8866, AS29244 and AS12716) cover only 55.9% of the population in Bulgaria. If we don't look at the AS level and consider the fact that Telcos can operate several ASNs in the same market (through mergers and acquisitions for example), then the percentage of population covered becomes even higher.

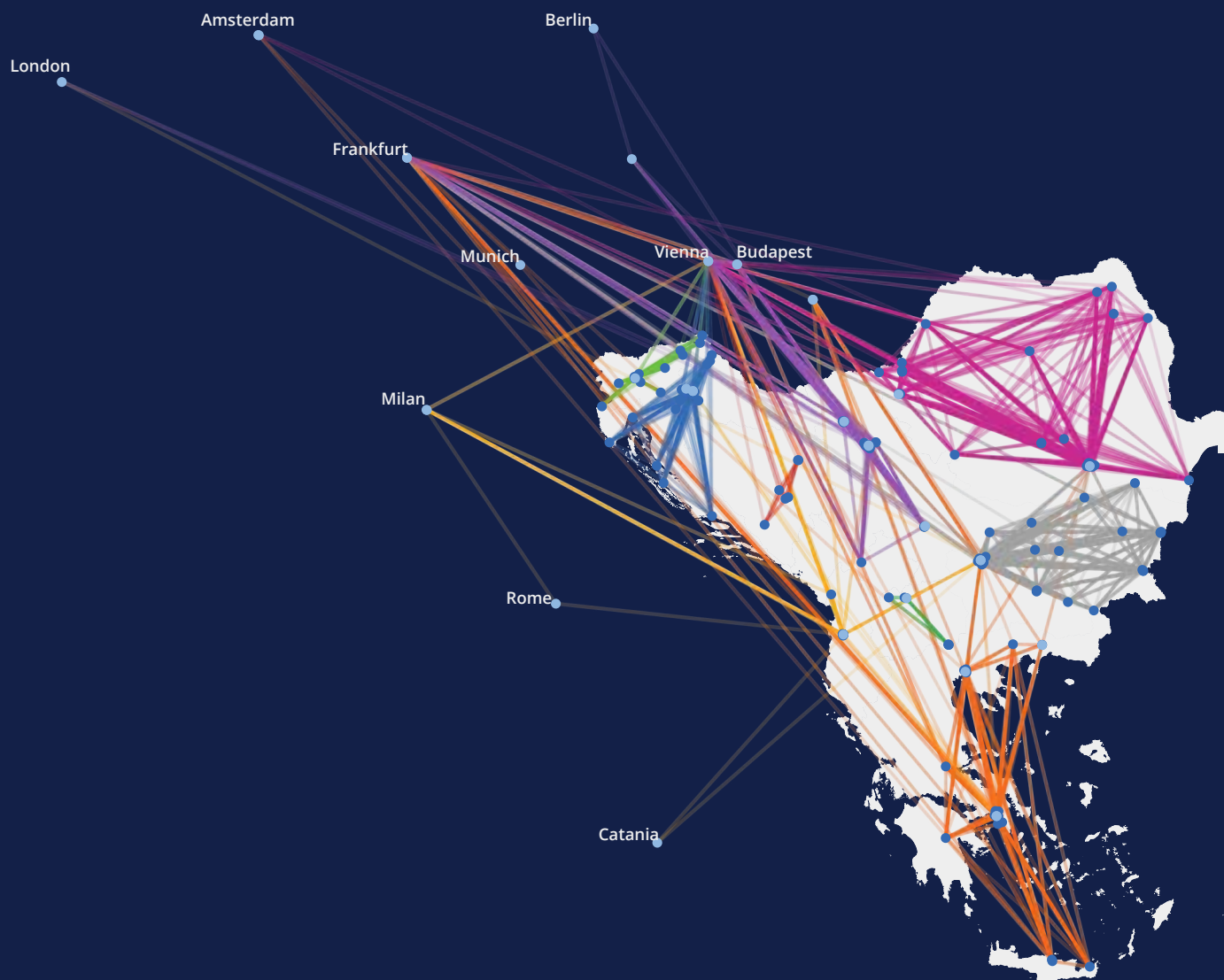
The reason behind this market concentration can be traced to the early days of telco incumbents who invested a lot in the infrastructure and had a vested interest in keeping the market as concentrated as possible to justify the returns. This control was also on the international connectivity up to a certain degree, this was, however, liberalised a while back with the entry of international transit providers such as Hurricane Electric, Arelion and Cogent, etc.

In theory, the fewer service providers and ISPs there are in a country, the easier it is to keep the traffic local between them. All they need to do is peer between themselves (at a private facility or in a public set up such as an IXP) and that's it, they could start pushing traffic over these local connections. This, however, can be influenced by factors such as politics, business agreements, the availability of interconnection facilities and the availability of proper network infrastructure.

The moment we start having lots of small to medium-sized ISPs, relying on private interconnections to exchange traffic becomes tricky. In essence, there are several issues at hand here:

→ In some countries, it is easy and cheap to find fiber circuits within a city; but that becomes quite expensive when we start looking at circuits between different cities, especially distant ones. In one instance, it was reported that it was financially cheaper to send traffic from one city to another via Frankfurt as opposed to doing it over a local fiber circuit connecting both cities. This was specifically commoditised after the market liberalisation and the entry of the international connectivity providers to some SEE countries

Figure 2:
Measuring the Proportion of Local Traffic that Remains Local in SEE



Source: [RIPE Atlas](#)

→ Market dynamics can also be subject to discrimination based on the size of the provider. It is often the case that we find the top few players (the big operators) peering and exchanging traffic between themselves, but they refuse to peer and connect to the smaller ISPs. Therefore, traffic originating or ending at these small ISPs might require some longer routing, even internationally sometimes. This is an area where IXPs are really useful in helping to connect these smaller ISPs and providing local routes to the bigger networks if possible. However, as stated earlier, we did witness cases where big operators connecting at certain IXPs do oppose having smaller ISPs join the IXP for a number of reasons

To test all of these assumptions on keeping the local traffic local (either via local IXPs or via other circuits), we ran a series of measurements across the region using RIPE Atlas Probes (Figure 2). The measurements were a series of traceroutes between the probes within the same national territory and then we analysed the paths these traceroutes took.



Figure 3:
Out-of-country Traffic Paths per SEE Country

	Total paths	Out-of-country paths	Out-of-country paths (%)
Albania	72	19	26.39
Bosnia and Herzegovina	28	3	10.71
Serbia	455	31	6.81
Greece	754	27	3.58
Romania	1544	29	1.88
Slovenia	418	6	1.44
Croatia	592	6	1.01
Bulgaria	2031	15	0.74
North Macedonia	25	0	0.00

Depending on the number of probes available, we were able to analyse a few dozen, up to a couple of thousand, paths per country. Figure 3 summarises our findings. Note: data for Albania includes aggregated paths from both Albania and Kosovo*, due to the unavailability of more granular data.

Clearly, the more paths we have, the better and more robust the results are, removing any bias from the system, such as how many ASes are covered by the probes or the type of networks hosting them (university vs. service provider vs. enterprise). These networks might have different upstream providers and hence the behaviour might be different. For instance, a significant number of probes or anchors are hosted by universities and we end up seeing research networks such as GEANT in the upstream paths of the connections made.

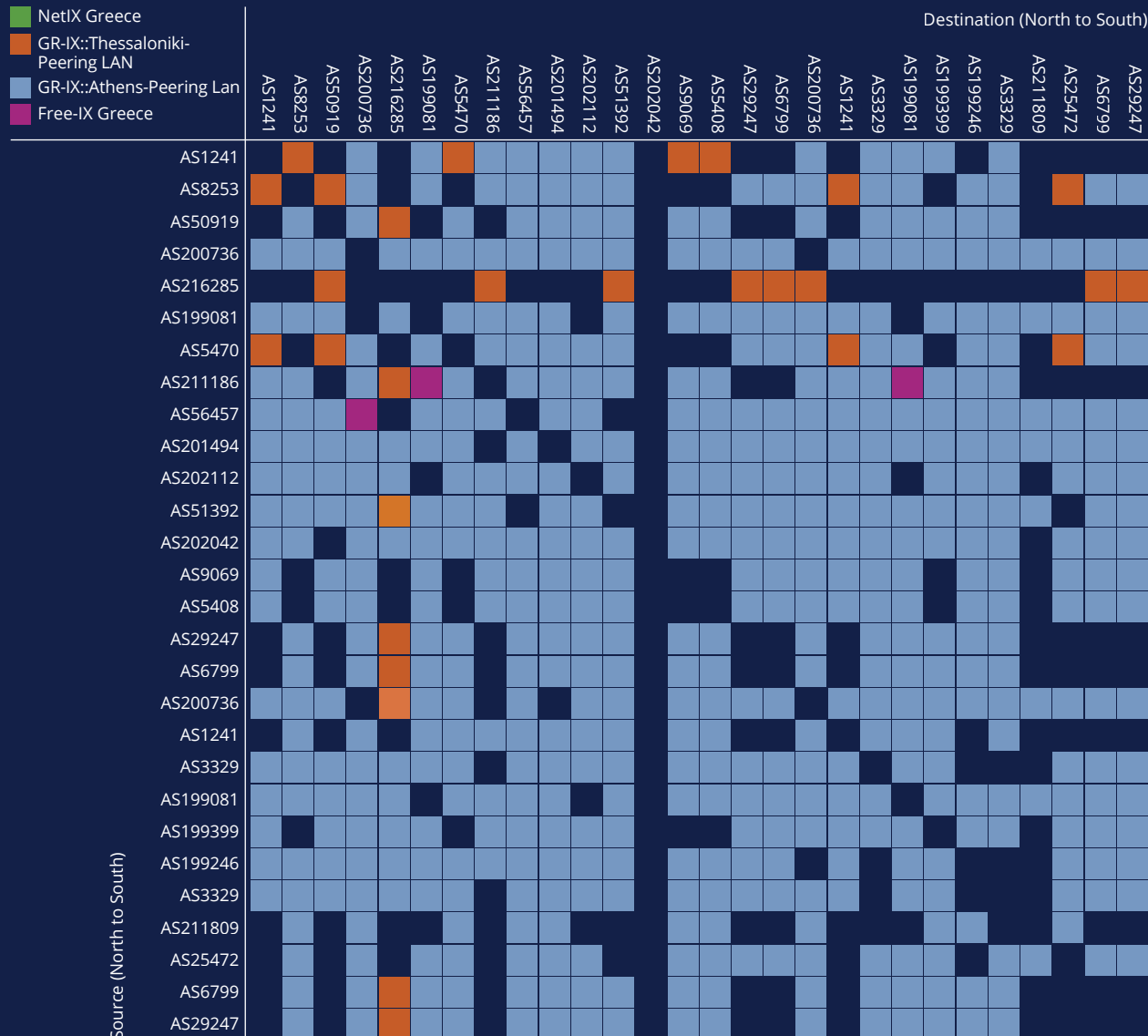
Given our data, we assume that a majority of the paths remain within the national territory. For instance, in Romania, only 1.88% of the observed 1,544 paths actually went outside Romania. The only outliers in the findings were Albania and Bosnia and Herzegovina with a respective percentage of 26.39% and 10.71% of connections leaving their borders. To note that the number of total observed paths in those countries was on the lower end compared to Romania or Bulgaria.

From the analysis, we also noticed that there were some interconnection points such as Frankfurt and Vienna where local traffic was being routed through. This is not surprising since a lot of the big operators in the region have invested in building connectivity to “nearby” interconnection hubs (such as Frankfurt, Vienna, Budapest and Amsterdam) to get access to content being hosted in these popular data hubs. So it is not surprising to see two operators, from the same country, using these extremal circuits to hand over the data. This could be done by design (some operators do not accept peering directly with others), lack of trust in the local partners or a faulty traffic engineering policy.

*This designation is without prejudice to positions on status, and is in line with UNSCR 1244/1999 and the ICJ Opinion on the Kosovo declaration of independence.



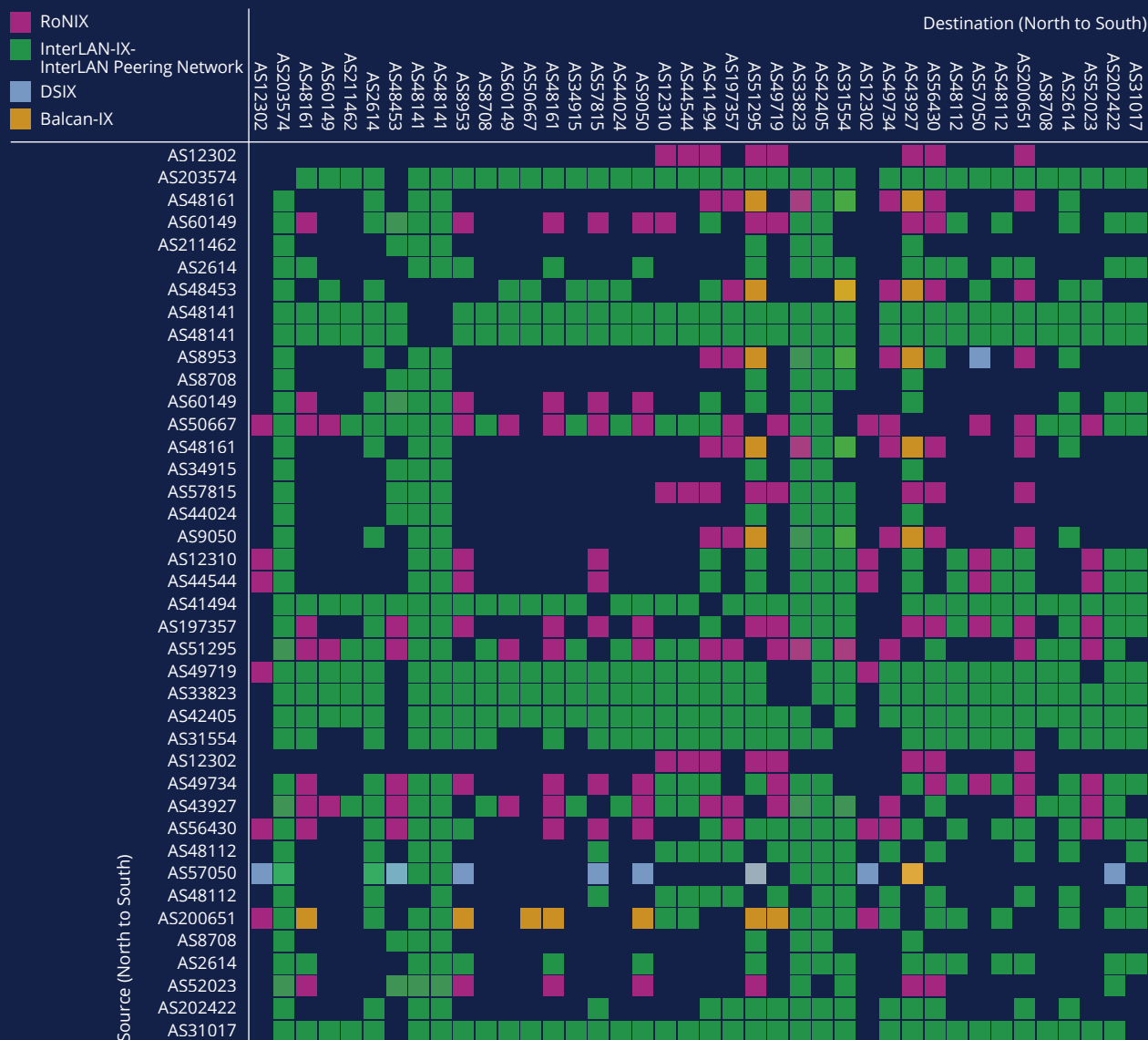
Figure 4:
Intra-country Paths: Greece



So now that we know a big chunk of the traffic is staying local, the next question would be to see whether local IXPs are playing a role in this. In other terms, is the traffic being exchanged locally via the IXP circuits or maybe through private interconnections between the operators themselves? We started looking deeper at the different hops identified in the traceroutes and we cross-checked the IXP LANs to see if there were any hops in the paths hosted at the local IXPs.

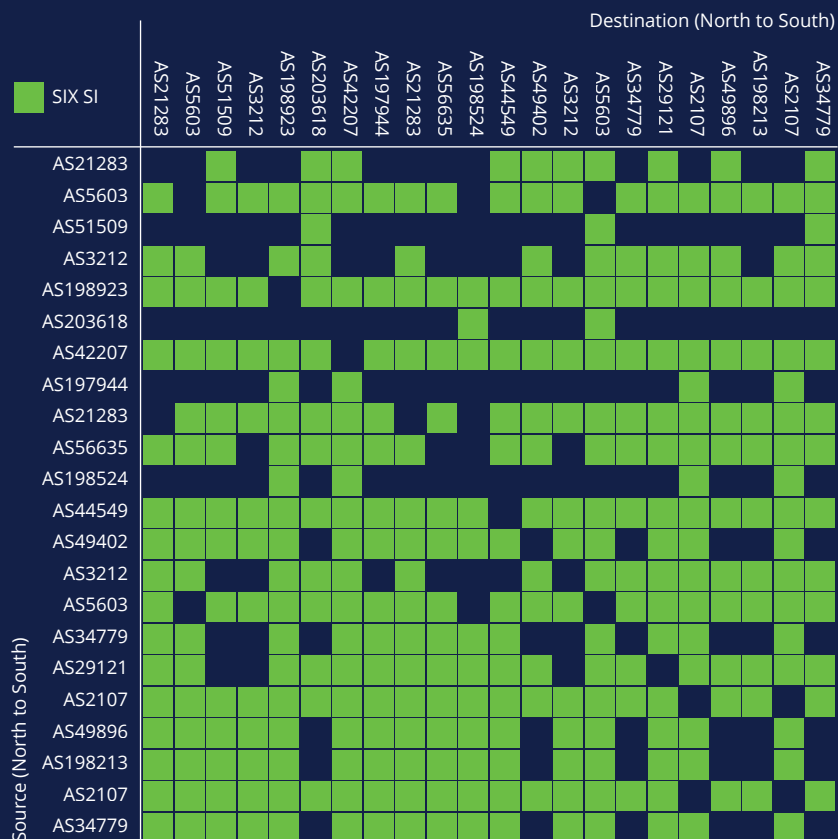
The results, when presented in a matrix format mapping AS_A to AS_B paths, showed some differences across the region. For example, when looking at Figure 4, we see that most Greek ASes were exchanging the traffic through a local IXP. We see that GR-IX plays a big role in facilitating the exchange of traffic.

Figure 5:
Intra-country Paths: Romania



When we look at Romania in Figure 5, the matrix looks less dense, suggesting that there is a good part of local traffic being exchanged outside of IXPs without leaving Romania. We were able to identify that InterLAN, and RoNIX to a lesser extent, do facilitate local traffic exchanges. This is normal since InterLAN was created when a big number of small ISPs in Romania decided to start an IXP to exchange traffic between themselves and to attract foreign content by creating a critical mass when it comes to volume of data exchanged.

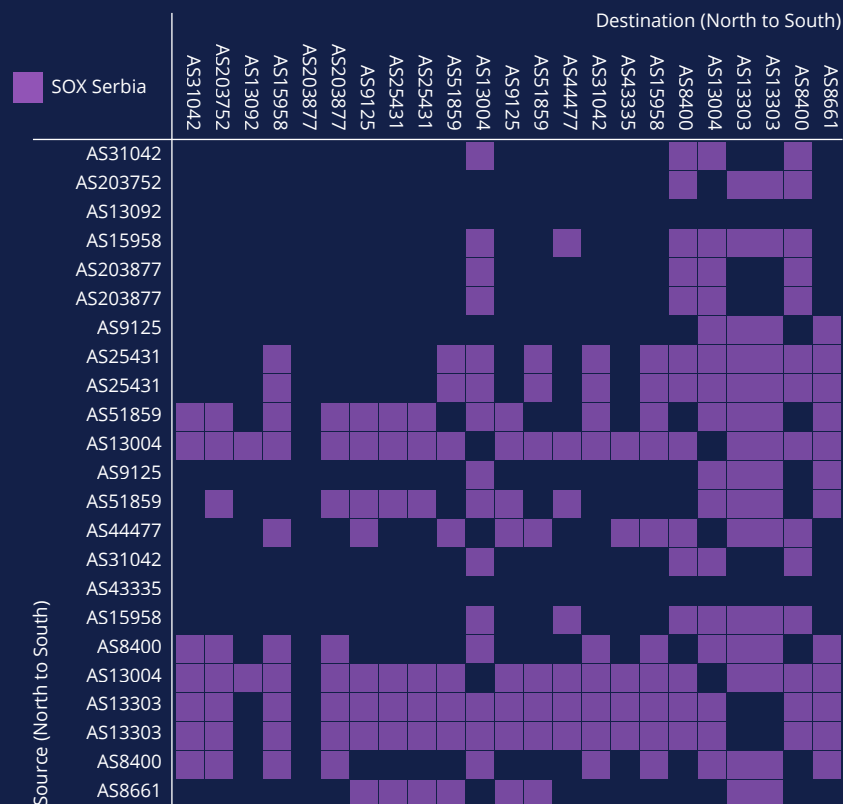
Figure 6:
Intra-country Paths: Slovenia



Even in countries where there is only one IXP, we do see a primary role for these IXPs in facilitating the local exchange of data. Figure 6 shows the case of Slovenia where we see most of the paths crossing through SIX.

As encouraging as this data is, there are still gaps to fill where IXPs can assume a bigger role in the local interexchange of data. Figure 7 suggests that almost half of the paths are not crossing through SOX in Serbia.

Figure 7:
Intra-country Paths: Serbia



Again, this is normal in the sense that the big operators in Serbia are probably handing over the traffic at other local facilities. But even if that is the case, providing redundant circuits and connectivity via the IXP goes a long way in strengthening the resiliency of a country and minimising cross-border traffic.

Figure 8:
DNS Hits on K-root Instances

	No of probes	No of measurements	% served from Local K-Root	% served from Foreign K-root	Local city and host of K-root	Top foreign K-root instances
Albania	22	5725	18.60	81.40	Tirana (Host.al Shpk)	Vienna, Athens, Miami, Frankfurt
Bosnia and Herzegovina	20	7171	60.20	39.80	Sarajevo (University of Sarajevo)	Zurich, Belgrade
Bulgaria	90	32286	85.50	14.50	Sofia (IPACCT Ltd.+ NetIX)	Athens
Greece	83	29178	92.70	7.30	Athens (Greek Internet Exchange)	Sofia
Croatia	39	13778	0.00	100.00	N/A	Vienna, Lisboa, Geneva
Montenegro	8	2871	0.00	100.00	N/A	Belgrade, Lisboa, Feldkirch
North Macedonia	9	3236	11.10	88.90	Skopje (IXP.mk)	Sofia, Pavlodar
Romania	78	27385	28.60	71.40	Bucharest (Interlan Internet Exchange)	Lisboa, Belgrade, Miami
Serbia	53	19014	67.80	32.20	Belgrade (SOX)	Amsterdam, Vienna
Slovenia	52	18475	0.00	100.00	N/A	Vienna, Frankfurt

1.2 Content localisation

Back when IXPs started emerging in the SEE region, there were not many options available for local content producers to host their content locally. Being relatively close to major content and interconnection hubs such as Frankfurt and Vienna, they made the strategic decision of hosting the content there.

There is a direct cost associated with hosting content abroad and subsequent cost that operators had to incur to provide transit and reachability to this content. All of this slowed down the investment in local data centres and delayed the emergence of local hosting platforms available to the local market.

This started to change with the advent of content delivery networks, cloud

services and hyperscalers, and with a constant increase in the need to localise data, either due to business needs (targeted content) or regulatory compliance (GDPR, for example).

What followed was a wave of investments in data centres in the region, spearheaded by the incumbents and big telecom operators. Later on, carrier-neutral data centres began to be mainstream with early movers in Bulgaria, Greece and Romania.

However, having content hosted locally does not automatically guarantee that local networks will be able to reach it directly. This is governed by technical and commercial arrangements, in other words, networks should announce the local



routes to each other and accept handling local traffic coming from other networks they peer with. In the event that such agreements are not in place, or where poor traffic engineering is in place, we might find scenarios where traffic ended up being routed internationally instead of remaining local.

To test this, we ran another series of measurements in the SEE region using RIPE Atlas probes. The measurements aimed to determine which K-root instances were used by the probes in question. The results are shown in Figure 8.

In cases where there is a local K-root instance such as Bulgaria, Greece and Serbia, the probes predominantly reach a local K-root. Romania is an exception here and exhibits an odd pattern. We do see the local instance is used (28.6%), but there are also many measurements going all the way to Lisbon/Portugal (40%) for an answer.

To understand the results better, we looked at probe behaviour at an ASN level. We noticed how probes in Digi Romania all select the K-root in Lisbon. That may well be a side effect of the company's peering policy at the IXP, which is a selective one. This means even though local resources are available, lack of active exchange of routes internally might result in traffic

leaving the country needlessly. To note that Digi Communications did announce that they are launching operations in Portugal back in November 2024, so that explains why the probes hosted there are hitting the K-root instance in Lisbon.

A similar behaviour was spotted in Albania and North Macedonia.

Determining the exact reason why these mis-routes are happening is not always easy. In general there are two options:

- The ASN which hosts the probe does not have an available route to the local K-root instance. This can happen for example when the K-root is hosted at an IXP, and the ASN is not peering there. It could also happen if the network hosting the K-root does not advertise the route to its competitors or other connected networks
- The ASN which hosts the probe does know a route to the local instance but because of BGP policies, a path to a foreign K-root is preferred

An important disclaimer here is that the hosts of the probes participating in the measurements are an important factor. Covering ASNs that are a small part of the population might not give adequate representation of what happens on the real Internet. This is why it is important to have

diversity in RIPE Atlas probe deployment from the perspective of:

- Geographical coverage/detect changes in circuits due to geographical reasons
- ASNs with eyeball coverage/measure the traffic from the perspective of a large group of users
- Different types of ASNs/detect difference in behaviours according to the types of networks

2. Fostering local interconnection to develop a digital economy

2.1 Open and inclusive membership policies

As mentioned in the previous chapter, most IXPs in the SEE region were initially established with a primary focus on their core mission: keeping local traffic, local. As a result, early participation typically encompassed a handful of local ISPs or academic networks aiming to reduce their dependence on costly international transit. This focus on ISPs inadvertently marginalised other key network operators, including governmental, enterprise, and academic networks, which also play a crucial role in regional connectivity.

Several structural barriers have hindered the broader growth of interconnection in the region. The lack of neutral data centres and hosting facilities, combined with the dominance of major northbound routes leading to Vienna and Frankfurt, have reinforced exclusivity and slowed the growth of domestic and regional interconnection.

Over time, most IXPs in the region have moved toward open membership models, dropping restrictive criteria such as the requirement to hold a national ISP licence. A few exceptions remain: BIX. BG restricts membership of personal networks. KOSIX stands out for its regulator-driven framework, where membership applications are reviewed

and approved by the regulatory authority; at the same time, all national providers offering transit are mandated to join. Elsewhere, IXPs generally require only basic technical conditions such as an Autonomous System Number, allocated IP address space, and upstream Internet connectivity.

As previously noted, many SEE IXPs struggle with outreach to potential new members. Key challenges include:

- **Incumbent influence:** Large incumbent ISPs often use their dominance within IXPs to block new entrants, whether by vetoing membership applications, threatening to withdraw if competitors join, or controlling access to the physical infrastructure needed for connection
- **Operator-side constraints:** Some IXPs lack the financial or human resources to actively recruit members, while others are reluctant to challenge incumbents or expand their reach beyond a narrow set of networks. This conservative approach leaves IXPs 'stagnant', serving only a small group of dominant players instead of acting as open, inclusive hubs for the broader digital economy
- **Awareness and market concentration:** Many potential participants remain unaware of the tangible benefits of peering, particularly

in highly concentrated markets where a few operators control most connectivity. In these environments, smaller networks and end users see little incentive to connect to the exchange

- **Infrastructure gaps:** The lack of robust infrastructure beyond capital cities, such as the high costs of long-haul fiber, the absence of neutral co-location facilities, and limited local loop access, further restrict participation and slow the broader expansion of domestic and regional peering

Open and inclusive membership policies significantly enhance the value of IXPs. By welcoming a diverse range of network operators, IXPs foster a competitive and innovative environment. As many services critical for daily life are now offered online, such as e-government, healthcare, and education platforms, which saw a dramatic surge in use during COVID-19, it has become even more crucial to ensure that these services are supported by resilient, low-latency, and cost-effective local infrastructure.

Moreover, such policies stimulate the growth of digital content industries, software development, and e-commerce. Startups, in particular, rely on these sectors for support, creating a ripple effect that drives economic diversification and job creation.



2.2 Who should connect at the IXP?

- **Research centres and universities:** Research institutions can utilise IXPs to access and share academic resources, collaborate on research projects, and engage in data-intensive experiments. The low-latency environment offered by IXPs is particularly valuable for real-time data analysis and scientific research. This type of participation is commonly seen in the SEE region, as many exchanges are hosted and operated by universities and research centres
- **Financial institutions:** The financial sector depends on low-latency, high-speed connectivity for real-time trading, financial data exchange, and secure transactions. Connecting to an IXP allows banks and other financial institutions to ensure that critical financial data flows efficiently and securely within the region, reducing reliance on longer international routes

In some parts of South East Europe, the banking sector is actively evaluating ways for all banks and relevant financial institutions to connect securely to the local IXP. If implemented, this initiative could drive additional investment from ISPs in local loops and interconnection infrastructure to ensure robust, low-latency access for these institutions, enhancing both resiliency and business continuity.

- **Startups and entrepreneurs:** Startups and entrepreneurial ventures often operate on tight budgets. IXPs provide them with cost-effective access to high-speed Internet connectivity, reducing operational costs and enabling faster time-to-market for their digital products and services. This benefit is amplified when paired with the availability of neutral, easily accessible data centres and co-location facilities, which lower the barriers to entry and make connecting to the IXP simpler and more feasible for emerging businesses
- **Government entities:** Government agencies and ministries can leverage IXPs to enhance their digital infrastructure and improve the delivery of online services to citizens. This fosters greater transparency, efficiency, and accessibility in governance. Governments should also lead by example, actively participating in IXPs and supporting a healthy, efficient interconnection and peering landscape within their jurisdiction

An example of such efforts within broader governmental strategies is the recent Croatian National Cybersecurity Strategy, which recommends that public and governmental organisations connect to CIX to enhance the security and resilience of their networks. The membership analysis shows government

ministries and regulatory agencies being present at the exchange.

Governmental presence can be seen at other SEE IXPs too. Examples include the Bulgarian Ministry of Electronic Governance connected at BIX or Slovenian National Regulatory Authority (AKOS) joining SIX.

- **Healthcare institutions:** In the era of telemedicine and digital health solutions, healthcare institutions benefit from reliable, low-latency connectivity. IXPs support the seamless exchange of medical data, facilitating remote consultations and other digital healthcare services. An example from the region is the IXP in North Macedonia, which provides low-latency access to the National Health System hosted at the same faculty as the IXP. This setup incentivises ISPs to connect and peer at the IXP to ensure a high-quality experience for their end users
- **Media and broadcasting:** Some IXPs provide value-added services, such as dedicated networks for sharing multicast entertainment streaming. This encourages broadcasters and TV stations to connect to the IXP, giving them easy access to content distribution. As more broadcasters and streaming services join, the IXP becomes increasingly attractive to multimedia streaming providers, creating a

Figure 9:
Total Number of ASNs Registered, Number of Local and Non-local Peers
Connecting to the Main IXPs in the SEE Region



*This designation is without prejudice to positions on status, and is in line with UNSCR 1244/1999 and the ICJ Opinion on the Kosovo declaration of independence.

**Kosovo does not have an officially assigned ISO 3166 country code, so organisations operating there use the country code of its neighbour in the RIPE Database.

Source: [HE](#) / Source: [PeeringDB](#)

snowball effect where more participants lead to further growth in connectivity and service availability. This type of service can significantly enhance the efficiency and cost-effectiveness of content delivery, benefiting both providers and consumers. Some IXPs in the region such as InterLAN and BIX offer multicast services to support the distribution of content

→ **IoT and smart city initiatives:** The Internet of Things (IoT) and smart city projects require robust connectivity for data collection, analysis, and decision-making. IXPs provide the infrastructure necessary to support IoT deployments and smart city initiatives

Figure 9 shows the number of local peers that connect to the IXPs in their respective countries compared to the number of non-local peers at those IXPs. The number of local ASNs is also mentioned to give an idea of the number of network operators in the national market.

Note: Not all local ASNs MUST be present at IXPs. It is mentioned here to give an idea on the potential size of the local addressable market and present an area of potential growth for the exchanges. The closer the various players of the digital ecosystem are, the better it is for the resiliency and the quality of the services offered. IXPs are a natural choice for bringing these players together in one place, in an efficient and scalable manner.



2.3 Cultivating a collaborative knowledge ecosystem

On a technical level, the primary function of an IXP is to act as an interconnection platform, enabling efficient traffic exchange among its peers. Yet, its role extends well beyond this technical core.

Equally important is the ability of IXPs to cultivate community collaboration around it. By bringing together operators, content providers, and other stakeholders, IXPs create an environment where knowledge is shared and professional ties are built, making the exchange not only a technical node but also a social and professional hub.

The strength and engagement of this community often determine the long-term success of an IXP. This is especially evident in regions such as South East Europe, where IXPs with limited resources rely heavily on active participation and member support. In such contexts, community engagement becomes a critical factor for sustainability, ensuring that the exchange continues to evolve despite structural constraints.

A defining characteristic of IXPs in the SEE region is their role as central points for collaboration and capacity development. From members-only meetings to the organisation and support of local,

national, and regional events, IXPs provide venues where the broader networking community can meet, exchange expertise, and share operational best practices.

Complementing these meet ups, SEE IXPs also maintain structured communication channels for stay informed, share critical updates and announcements and security alerts, etc. Mailing lists, messaging channels and dedicated forums enable operators to remain connected between events.

At the national level, many IXPs are closely tied to Network Operator Groups (NOGs). In Serbia, Greece, Romania, and Bosnia and Herzegovina, exchanges often serve as organisers or major supporters of NOG initiatives, consolidating local communities and expanding technical capacity.

Network Operators' Groups (NOGs)

NOGs are grassroots organisations that bring together network operators, technicians, and professionals from the telecommunications and Internet sectors. They provide a platform for knowledge sharing, troubleshooting, and networking. Active participation in NOGs fosters personal connections and strengthens the IXP community.

Regionally, the SEE Meeting has become a key platform for collaboration, bringing together operators from across SEE and beyond. Functioning as a de facto regional NOG, it provides a stage for knowledge exchange and dialogue, with IXP operators themselves playing an active role through the Programme Committee. This ensures that discussions are firmly anchored in operational realities and responsive to the evolving needs of the community.

Lastly, SEE IXPs are integrated into the broader European ecosystem through EURO-IX. As members, they can benefit from engaging with a global IXP network through a broad range of activities such as technical workshops, reports, knowledge exchange and access to peering tools. Annual meetings also offer the opportunity to liaise with other members of the industry such as content and hyperscalers.

Here are some key areas where sharing best practices and experiences can be particularly beneficial:

→ **Technical optimisation:** Peers exchange insights on optimising network configurations, reducing latency, and enhancing the efficiency of traffic exchange. Sharing technical best practices ensures that IXPs operate at peak performance



- **Security measures:** Cybersecurity is a top priority in the digital age. Peers regularly collaborate on sharing cybersecurity best practices and strategies to protect IXPs and the broader digital ecosystem from threats
- **Technical assistance:** International organisations, such as the Internet Society (ISOC) and the Packet Clearing House (PCH), among others, provide technical assistance and resources to nascent IXPs. They offer guidance on infrastructure set up, security measures, and operational best practices
- **Business models:** IXPs can learn from successful business models adopted in other regions. Understanding how different pricing structures, revenue diversification strategies, and sustainability measures have worked elsewhere can inform decision-making
- **Regulatory soundboarding:** Government representatives and regulatory bodies can share insights into proposed regulatory approaches capitalising on the collective experience the peers have gained of the local, regional and global peering dynamics
- **Advocacy groups:** Advocacy groups can champion the interests of IXPs within the broader digital ecosystem. They can raise awareness about the importance of IXPs, lobby for supportive policies, and promote the economic benefits of local Internet traffic exchange
- **Innovation initiatives:** Collaboration can extend to innovation initiatives. Research centres, universities, and technology hubs can partner with IXPs to explore emerging technologies, such as 5G, IoT, and cloud computing, and their implications for IXPs and digital transformation
- **Capacity building:** Initiatives focused on capacity building, training, and skills development are instrumental in nurturing talent within the IXP community
- **Workshops, seminars, and educational programs:** Can empower individuals and organisations to contribute effectively to the IXP ecosystem

3. Attracting global hyperscalers and content providers

The effectiveness of IXPs in the region depends on the active involvement of a broad spectrum of stakeholders. Internet service providers, content platforms, cloud operators, hyperscalers, and data centres form the backbone of the peering ecosystem, each contributing in distinct ways to improve connectivity, lowering latency, and driving innovation.

Cloud and content players – including global technology leaders as well as local creators – are particularly crucial in this ecosystem. They produce and host digital assets such as websites, apps, and streaming services. By interconnecting through IXPs, they can distribute content more efficiently to regional users, improving performance and reducing delays. Hosting content locally at IXPs further accelerates delivery and supports the expansion of the region's digital content economy.

Given the size of some markets in the SEE region, we cannot certify that the region as a whole has been successful in attracting and hosting these global players. The exceptions here are:

- Bulgaria: Where we see a heavy density of international and regional cloud, content and OTT providers peering at BIX.BG and NetIX
- Romania: With a high density of content peering at InterLAN-IX followed by RoNIX and Balcan-IX

- Greece and Serbia: With a sizable presence of the above players peering at GR-IX: Athens and SOX respectively

This exception can be attributed to several factors:

- The ease of regulations in those countries which made it attractive for global players to come and establish their presence
- The bigger size of the population in these countries as opposed to others in the SEE region
- The proximity of Sofia to a big market like Turkey also made it an attractive destination to host content and services destined for the Turkish market
- Availability of neutral a data centre and good connectivity options (both local and international)

There is another reason why some of the above IXPs were successful in connecting content providers. It is thanks to a proactive approach to go and peer at big data hubs to gain access to the content directly. This required investing in circuits that provide acceptable latency back to their home countries. In essence, they went to where the content was instead of bringing the content to them. For example, SOX is present in Vienna; InterLAN-IX is present in Frankfurt;

and NetIX is in Vienna, Frankfurt and Amsterdam.

While this approach was helpful at the beginning to secure access to the content, big CDNs and streaming services who rely on high degrees of localisation and targeted content are skeptical and reluctant to continue peering with IXPs following a distributed model since this might cause some undesired asymmetric routing. In other terms, CDNs prefer to peer as close as possible to the end users. This would guarantee a better user experience overall.

Figure 10:
Cloud, CDN and OTT Leaders in IXP Participation in the SEE Region

	Total (in G)	No. IXPs	No. Locations
Akamai	340	3	2
Amazon	400	2	2
Anexia	30	3	3
BelCloud	72	5	3
ByteDance	400	3	3
Cloudflare	1080	15	6
Google	1380	8	3
M247	110	5	3
Meta	2090	10	4
Microsoft	790	8	4
Riot Games	50	5	2
Valve	400	3	3
Yahoo!	40	3	2

Source: [PeeringDB](#)

Figure 10 shows the top list of content and cloud providers present at the IXPs in the SEE region.

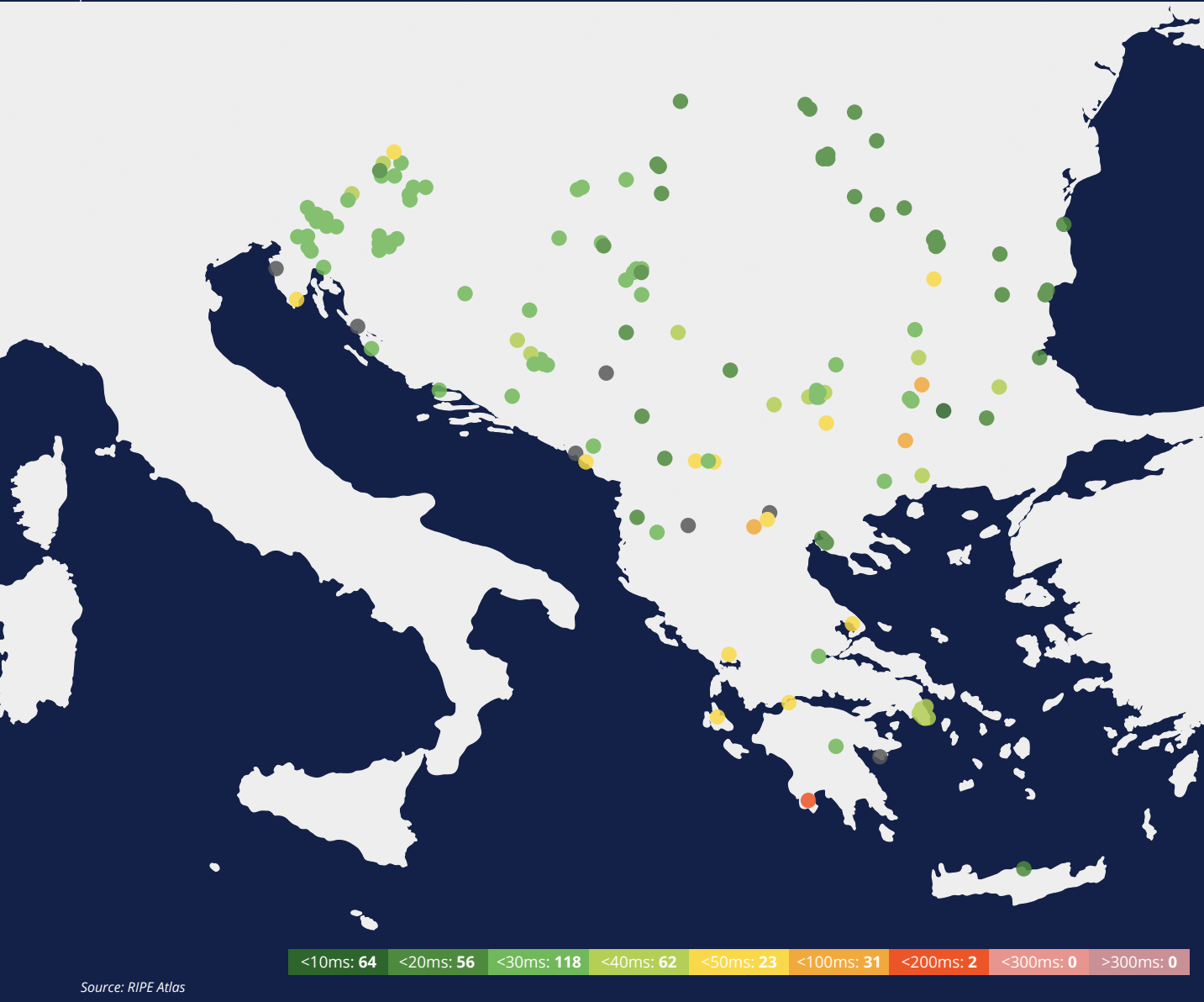
Cloudflare is leading in terms of IXP coverage with active peerings taking place in 15 IXPs across six countries. It is followed by Meta (peering at 10 IXPs across four countries), Microsoft (peering at eight IXPs across four countries) and Google (peering at eight IXPs across four countries)

It is important to note that Cloudflare and Google made an early move to the region and established a presence in most of SEE. This presence manifested either through private peerings directly with the service operators or through peering at the IXP where they could be reached by the general members of the exchange. The use of cache engines installed inside the operator networks is also a preferred method for these global players to provide content.

Since there is a small number of big operators representing a big chunk of the market share in most of the SEE markets, it is easy for content providers to go down the route of installing caches inside the operators without necessarily being present at the IXP. This is why some of these content players did end their membership at the exchanges a few years back.

Given that not all of the global players are present in all SEE markets at once, there is a growing benefit in establishing inter-regional connectivity so that the users in the neighbouring countries can benefit from relatively lower delays when accessing certain types of content. If planned correctly, the IXPs can play a considerable role in this. This is probably why some IXP operators reported plans to extend their presence to neighbouring countries.

Figure 11:
Reaching a Content Platform at InterLAN Using an IPv4 Destination



A series of measurements (Figure 11) were run using RIPE Atlas probes deployed in the SEE region. These tests measured the performance and latency of the connections originating from the probes towards a regional content platform connected at an IXP in Romania.

The probes in Greece and North Macedonia faced significant delays in reaching this destination. The low latency is the result of having nearby servers or access to those servers in neighbouring locations through inter-regional peering.

While probes in Bulgaria normally reached the destination quickly, there were five probes that showed high latency compared to other probes in Bulgaria. On closer analysis, we noticed that the traceroutes were taking scenic routes through Austria, Germany and Hungary.



Data Centres

Data centres can foster efficient IXP operations by supplying the physical infrastructure and co-location spaces needed for efficient functioning. Acting as neutral hubs, they provide an environment where service providers, content networks, and other operators can establish interconnections. Through their focus on reliability, security, and scalability, data centres make it possible for IXPs to accommodate the growing demands of Internet traffic.

Beyond their core role, data centres often deliver additional services – such as cloud hosting and disaster recovery – that add further value to the overall IXP ecosystem.

It is important to highlight that in the SEE region, as noted earlier, many data centres are still run by telecom operators. In contrast, IXPs usually perform best in carrier-neutral facilities, which allow various network providers to co-locate infrastructure without being subject to the control of a single telecom company. The expansion of carrier-neutral data centres helps create a more diverse ecosystem, giving stakeholders greater flexibility for hosting, peering, and interconnection.

This diversity is mature in cities like Sofia and Bucharest and we are currently seeing quite some

investments in developing new data centres in Greece coupled with investments in submarine cables as well. This will attract even more networks to host and connect which, in return, will encourage more growth of carrier-neutral data centres. Ultimately, this leads to promoting competition, innovation and resilience of the digital infrastructure.

Figure 12:
Measuring Interconnection in the SEE Region



Source: RIPE Atlas

4. Becoming a hub for exchanging regional traffic

4.1 Enhancing regional and global digital connectivity

While improving local performance, IXPs also play an essential role in advancing regional and global connectivity. Thanks to its geographical position, the SEE region is increasingly serving as a bridge, connecting the Middle East, the Caucasus, and Northern Africa to the major interconnection hubs of Western Europe.

Several developments highlight this potential. In Greece, multiple submarine cable projects are building landing stations that link the Middle East, Western Africa, and India to Europe. Building on

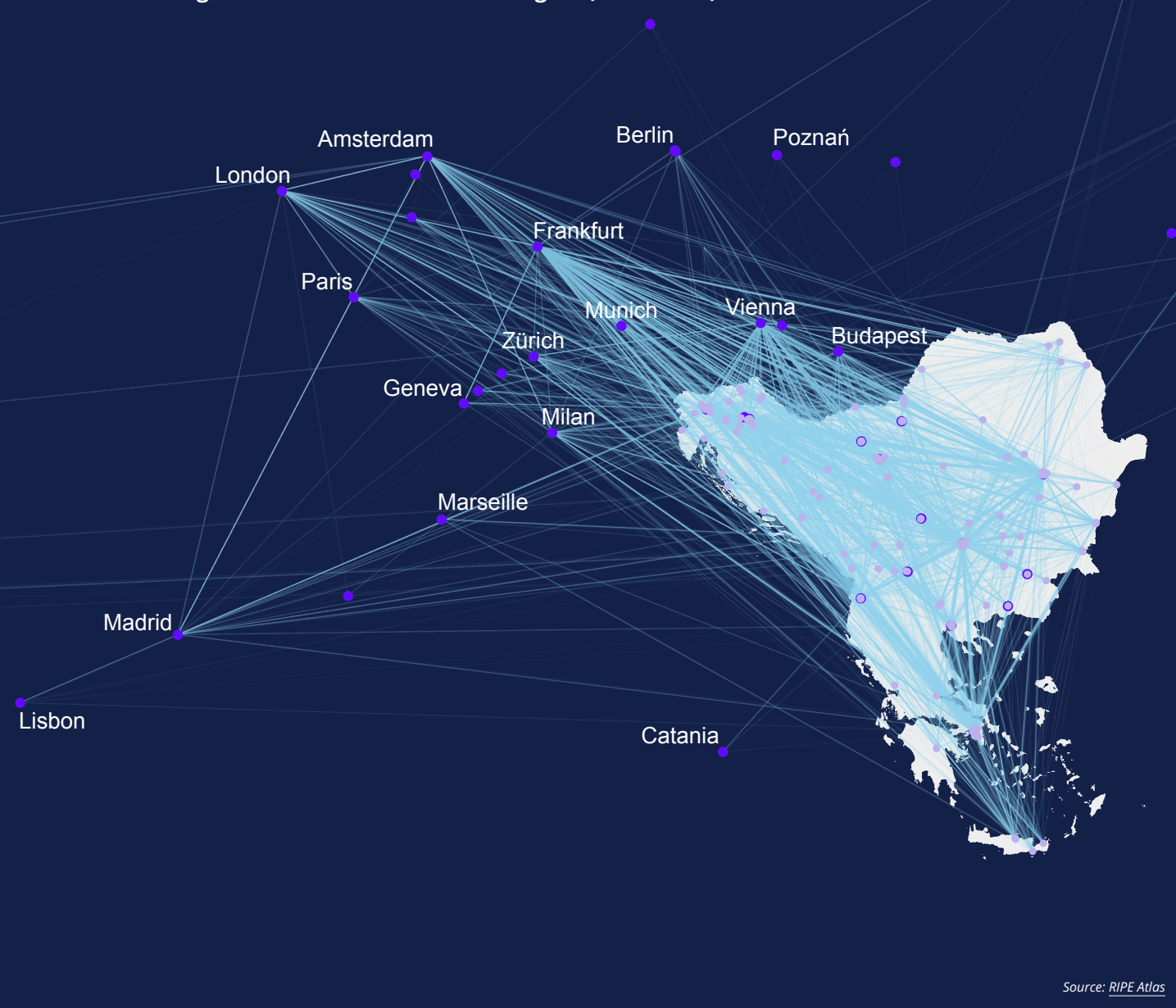
this, GR-IX has announced plans to extend its footprint to Crete, by opening a presence at a newly established neutral data centre located near the landing sites. Albania is positioning itself as a subsea connectivity hub, with new plans for an express cable linking Albania and Egypt. On the eastern side of the region, Bulgaria's location on the Black Sea attracts operators from the Caucasus, Middle East and Central Asia seeking access to global content, Meanwhile, Belgrade's central position makes it a natural convergence point for networks across neighbouring countries. Together, these factors position SEE IXPs as critical gateways for global Internet traffic, stimulating investment, knowledge

transfer, and economic growth, while supporting digital innovation across the region.

The impact is amplified when operators peer at IXPs in neighbouring countries, improving regional latency and creating a more cohesive digital ecosystem. As pointed out in the previous chapter, most of the global cloud and content providers have established a presence in the region, however, not all of them are present across the region. Given the fragmented nature of the SEE market, full coverage is unlikely.

Strengthening regional connectivity delivers multiple

Figure 13:
Measuring Interconnection in the SEE Region (Zoomed in)



benefits. It promotes economic integration among neighbouring countries, supports cross-border trade, and facilitates the exchange of knowledge and cultural content. In addition, it enhances resilience, as local IXPs can maintain operations even if international links experience disruptions.

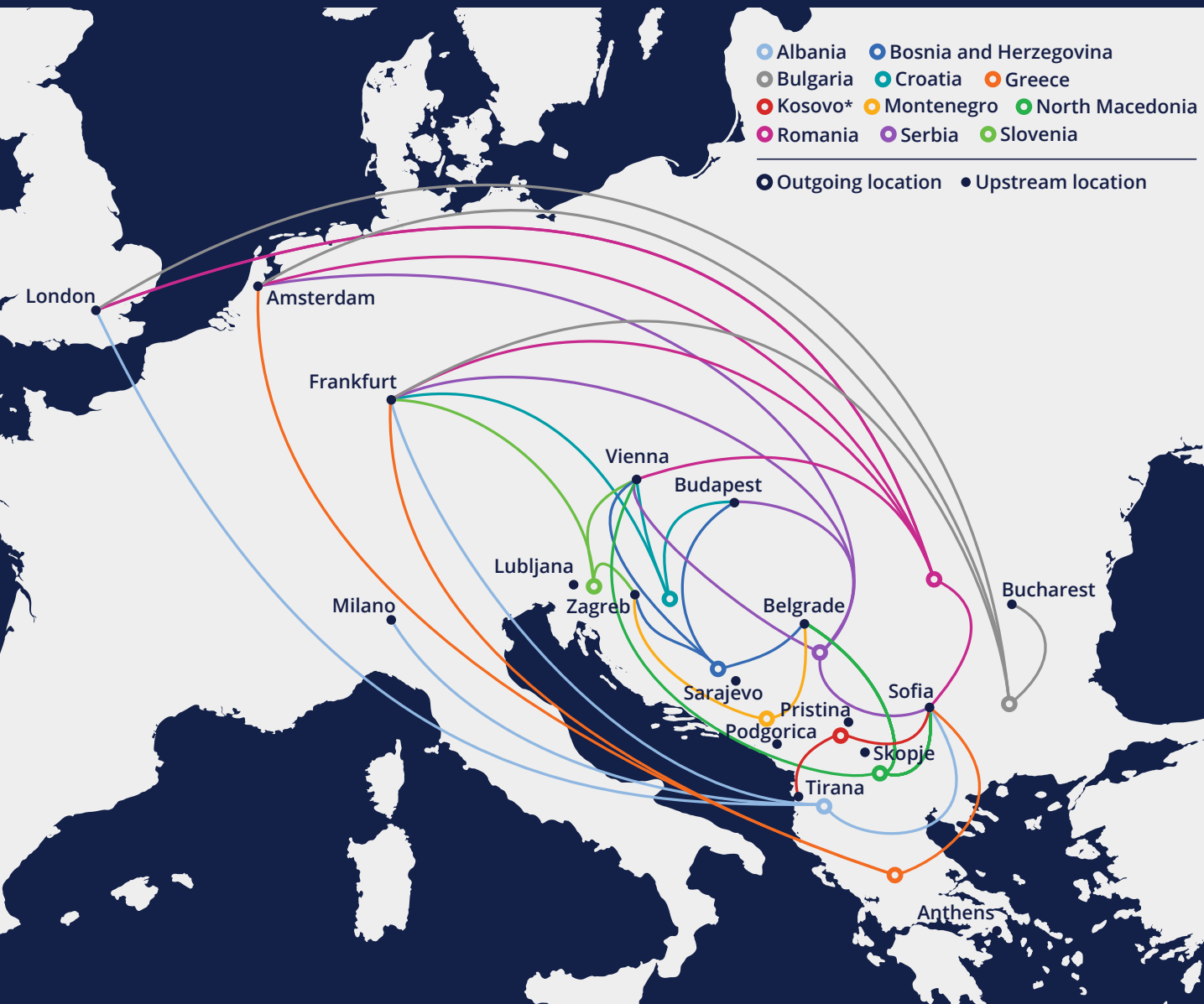
To better understand the regional landscape and assess current traffic patterns, we carried out a series of traceroute measurements using RIPE Atlas probes located across the region. The aim was to see how often the paths between probes remained within the region as opposed to leaving SEE and returning through external circuits. Figure 12 shows the paths from the traceroutes' results.

A closer look at the region (Figure 13) shows more details.

In total, 40,833 IPv4 paths were observed, of which roughly 79% remained within the region, while 21% left the SEE region.

Of all paths, 38% crossed over one or more SEE IXPs, demonstrating the important role they play in local and regional interconnection. The IXPs most frequently observed in the measurements were NetIX Sofia, InterLAN, SOX, and BIX.BG, highlighting the critical hubs that currently facilitate traffic flows across the region. At the same time, a small share of

Figure 14:
Key Interconnection Hubs for Top SEE Operators



total paths (3%) traversed a SEE IXP but also left the region before returning. Our data further indicates that international hubs in Western and Central Europe, such as Vienna and Frankfurt, continue to play a significant role in interconnecting some SEE networks. As a disclaimer, we acknowledge that the distribution of RIPE Atlas probes across the SEE region is uneven, which impacts the number of observed paths.

To verify these findings, we looked at which IXP locations the top SEE operators were connecting. As anticipated, we saw Vienna, Frankfurt – both out of region – and Sofia stand out as key interconnection gateways, reflecting a combination of historical transit routes and strategic peering choices. Smaller markets, or those still expanding their domestic infrastructure, such as Kosovo* and Albania, tend to rely on nearby hubs in neighbouring countries, whereas larger markets, including Serbia and Romania, maintain multiple paths to enhance both connectivity and resilience. The findings are shown on the map below, with arrows representing the most commonly seen traffic paths (Figure 14).

**This designation is without prejudice to positions on status, and is in line with UNSCR 1244/1999 and the ICJ Opinion on the Kosovo declaration of independence.*



Figure 15:
Top SEE ISPs Present at IXPs in the SEE Region

	Number of regional operators at SEE IXP(s)	Total capacity (in G)	Number of markets top ISPs operate from
Albania	0	0	0
Bosnia and Herzegovina	0	0	0
Bulgaria	6	191	4
Croatia	3	40	2
Greece	1	1	1
Kosovo*	0	0	0
Montenegro	0	0	0
North Macedonia	2	20	2
Romania	1	20	1
Serbia	1	10	1
Slovenia	0	0	0

As a complementary perspective in Figure 15, we mapped the presence of the largest ISPs in each SEE market at regional IXPs.

The analysis shows that most operators are only connected at their national exchanges, limiting the potential for regional traffic exchange. Notable exceptions are the exchanges in Belgrade, Sofia and Bucharest, which attract networks from multiple countries and are emerging as regional interconnection hubs. These findings suggest that while local peering remains the norm, a small number of strategically located IXPs play a broader role in facilitating regional connectivity.

To further explore this, we used another set of RIPE Atlas SEE region probe measurements. This time we measured the performance and latency of the connections originating from the probes towards certain destinations hosted in regional IXPs.

We conducted three traceroute measurements targeting:

- A global CDN hosted at BIX.BG
- A European-based cloud and hosting provider at InterLAN
- A regional cloud provider at SOX

Across all tests, latencies remained consistently low for most of SEE, generally below 20 ms. Minor variations were observed in a few cases, such as Kosovo*, Bosnia and Herzegovina, and Montenegro, particularly when accessing the European cloud provider.

We also observed some variation within countries. Even when most probes reported low latency, a few, particularly those outside major cities, showed higher latency. This likely reflects gaps in domestic infrastructure, such as

*This designation is without prejudice to positions on status, and is in line with UNSCR 1244/1999 and the ICJ Opinion on the Kosovo declaration of independence.



limited fiber coverage or last-mile constraints, and suboptimal routing or limited local peering. Probes in Greece, in particular, consistently experienced higher latency to others in the SEE region, highlighting comparatively limited connectivity between Greece and the rest of the region.

These results indicate that content and services, whether global, European, or regional, can be accessed quickly and reliably across the SEE region. They reflect the maturity of the region's IXPs and the effectiveness of both local and some cross-border peering in supporting high-performance connectivity. The generally low latencies also reflect the investments many ISPs have made in infrastructure to reach major 'nearby' interconnection hubs, such as Frankfurt, Vienna, and Budapest. These hubs allow operators to exchange intra-SEE traffic and then leverage the same infrastructure to route it efficiently back to its intended destination.

On a global scale, SEE's IXPs have the potential to decentralise Internet traffic by reducing reliance on major international gateways such as Marseille and Sicily in the Mediterranean Sea. This decentralisation mitigates the risks associated with congestion, outages, or other disruptions at these key transit points and strengthens the overall stability of the global Internet.

5. Summary and future outlooks

5.1 Looking ahead

We do not expect to see a significant growth in the number of IXPs established in the SEE region as the market seems saturated and local connectivity remains highly concentrated in several of the observed countries, which creates considerable barriers to entry for new players.

Saying this, countries with large geographical and demographical distribution could see an increase in the move towards a distributed IXP platform, where the same IXP operator has an interconnected presence in different cities. This is already happening in Serbia and Romania where SOX and InterLAN-IX have a presence at facilities in five different cities, respectively. We expect to see more of this happening across the region should the access conditions to fiber and local connectivity become more favourable.

The landscape for regional interconnections is not expected to change drastically in the next few years given that operators in the region can easily reach major data hubs like Vienna and Frankfurt and a lack of significant regional cross-border content platforms operating in the SEE region. The absence of regional zones and POPs of big cloud and content providers in the region (except for Bulgaria and

Greece) also slows the market's appetite to put pressure on easing existing constraints on the cross-border connections.

5.2 Recommendations from the field

From mid-2024 to mid-2025, we surveyed a number of IXP operators and managers in the SEE region to collect their first-hand experience in running exchanges, registering both their strengths and potential areas of improvements. We observed the following:

- Some IXPs - especially those run as a side project or as an “ad-hoc” service provided by a research centre or university - will need to reevaluate their operations in terms of resources and personnel needs should they want to guarantee a sustainable operational model of the exchange. Such a model would allow growth and future expansion if needed
- It is essential to establish open participation and peering policies that welcome all networks, regardless of size or scope, to peer at IXPs. Removing restrictions on network eligibility fosters a more inclusive environment, encouraging a diverse array of participants and promoting a richer exchange of data. This is a common theme we identified earlier when doing the study for the Middle East countries

- The need for more investments in carrier-neutral data centers and hosting facilities in the SEE region. This would make establishing and connecting to an IX easier, and it also encourages content players and service providers to come and peer at the same location and reach as many networks as possible, instead of doing it in a fragmented manner elsewhere. This neutrality ensures fair competition among participants at IXPs, fostering an environment where networks of all sizes can connect and exchange data without facing undue biases or restrictions. This should be coupled with cheap and ubiquitous access to fiber backhauling across the whole country, without being limited to the big cities only
- A considerable number of IXPs are building their 'future' plans around the objective of attracting international content players to the exchange. While this is an understandable and positive ambition, tying the success (and ultimately the survival) of the exchange to this goal primarily is not a healthy situation. Exchanges should instead turn their focus inwards and invest in developing stronger local communities around them by bringing all the relevant networks to the exchange while working on promoting better peering policies



between its members, extending connectivity to the small operators and conducting capacity building initiatives. The bigger the mass and volume of data generated by locally connected networks, the more attractive the exchange will become for outside networks to come and connect there

- There is a lack of IT talent in some parts of the SEE region which ultimately reflected negatively on the operations of the IXP both internally and externally. Internally, the IXP needs technical people to run and maintain the exchange but who can also be community champions and pioneers that have the time and capacity to reach out to local players and convince them to come and peer at the exchange. Externally, operators and service providers need experienced peering personnel who recognise the importance of a healthy and resilient peering strategy, emphasising the need to offload traffic locally when possible, preferably at the IXP, instead of carrying traffic needlessly over long distances. Absence of such talent at either side will be detrimental for the good operations of the IXP. The RIPE NCC has dedicated considerable resources for technical capacity building initiatives in the SEE region in order to fill the gaps and highlight the industry's best practices
- The involvement of governments and

regulatory bodies in the operations of the IXPs is not homogeneous across the region, which is normal since countries have different regulatory frameworks. Generally speaking, IXPs do not need special licences to operate, which is a good thing that can encourage new players. However, there are over-reaching frameworks that might affect the operations of the IXP in some countries, especially for those operating in an EU country. For example, the NIS-2 directive might have an impact on the obligation and daily activities of some of the IXPs depending on the size or role these IXPs are fulfilling in their respective countries. Keeping an eye on this space will be important to determine the real impact such regulations will ultimately have on the IXP landscape



Appendix 1 - Operator matrix (March 2025)

		Slovenia	Croatia	Bosnia and Herzegovina	Serbia	Montenegro	Romania			Bulgaria						Albania	North Macedonia	Greece					Kosovo***
		SIX	CIX	BHPIX	SOX	MIXP	InterLAN	RoNIX	BALCAN-IX	BIX.BG	NetIX	B-IX (Balkan-IX)	MegaIX Sofia	Varna IX	T-CIX	ANIX	IXP.mk	GR-IX: Athens	GR-IX: Thessaloniki	SEECIX	THESS-IX	NetIX Greece	KOSIX
Slovenia	AS5603	200G																					
	AS3212	200G																					
	AS34779	200G	10G							10G													
	AS21283	40G																					
	AS9119	10G	10G		10G					10G							10G						
Croatia	AS5391		30G														10G						
	AS15994		80G																				
	AS205714		200G																				
	AS44306		80G																				
Bosnia and Herzegovina	AS25144																						
	AS9146			20G																			
	AS42560																						
	AS20875																						
Serbia	AS8400				400G						20G												
	AS31042		20G		400G		10G		10G	20G	20G												
	AS15958				200G																		
	AS9125				40G																		
	AS44143				Capacity unknown																		
Montenegro	AS43940					Capacity unknown																	
	AS15397					Capacity unknown																	
	AS8585					Capacity unknown																	
Romania	AS8708						100G																
	AS9050						10G		40G		10G												
	AS12302							10G															
	AS8953						100G	100G															
Bulgaria	AS8866									20G	100G	10G		10G					1G				
	AS8717									200G	20G	20G		10G									
	AS29244									100G				1G									
Albania	AS42313																						
	AS50973															1G							
Kosovo***	AS206262																						10G
	AS21246																						10G
	AS33983																						10G
	AS29170																						10G
North Macedonia	AS6821																10G						
	AS43612																10G						
	AS34772										100G						1G						
	AS41557																10G						
	AS34547																10G						
Greece	AS6799																	800G	20G				
	AS3329																	600G	200G				
	AS25472																	200G	10G	10G			
	AS1241																	200G	10G				

*This designation is without prejudice to positions on status, and is in line with UNSCR 1244/1999 and the ICJ Opinion on the Kosovo declaration of independence.

**Kosovo does not have an officially assigned ISO 3166 country code, so organisations operating there use the country code of its neighbour in the RIPE Database.



Appendix 2 - Content matrix (March 2025)

	Slovenia	Croatia	Bosnia and Herzegovina	Serbia	Montenegro	Romania			Bulgaria					Albania	North Macedonia	Greece					Kosovo***	Total (in G)	No. IXPs	No. Countries	
	SIK	CIX	BHNIX	SOX	MIXP	InterLAN	RoNIX	BALCAN-IX	BIX.BG	NetIX	B-IX (Balkan-IX)	MegaIX Sofia	Varna IX	T-CIX	ANIX	IXP.mk	GR-IX: Athens	GR-IX: Thessaloniki	SEECIX	THESS-IX	NetIX Greece				KOSIX
Akamai						200			40	100													340	3	2
Amazon									200G								200G						400	2	2
Anexia						10G				10G							10G						30	3	3
BelCloud						20G			40G				1G				10G	1G					72	5	3
Blizzard Entertainment						10G				10G													20	2	2
ByteDance				200		100G				100G													400	3	3
CacheFly						10G	10G																20	2	1
Cloudflare		40		40		100G	10G	10G	20G	200G	100G	10G		10G		20G	400G	10G	10G		100G		1080	15	6
Delta Cloud									300G	100G													400	2	1
Edgoo	10																						10	1	1
Fastly									200G														200	1	1
Google				80		200G	40G		600G	400G	20G	20G		20G									1380	8	3
Hetzner Online				100						200G													300	2	2
Huawei							20G																20	1	1
i3D.net						100G		10G															110	2	1
M247				10		20G	10G	60G		10G													110	5	3
Mainstream				40																			40	1	1
Meta				400		200G	200G	200G	200G	420G	400G	20G		20G	30G								2090	10	4
Microsoft		40				20G		200G	200G	100G		10G					200G		20G				790	8	4
Netflix						100G	100G								10G*								210	2	2
OVHcloud										100G													100	1	1
Riot Games									10G	10G	10G	10G					10G						50	5	2
Softnet	10	10		10					10G							10G							50	5	5
Sony																	10G						10	1	1
Valve				200		100G				100G													400	3	3
Yahoo!								10G	20G	10G													40	3	2

*This designation is without prejudice to positions on status, and is in line with UNSCR 1244/1999 and the ICJ Opinion on the Kosovo declaration of independence.

**Kosovo does not have an officially assigned ISO 3166 country code, so organisations operating there use the country code of its neighbour in the RIPE Database.

Source: [PeeringDB](#)



www.ripe.net