Scanning the IPv6 Internet Using Subnet-Router Anycast Probing

MAYNARD KOCH, TU Dresden, Germany
RAPHAEL HIESGEN, HAW Hamburg, Germany
MARCIN NAWROCKI, NETSCOUT, USA
THOMAS C. SCHMIDT, HAW Hamburg, Germany
MATTHIAS WÄHLISCH, TU Dresden, Germany

Identifying active IPv6 addresses is challenging. Various methods emerged to master the measurement challenge in this huge address space, including hitlists, new probing techniques, and AI-generated target lists. In this paper, we apply active Subnet-Router anycast (SRA) probing, a commonly unused method to explore the IPv6 address space. We compare our results with lists of active IPv6 nodes obtained from prior methods and with random probing. Our findings indicate that probing an SRA address reveals on average 10% more router IP addresses than random probing and is far less affected by ICMP rate limiting. Compared to targeting router addresses directly, SRA probing discovers 80% more addresses. We conclude that SRA probing is an important addition to the IPv6 measurement toolbox and may improve the stability of results significantly. We also find evidence that some active scans can cause harmful conditions in current IPv6 deployments, which we started to fix in collaboration with network operators.

CCS Concepts: • **Networks** → **Network measurement**; **Network structure**; **Network security**; **Network protocols**; **Public Internet**; **Routers**.

Additional Key Words and Phrases: IPv6, BGP, scanning, routing loops, subnet-router anycast

ACM Reference Format:
Maynard Koch, Raphael Hiesgen, Marcin Nawrocki, Thomas C. Schmidt, and Matthias Wählisch. 2025. Scanning the IPv6 Internet Using Subnet-Router Anycast Probing. *Proc. ACM Netw.* 3, CoNEXT4, Article 50 (December 2025), 15 pages. https://doi.org/10.1145/3768997

1 Introduction

Internet research often relies on measurements, which in turn require a representative picture of its population for interpretation. In IPv4, researchers commonly make use of probing the entire address space, which is quickly achievable thanks to stateless scanning [7]. The huge IPv6 address space renders related approaches impossible, leaving measurement researchers with a largely unknown object of investigation.

About a decade ago, the community started to counter this restriction by collecting active IPv6 addresses [36]. Since 2016, the TU Munich (TUM) assembles a comprehensive hitlist of active IPv6 nodes [13], which established as a highly valuable community service. Since then, a significant research body has built upon the TUM Hitlist as input to various IPv6 measurement studies.

Authors' Contact Information: Maynard Koch, TU Dresden, Dresden, Germany, maynard.koch@tu-dresden.de; Raphael Hiesgen, HAW Hamburg, Hamburg, Germany, raphael.hiesgen@haw-hamburg.de; Marcin Nawrocki, NETSCOUT, Westford, MA, USA, marcin.nawrocki@netscout.com; Thomas C. Schmidt, HAW Hamburg, Hamburg, Germany, t.schmidt@haw-hamburg.de; Matthias Wählisch, TU Dresden, Dresden, Germany, m.waehlisch@tu-dresden.de.

ACM 2834-5509/2025/12-ART50
https://doi.org/10.1145/3768997

However, scalable IPv6 scanning that does not rely on external input sources other than BGP announcements remains an unsolved challenge.

In this paper, we reconsider state-of-the-art IPv6 scanning approaches and propose a rarely used method, Subnet-Router anycast (SRA) probing, to explore the IPv6 address space. In SRA probing, a scanner sends packets to an IPv6 address that represents a potential subnet prefix and all host bits are set to zero, *e.g.*, the SRA address of `2001:db8:1::/48` is `2001:db8:1::`. Unlike probing random addresses, SRA probing significantly reduces the impact of ICMPv6 error message rate limiting, as this method triggers ICMPv6 Echo replies from routers operating interfaces directly connecting the probed subnets.

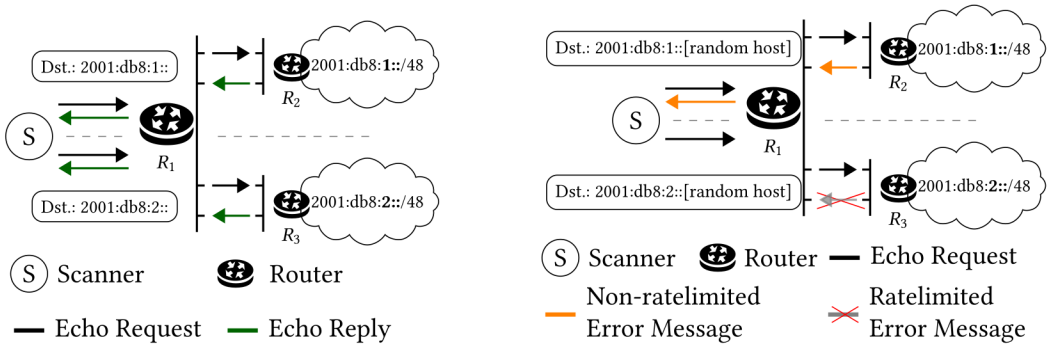
The remainder of this paper is structured as follows.

(1) We introduce Subnet-Router anycast probing and partition the routable IPv6 address space into smaller subnets (§ 3).
(2) We provide detailed insights into our measurement results (§ 4). Our findings show that SRA probing finds on average 10% more addresses than random probing for routers in active subnets. SRA probing discovers 80% more addresses compared to targeting router addresses directly. We observe varying response rates for ICMPv6 Echo Reply messages between 1.3% and 35.2% depending on the targeted subnet set.
(3) We compare our SRA probing results to popular public datasets as well as passively collected IXP flowdata (§ 5). The majority (97%-99.9%) of IPv6 addresses we discover with SRA probing are not contained in any of the datasets we use for comparison.
(4) We discover a critical amplification threat related to scanning the current IPv6 infrastructure (§ 6) and report about mitigation with operators.

We conclude from our findings that our current perspective on the operational IPv6 Internet is still largely incomplete and further efforts are needed to overcome our limited view (§ 7).

2 Background and Related Work

Subnet-Router anycast addresses. Subnet-Router anycast (SRA) addresses have been originally introduced in RFC 1884 [16] in 1995. Since then, they are integral part of IPv6 [17, §2.6.1]. SRA addresses enable applications to communicate with a router of the subnet, without knowing the actual IPv6 router address.



(a) SRA probing.

(b) Random probing.

Fig. 1. IPv6 Scanning based on different probing methods. Random probing leads to ICMP error message rate limiting (at R_3), therefore we discover more router IP addresses with SRA probing because SRA elicits ICMP Echo replies instead of ICMP error messages.

Table 1. Overview of active and passive IPv6 measurement methods considered in this work.

Method	Discovery of	Observed Addresses [#]
Random Probing	Router (Core)	1.3M [2], 9.5M [4]
	Router (Periphery)	64M [32], 52M [21], 44M [18]
Hitlist	Active End Hosts	20M [25]
IXP Flows	Active End Hosts	146M [13], 198M (this work)
SRA Probing (this work)	Router (Core and Periphery)	133M

Syntactically, SRA addresses are unicast addresses. They represent the subnet, *i.e.,* the host part of the IPv6 address is set to 0, *e.g.,* for `2001:db8:1::/48` the SRA address is `2001:db8:1::0`. Each router is required to support a Subnet-Router anycast address if it has an interface to this subnet. Routers receiving a packet targeting an SRA address of one of its subnets should reply with their own full source address. For example, a router with the two interfaces `2001:db8:1::2/48` and `2001:db8:10::2/48` receives a packet to `2001:db8:1::0` via its interface `2001:db8:10::2/48` will reply with the source address `2001:db8:10::2`. Notably, a router is not required to reply, there are behavioral differences of SRA implementations [6]. We illustrate SRA probing in Figure 1(a), in contrast to random probing (see Figure 1(b)) we circumvent ICMP error message rate limiting at R_1, thus we discover more router addresses with SRA probing. We will make use of SRA addresses to explore new active subnets and new IPv6 router addresses. So far, only very limited insights into this approach exist [3], and we provide the first comprehensive measurements.

Active measurements. A full scan of the IPv6 address space is not scalable. Therefore, active measurements, which send probe packets to specific target addresses, try to limit the scope of targets. A straightforward option is to send one probe packet to any IPv6 prefix visible in public BGP dumps [4, 8, 30, 39]. This reduces probing (*i.e.,* addresses) but is relatively selective since BGP announcements include larger covering prefixes of more specific active subnets. To broaden coverage, prefixes available in BGP are split into equally sized, more specific prefixes, usually of size `/48` or `/64`.

When deciding on the actual target address, there are currently three principal options. (*i*) Select a random address within a given (sub)prefix. (*ii*) Select an address from a hitlist. (*iii*) Artificially generate addresses by extrapolating knowledge about assignment of IPv6 addresses.

Targeting a random address has very high chances of not reaching an active end host address, instead replies rather reveal routers. Holzbauer *et al.* [18] show that related ICMP error messages issued by routers can be used to get a better understanding of active networks. Selecting an address from a hitlist is often combined with traceroute measurements to discover nodes (*i.e.,* router, middleboxes) between source and destination. Tools such as ZMapv6 [11], XMap [21], and Yarrp [1, 14] provide those capabilities for IPv6. Low-byte addresses such as `<Prefix>::1` reflect a common assignment pattern. CAIDA Ark [4] and RIPE Atlas [30] are distributed measurement platforms that regularly target low-byte addresses. Target Generation Algorithms (TGA) try to discover more advanced structures to predict other potentially active addresses [10, 36]. Steger *et al.* [35] evaluated the hit rate of TGAs compared to the TUM Hitlist. One fundamental challenge of those approaches is that they require seeding, usually based on knowledge gathered via passive or other active measurements—the output depends on the input. We give an overview of active probing techniques and the number of discovered addresses in Table 1.

Challenges in active measurements. Active scans face the challenge of ICMP rate limiting [27, 28] since ICMPv6 [5] requires that a node must limit the rate of ICMPv6 error messages it originates.

Such rate limiting can cause irregular on-off behavior of routers [28], therefore, impacting the reliability and stability of scan results. This harms not only scans targeting locally unreachable networks ("No Route to Destination") but, in particular, random addresses ("Address Unreachable"). We tackle this challenge by targeting Subnet-Router addresses—addresses to which one router should always reply with an ICMPv6 Echo instead of an error when the network is active.

Passive measurements. Passive measurements derive active IPv6 addresses by observing IPv6 communication or finding additional hints that refer to potentially active IPv6 addresses. Those approaches include the analysis of server logs of common services such as NTP pools [31], or exploit non-existing [9] or existing [2, 32, 38] IPv6 DNS records based on reverse DNS or common names, *e.g.,* derived from top lists [33] or TLS certificates publicly available in CT logs [13].

Those and other sources are compiled in the TUM Hitlist [13, 35, 41], the most popular public list of active IPv6 addresses, which serves in many studies as a point of reference (*e.g.,* [19, 34, 38, 40]). The initial data set of the 2016 TUM Hitlist contained IPv6 addresses based on passive flow data captured at a large Internet Exchange Point. Their IXP collection comprises 146M unique IPv6 addresses (see Table 1)

In our study, we compare the addresses contained in the TUM Hitlist and our one-month address collection from the IXP with the addresses we discover through SRA probing (see Table 1).

3 Measurement Method and Setup

We propose Subnet-Router anycast probing, an IPv6-compliant approach using ICMPv6 Echo requests. This active, controlled measurement aims for detecting routers at the Internet core and edge, depending on the probed subnets. Little to no attention has been paid to scanning SRA addresses to unveil IPv6 router infrastructure.

Prior active methods to explore the IPv6 space [1, 2, 18, 21, 32, 39] rely on random probing of the IPv6 address space. While targeting unassigned addresses leads to ICMPv6 error messages, these messages only give an incomplete picture due to ICMPv6 error message rate limits [5]. We instrument SRA addresses to mitigate rate limiting in our measurements since requesting these addresses triggers ICMPv6 Echo replies. We now describe our method and setup to deploy large-scale SRA scans.

3.1 Subnet-Router Anycast Probing

Querying Subnet-Router anycast (SRA) addresses should trigger an ICMPv6 Echo reply from a router that has an interface for the respective subnet. To successfully deploy our probing, we need to partition the IPv6 address space such that each partition represents an active subnet, cope with IPv6 aliasing, and map a reply to the original request since the source address of the replying router may be unrelated to the targeted subnet.

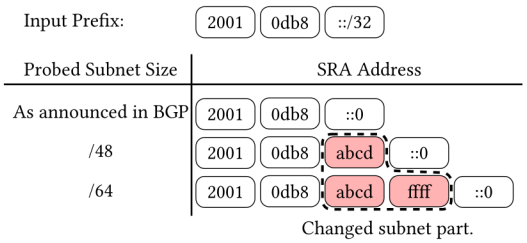


Fig. 2. Example construction of a single SRA address for every target subnet given a single input prefix.

Partitioning the address space announced in BGP to create SRA addresses. At the time of writing, approximately 200k IPv6 prefixes are announced in BGP. Probing the Subnet-Router anycast address of each routable prefix as it is announced in BGP misses internal, more specific subnets. To balance scan traffic and increase the chance of discovering new addresses, we partition the routable address space into three stages. We start by querying the SRA address of each announced prefix (Stage 1). Then, we partition the routable address space into /48 subnets (Stage 2) and scan the SRA

Table 2. Comparison of different input sets to probe Subnet-Router anycast addresses and their effectiveness for SRA probing. The hitlist input reveals the most router IP addresses while probing only 700M SRA addresses.

Input for probing				Results	
Source	Subnets [#]	Subnet-size	Addr. [#]	Replies [#]	Router IPs [#]
BGP (All)	200k	As announced	200k	38k (19%)	28k (14%)
BGP (All)	200k	/48	11B	350M (3.2%)	4M (0.04%)
Route(6) (All)	1M	/64	10B	570M (5.7%)	14M (0.14%)
BGP (/48)	100k	/64	6.5B	1.3B (20%)	45M (0.69%)
Hitlist (Unique /64s)	700M	/64	700M	90M (13%)	72M (10.3%)
Total			28.2B	2.32B	135M (Distinct 133M)

address of each subnet. Even though common routing policies should prevent announcements more specific than a /48, we found 3k prefixes more specific than /48. In these cases, we scan the SRA address of the /48 supernet, unless it is included in another announcement. Partitioning into /48 subnets results in 15 billion potential targets. Finally, we partition all /48 announcements (≈100k) further into /64 subnets (Stage 3). This step generates +≈6.8 billion target addresses for scanning.

For each stage, we construct the target addresses as follows. In Stage 1, we leave all bits of the given input prefix unchanged. In Stage 2, we create all bit combinations of the first 16-bit block that follows the original subnet prefix, which yields 2^{16} new addresses per input prefix. In Stage 3, we take the subsequent 16-bit block into account and generate all possible 2^{32} combinations to construct SRA addresses for probing. As the number of addresses to probe grows exponentially, we limit the third stage to only use `/48` announcements and do not generate addresses more specific than a `/64`. We employ this multi-stage approach to determine which input set is most suitable for SRA probing. Figure 2 shows an example address for each stage given the input prefix `2001:db8::/32`.

Creating SRA addresses using other input sources. BGP announcements reflect intended reachability. There are, however, other sources containing more specific subnet assignments, which can be used to leverage the effectiveness of our method. In addition to BGP announcements, we consider two input sources to create SRA addresses. First, we collect `Route(6)` objects from IRR databases, which predominantly contain /48 prefixes. For each of the nearly 1M prefixes, we create up to 10k random /64 SRA addresses, adding up to 10B targets. Second, we construct a target set from the TUM Hitlist (2.5B addresses) by taking the first 64 bits of each host address and set the remaining 64 bits to zero, which results in 700M distinct targets.

IPv6 Alias Resolution. In IPv6, operators may configure their networks as aliased, which means they reply to, *e.g.,* ICMPv6 Echo requests on any address. Several studies have investigated this effect and developed methods to detect if a subnet is aliased or not [12, 22]. To overcome this issue in our measurements, we make use of the fact that SRA addresses are typically not assigned to hosts; therefore, we filter for replies that originate from the same source we requested (the `::0` address), as this is an indicator for an aliased network. Additionally, we check whether the remaining source IP addresses are part of the aliased prefix list provided by the IPv6 hitlist service [25]. Our approach reduces the impact of aliased prefixes and serves as a trade-off to maintain high scan performance. We are aware of the limitation that this approach may misclassify a small portion of addresses, but we consider the impact to be negligible.

Capturing replies. We need to match the target IP address in our probing packet (*i.e.,* the SRA address) to the replying IP address (*i.e.,* the router IP address). To that end, we encode the target SRA address in the ICMPv6 payload and extract it from the incoming reply. This takes advantage of

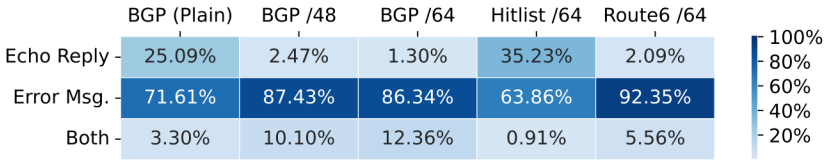


Fig. 4. Relative ratio of ICMP replies, grouped into Echo replies, error messages, and ambiguous values for router IP addresses that sent error messages for some probed subnets and ICMPv6 Echo replies for others.

ICMP, which includes parts of the original request in the reply. In addition to ICMPv6 Echo replies, we capture any type of ICMPv6 error message such as "Time Exceeded" or "No Route to Host".

Activity of router addresses. Hitlists focus on active host discovery. To that end, we inspect the activity of all found addresses–from both, ICMPv6 Echo replies and ICMPv6 error messages–by probing them once a day over the course of a week from November 5 to November 13, 2024. We report on our findings in Section 4.

Stability of SRA probing. To better understand the effectiveness of SRA probing, we inspect if re-probing the SRA address elicits a response from the same router IP address. While changes may indicate a network change, they would significantly impact the reliability of results obtained from SRA probing. Therefore, we re-probe the `/64` SRA addresses we created based on the TUM Hitlist in six scans, distributed over two days, and analyze the stability of the found addresses.

3.2 Measurement Setup

We perform our active probing in October and November 2024 and repeat one SRA BGP (only `/48`) scan in February 2025. When using input sources other than BGP, *e.g.,* the TUM Hitlist, we ensure that datasets are aligned in time. We use a single vantage point located in Europe, connected to a large IXP and with 1Gbit/s upstream. Neither we nor our upstream filters traffic. For active probing, we use a fork of the TU Munich ZMapv6 tool [11] with a modified version of the ICMPv6 Echo scan module and a custom GO implementation as an address generation tool, serving as input for ZMap. We limit the scan rate to 200k packets per second. We perform each scan at least twice, the re-probing of the found router IP addresses is done seven times, and we run SRA probing of the TUM Hitlist `/64` six times. The final list of router IP addresses is compiled from the initial scan of each input source.

Metadata mapping. We use the free MaxMind GeoIP database [24] to map source IP addresses to countries, the RouteViews dataset [37] to map IPv6 addresses to Autonomous System Numbers (ASNs), and the IPinfo ASN database [20] to identify the types of Autonomous Systems (ASes) associated to router IP addresses we reveal with SRA probing.

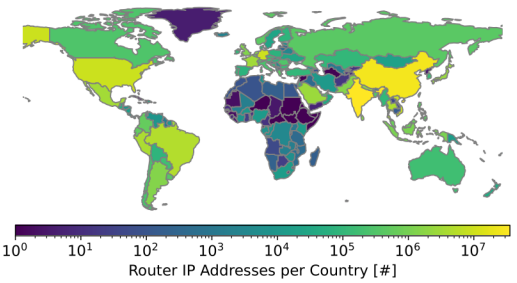


Fig. 3. World-wide distribution of router IP addresses found with SRA probing.

4 Subnet-Router Anycast Measurements

We probe more than 28B Subnet-Router anycast addresses in 5 scans, observing more than 2.3B replies from 133M distinct IP addresses distributed in over 218 countries (see Figure 3) with a strong bias towards India (27%) and China (20%). We observe widely varying response rates per scan, ranging from 3.2% (BGP /48) up to 20% (BGP /64). The ratio between newly discovered routers and probed IP addresses strongly depends on the input source, see Table 2. With 72M unique router

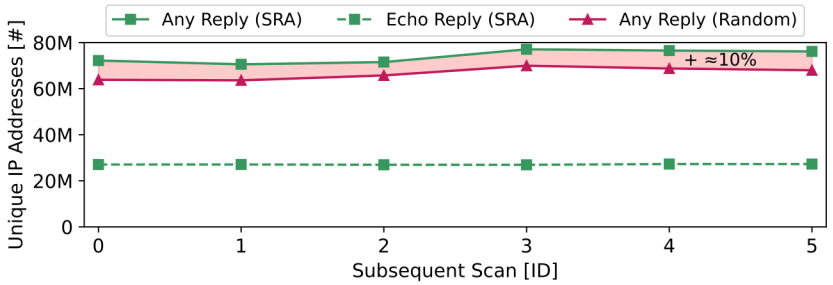


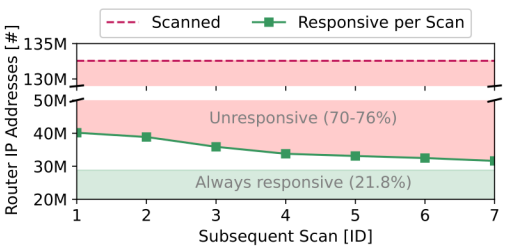
Fig. 5. Comparison of SRA vs. random probing of all /64s from the TUM Hitlist. With SRA probing, we observe ≈ 10% more addresses than with random probing. While the total number of replies varies, the number of Echo replies remains stable.

IP addresses discovered by sending only 700M requests (all unique /64s generated from the full TUM hitlist) the discovery rate exceeds 10% while it remains below 1% for all other scans, except for the plain BGP prefix scan, which shows a higher reply rate in relative terms. With only 28K router IP addresses and an overlap of >90% with the other scans, the effect is negligible. The reason for that is that the different data sources provide different types of networks. Generating more specific subnets based on BGP (or `Route(6)`) input data, usually leads to subnets that are not assigned to any router interface, triggering many ICMP error messages when probed. On the other hand, the /64 subnets resulting from the TUM Hitlist are not artificially generated but cut-off from the host address of an (at least at some point in the past) active host. Therefore, it is much more likely that the probed subnet is active and assigned to a periphery router, which throws no error message but responds with an ICMPv6 Echo reply.

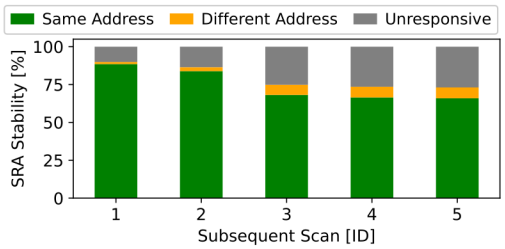
ICMP Response Types. Figure 4 illustrates the per scan distribution of Echo replies vs. error messages. While we receive more error messages in general, the `Route(6)` /64 scan receives more than 92% error messages for probed subnets. The reason for that lies in the random generation of 10k /64 subnets. Nearly 50% of the `Route(6)` objects announce a /48. This means that the random subnet generation covers only 15% of the possible /64 subnets for a single /48. Our observations also imply that these subnets are sparsely populated. We observe the highest Echo reply rates (35%) for the Hitlist /64 scan—probing the periphery of a network is far more effective in case of SRA probing. This confirms our prior assumption that deriving SRA addresses from active devices increases chances to hit a subnet router, which ultimately leads to significantly more Echo replies.

Advantage of SRA probing. SRA probing shows full advantage when re-probing active subnets. Consecutive scans are not affected by common ICMP error message rate limiting [27, 28] since sending probes to an enabled SRA address will trigger an ICMP Echo reply message, independently whether the router IP address changes or not. Random probing, on the other hand, triggers ICMP error messages (*e.g.,* "Address Unreachable") when a successfully probed random address changes in the future, and too many error messages will be suppressed. Additionally, the chance to hit an active device at all using a random IPv6 address is almost zero.

Figure 5 shows the total number of discovered router IP addresses based on SRA and random probing for a measurement series using the Hitlist /64 subnets. Per scan campaign, we find about 10% more router IP addresses with SRA probing. The number of router IP addresses that respond with an Echo reply message remains stable, which clearly shows that our SRA scans are far less affected by ICMP rate limiting. We also find $\approx 9M$ router IP addresses exclusively with SRA probing, which strengthens the use of SRA probing. The overlap of two consecutive scans, however, remains at a steady level but is below 70%. The observability of a router IP address is highly influenced by ICMPv6 rate limiting.



(a) Visibility, *i.e.,* probing the router IP addresses directly. 28M router IP addresses replied to Echo requests in any scan.



(b) Stability, *i.e.,* re-probing SRA addresses. For at least 66%, the same SRA address triggered a reply from the same router IP address in all scans.

Fig. 6. Visibility and stability of the discovered router IP addresses.

Visibility and stability of router addresses. Stability of addresses is an important factor when creating hitlists. To better understand the potential of SRA scanning in finding router addresses that remain reachable, we analyze if we (*i*) elicit a response when probing the router IP address directly and (*ii*) trigger a response from the same router IP address when re-probing the same SRA address. We re-probe all router addresses found in each SRA scan every day for a week and re-probe the Hitlist /64 SRA addresses six times within 2 days. Figure 6(a) illustrates the churn of detected router IP addresses. Only 28M out of 133M addresses always reply to Echo requests. However, we observe a significantly higher stability when re-probing the SRA address (see Figure 6(b)). After two days, we observe 66% of the probed SRA addresses to still reveal the same router IP address as before, changes are rare (max. 7%), and we do not elicit a response for the same SRA address for about 27% in the last scan. Re-probing after three months revealed that while for 18% the SRA address reveals another router IP address, about 40% of the router IP addresses are still reachable via the same SRA address. These results show that most routers do not reply to direct ICMPv6 Echo requests but are to a major part reliably discoverable through SRA probing.

Prevalence and stability of ASNs and IPv6 prefixes. The top 5 ASes from which the router IP addresses originate are shown in Table 3. The router addresses we find (first group of columns) cover 16k ASNs, and 11% of the IP addresses originate from the top ASN. We observe a clear bias towards networks in Asia, being more responsive than others. Over the course of our six consecutive scans (not shown), ≈ 87% of the prefixes remain unchanged, leading to a stable set of ASes of ≈ 96%. We further report on the network type distribution in Appendix E.

5 Comparing SRA Probing to Other Datasets

We compare our measurement results with multiple datasets of different characteristics. These datasets are (*i*) publicly available IPv6 traceroute measurements, (*ii*) a popular public hitlist of active hosts, and (*iii*) flow data of one month provided by a large regional Internet Exchange Point (IXP).

We observe little overlap in terms of IP addresses, and each data source reveals a different set of ASNs from which most of the IP addresses originate, signifying the diversity of all collected datasets (see Table 3). Considering all ASNs, however, shows that more than 99% of the ASes found through SRA probing are also present in the other datasets (see Figure 7). We analyze these observations further in this section.

5.1 Comparison with Public IPv6 Traceroute Measurements

We use traceroute data provided by CAIDA [4] and RIPE Atlas [30]. Both datasets are from October 4, 2024 to align in time with our measurement campaign. It is worth noting that we target orders of magnitude more IP addresses (28.8B targets vs 17.7M targets in the CAIDA dataset and

Table 3. Top 5 ASes per data source and the relative share of IP addresses per AS. We highlight ASes from SRA probing that are among the top 5 ASes in at least one other data source (bold font).

	This Work				Traceroute Measurements				Other	
	SRA Probing		IXP Flows		CAIDA ITDK		RIPE Atlas		TUM Hitlist	
Rank	ASN	IP addr. [%]	ASN	IP addr. [%]	ASN	IP addr. [%]	ASN	IP addr. [%]	ASN	IP addr. [%]
1	**45609**	11.15	6805	43.06	36183	15.49	16509	1.93	13335	25.62
2	**9808**	6.07	3209	21.55	16509	11.18	11172	1.89	12322	9.97
3	45271	4.63	8881	8.50	13335	6.04	**9808**	1.78	5607	3.38
4	38266	4.27	16202	6.06	19551	2.96	174	1.58	55836	3.20
5	**4134**	4.12	20880	4.23	**45609**	2.83	1299	1.22	**4134**	1.99

687k targets in the RIPE dataset) and that the methods differ. We argue that the comparison is still appropriate for the following reasons. First, these datasets are common sources of comparison when analyzing IPv6 scanning methods. Second, our measurements take 1.5 days to cover 28.2B SRA addresses. The RIPE Atlas measurements, for example, need 13 days. Even if we probe more targets in our setup, we do not treat other methods unfairly given the number of addresses explored per time. Neither Ark nor RIPE Atlas would be able to scan 28.8B targets, and we are interested in what is possible given the current state of the art and SRA probing.

CAIDA Ark IPv6 Topology Dataset. A globally distributed set of Archipelago (Ark) nodes continuously probes all IPv6 prefixes announced in BGP every 24 hours. Each node sends traceroutes to a single random destination address as well as the address `<prefix>::1` of each prefix. We discover 133M router IP addresses that are not included in the CAIDA data set, and CAIDA discovers 9.4M addresses we do not observe. These observations further motivate the additional benefit of probing SRA addresses since they highly improve topology measurements with additional data.

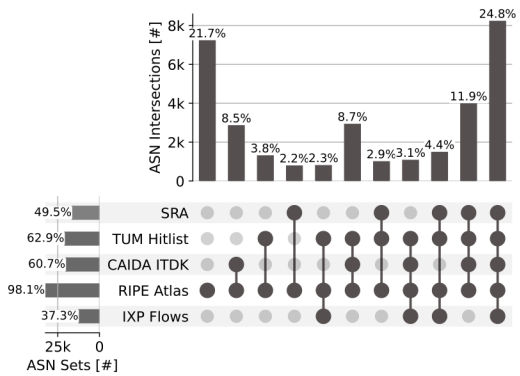
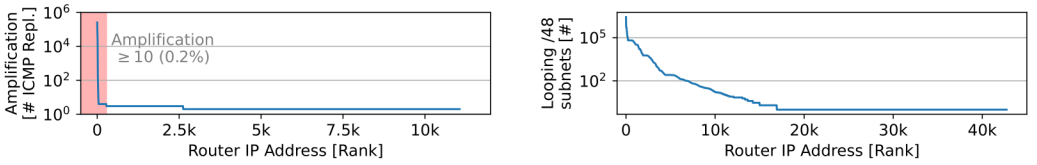


Fig. 7. Overlap of ASes between all data sources. Subsets <2% are not shown but presented in Appendix D.

RIPE Atlas Traceroute Measurements. RIPE Atlas is a measurement platform managed by the RIPE Network Coordination Centre (RIPE NCC) and consists of thousands of globally distributed nodes. Similar to the CAIDA IPv6 Topology Dataset, RIPE Atlas [29] target the `<prefix>::1` address of each prefix announced in BGP.

We base our comparison on data collected by 6549 globally distributed Atlas nodes targeting 624k IPv6 addresses. The Atlas scans reveal 401k router IP addresses, which is only 0.3% of what the SRA probing discovered. On the other hand, we discover only 48.5k router IP addresses that RIPE Atlas also does. Similar to CAIDA, the overlap is minimal, highlighting the benefits of SRA address probing and the potential for combining methods to achieve more comprehensive datasets. In terms of ASes, RIPE Atlas contains a large number of IP addresses belonging to ASes that are not observed in any of the other data sources (see Figure 7). There are two reasons. First, RIPE Atlas probes are deployed in much more ASes than probes of other traceroute projects. Second, routers use different source IP addresses when replying to SRA requests than to traceroute. In the case of SRA, some routers use the peering LAN IP address as source address, which often belongs to the IP address space of the upstream provider, while replies to traceroutes tend to use the IP address of



(a) Amplification factor per router IP address that sends more than one ICMP reply per request. For 98% the amplification factor is ≤ 10. Some few routers, however, amplify single requests by a factor of >200k.

(b) Frequency of /48 subnets that cause a routing loop per router. A few routers create routing loops to more than 100M /48 subnets.

Fig. 8. Overview of routing loops and amplification factors.

the served subnet. Mapping router IP addresses to ASNs is therefore more error-prone in the case of SRA probing.

5.2 Comparison with a Public IPv6 Hitlist

We rely on the TUM IPv6 hitlist service [25]. This service regularly provides a list of active, dealiased IPv6 end-hosts. We compare it to the extended version of the hitlist, which also includes the results of traceroute measurements targeting the collected active hosts, in order to find additional router addresses [13]. We use the hitlist from September 21, 2024, which contains approximately 20 million active hosts. We discover 4.4M addresses to be part in both address sets. 94% of the addresses discovered via SRA probing, however, are unknown to the hitlist. We will provide our data as new source to further improve the coverage of the hitlist service.

5.3 Comparison with IXP Flow Data

We analyze one month of sampled (1:16k) IXP flow traffic. During this period, we observe 2.5B packets from 141M source and 87M destination addresses, resulting in a total of 198M unique addresses, and 35M addresses that appear as both source and destination. In terms of autonomous systems, we observe packets originating from 10k ASNs and targeting 11k ASNs, leading to 12k different ASes. The flow traffic shows a bias towards a few, highly active ASNs that are responsible for more than 60% of our packets (see Table 3).

Comparing our SRA dataset with the IXP flow data, which are aligned in time, we observe only 152k IPv6 addresses (0.2% of our overall data) that are also visible in the flow data.

6 Routing Loops and Amplification

Routing loops [18, 21, 23] and amplification of looping packets [15, 26] are a known problem in IPv6 deployments. We confirm that both problems are still present. They lack attention from the operator community. During our active scans, we discovered a serious bug in the firmware of common router vendors that is triggered by routing loops and can lead to significant amplification. A single ICMPv6 Echo request can result in more than 250,000 replies from the same router. We confirmed our observations with network operators and router vendors. Routing loops, in conjunction with the amplification bug, can be exploited for denial-of-service attacks, posing a significant risk to network security. Our SRA probing allows for careful, more complete discovery of this risk.

Reason for routing loops. Routing loops are caused by incorrectly configured routes between a customer and provider such that packets to inactive subnets of provider aggregated address space assigned to the customer are sent back and forth between customer and provider until the IPv6 hop limit exceeds. This misconfiguration can be fixed easily (details in Appendix C). What concerns us most is that some routers exponentially replicate the looping ICMPv6 Echos, which also leads to an exponentially increasing amplification of Time Exceeded messages.

Figure 8(a) visualizes the distribution of amplification factors gathered during our initial scan using a hop limit of 64 hops. The magnitude of the amplification can be reduced by using even smaller hop limits. To reduce the impact of our scans on the network, we set the hop limit value to 64 for all follow-up measurements.

Prevalence of routing loops and amplification. We use the results from our BGP /48 measurement to analyze the current deployment of routing loops in more detail. We observe 141M /48 subnets to trigger a routing loop. These subnets affect 43k router IP addresses. The majority of the router IP addresses (60%) is responsible for a single subnet that triggers a routing loop, while some few routers connect more than 1M incorrectly configured /48 networks (see Figure 8(b)). Of the 41k router IP addresses affected by routing loops, 11k are also affected by amplification (see Figure 8(a)). These amplifying subnets highly concentrate in Brazil (23%). While 99.8% of the amplification factors are below 10, a few routers amplify single ICMP Echo requests by a factor >100k (see Figure 8(a)). These routers are primarily located in Germany and the US. We provide more details on routing loops and amplification factors across countries in Appendix F.

Responsible disclosure and advice. Packet floods harm performance of routers and links. We argue that the measurement community should consider limiting IPv6 scans of inactive (or unknown) networks given the current state of deployment, as these scans could otherwise lead to loops and unintended consequences. To monitor the current situation, we advise low frequency scans with small hop limits (*e.g.,* 64). To improve the situation, we implemented a responsible disclosure policy and contacted 5340 network operators. Originally, we observed routing loops in 141M /48 subnets, which decreased in 263 ASes by a total of 7.7M loops until May, 2025.

7 Discussion and Conclusion

Visibility. We verified the visibility of all router IPv6 addresses that we found using SRA probing. More than 70% do not respond when queried directly. We argue that these addresses will rarely show up on hitlists because of their unresponsiveness. Some of them could have been discovered by random probing and considering ICMPv6 error messages, which, however, will trigger more likely rate limiting. Overall, reaching statistically reliable statements about the IPv6 population is still an open challenge, but we showed that reconsidering probing techniques may improve the stability of results significantly.

Stability and rate limiting. Rate limiting is a key reason for instability of detected IPv6 addresses. We showed that probing the SRA address of a target subnet provides more stable results than random probing because SRA circumvents rate limiting of ICMPv6 error messages. We observed, however, variations in the number of responses also for ICMPv6 Echo replies. To what extent rate limiting techniques beyond those proposed in RFC 4443 are deployed should be part of future work.

Responsible scanning. Active measurements of inactive address space may lead to significantly amplified traffic. Not all common measurement tools report about this unintended traffic, which then is only visible in raw packet captures. We started to address these problems in collaboration with network operators and vendors. We hope that our data will help to limit this unintended traffic in future research.

Acknowledgments

We would like to thank our shepherd Philipp Richter and the anonymous reviewers. This work was partly supported by the Federal Ministry of Research, Technology and Space (BMFTR) within the projects IPv6Explorer (16KIS1815) and AI.Auto-Immune (16KIS2333 and 16KIS2332K).

References

[1] Robert Beverly. 2016. Yarrp'ing the Internet: Randomized High-Speed Active Topology Discovery. In *Proc. of ACM IMC*. ACM, New York, NY, USA, 413–420. https://doi.org/10.1145/2987443.2987479

[2] Robert Beverly, Ramakrishnan Durairajan, David Plonka, and Justin P. Rohrer. 2018. In the IP of the Beholder: Strategies for Active IPv6 Topology Discovery. In *Proc. of ACM IMC (IMC '18)*. ACM, New York, NY, USA, 308–321. https://doi.org/10.1145/3278532.3278559

[3] Tristan Bruns. 2020. *Network Reconnaissance in IPv6-based Residential Broadband Networks*. Master's thesis. University of Bremen.

[4] CAIDA. 2008. Ark IPv6 Topology Dataset. https://catalog.caida.org/dataset/ipv6_allpref_topology. https://doi.org/dataset/ipv6_allpref_topology Dates used: Oct. 04, 2024.

[5] A. Conta, S. Deering, and M. Gupta. 2006. *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*. RFC 4443. IETF. https://doi.org/10.17487/RFC4443

[6] Daryll Swer. 2023. Behavioural differences of IPv6 subnet-router anycast address implementations. https://blog.apnic.net/2023/08/28/behavioural-differences-of-ipv6-subnet-router-anycast-address-implementations

[7] Zakir Durumeric, Eric Wustrow, and J. Alex Halderman. 2013. ZMap: Fast Internet-Wide Scanning and its Security Applications. In *Proc. of the 22nd USENIX Security Symposium*. USENIX Assoc., Berkeley, CA, USA, 605–620.

[8] Isabell Egloff, Raphael Hiesgen, Maynard Koch, Thomas C. Schmidt, and Matthias Wählisch. 2025. A Detailed Measurement View on IPv6 Scanners and Their Adaption to BGP Signals. *Proceedings of the ACM on Networking (PACMNET)* 3, CoNEXT3 (September 2025), 15:1–15:23. https://doi.org/10.1145/3749215

[9] Tobias Fiebig, Kevin Borgolte, Shuang Hao, Christopher Kruegel, and Giovanni Vigna. 2017. Something From Nothing (There): Collecting Global IPv6 Datasets From DNS. In *Proc. of PAM Conf.* Springer, Springer, Berlin Heidelberg, 30–43. https://doi.org/10.1007/978-3-319-54328-4_3

[10] Pawel Foremski, David Plonka, and Arthur Berger. 2016. Entropy/IP: Uncovering Structure in IPv6 Addresses. In *Proc. of the ACM IMC* (Santa Monica, California, USA) *(IMC '16)*. ACM, New York, NY, USA, 167–181. https://doi.org/10.1145/2987443.2987445

[11] Oliver Gasser. 2022. ZMapv6: Internet Scanner With IPv6 Capabilities. GitHub. https://github.com/tumi8/zmap

[12] Oliver Gasser, Quirin Scheitle, Pawel Foremski, Qasim Lone, Maciej Korczyński, Stephen D. Strowes, Luuk Hendriks, and Georg Carle. 2018. Clusters in the Expanse: Understanding and Unbiasing IPv6 Hitlists. In *Proc. of the ACM IMC*. ACM, New York, NY, USA, 364–378. https://doi.org/10.1145/3278532.3278564

[13] Oliver Gasser, Quirin Scheitle, Sebastian Gebhard, and Georg Carle. 2016. Scanning the IPv6 Internet: Towards a Comprehensive Hitlist. In *Proc. of TMA* (Louvain La Neuve, Belgium). IFIP, Laxenburg, MD, Austria, 1–8.

[14] Eric W Gaston. 2017. *High-Frequency Mapping Of The IPv6 Internet Using Yarrp*. Ph. D. Dissertation. Monterey, California: Naval Postgraduate School.

[15] Dallan Goldblatt, Calvin Vuong, and Michael Rabinovich. 2023. On Blowback Traffic on the Internet. *CoRR* (2023). https://doi.org/10.48550/ARXIV.2305.04434

[16] R. Hinden and S. Deering. 1995. *IP Version 6 Addressing Architecture*. RFC 1884. IETF. https://doi.org/10.17487/RFC1884

[17] R. Hinden and S. Deering. 2006. *IP Version 6 Addressing Architecture*. RFC 4291. IETF. https://doi.org/10.17487/RFC4291

[18] Florian Holzbauer, Markus Maier, and Johanna Ullrich. 2024. Destination Reachable: What ICMPv6 Error Messages Reveal About Their Sources. In *Proc. of ACM IMC* (Madrid, Spain). ACM, New York, NY, USA, 1–15. https://doi.org/10.1145/3646547.3688420

[19] Bingnan Hou, Zhiping Cai, Kui Wu, Tao Yang, and Tongqing Zhou. 2023. 6Scan: A High-Efficiency Dynamic Internet-Wide IPv6 Scanner With Regional Encoding. *IEEE/ACM Transactions on Networking* 31, 4 (2023), 1870–1885.

[20] IPinfo. 2025. ASN Database for IP and Network Analysis. https://ipinfo.io/products/asn-database

[21] Xiang Li, Baojun Liu, Xiaofeng Zheng, Haixin Duan, Qi Li, and Youjun Huang. 2021. Fast IPv6 Network Periphery Discovery And Security Implications. In *IEEE DSN 2021*. IEEE, IEEE, Washington, DC, USA, 88–100.

[22] Matthew Luckie, Robert Beverly, William Brinkmeyer, and kc claffy. 2013. Speedtrap: Internet-Scale IPv6 Alias Resolution. In *Proc. of ACM IMC*. ACM, New York, NY, USA, 119–126.

[23] Markus Maier and Johanna Ullrich. 2023. In The Loop: A Measurement Study Of Persistent Routing Loops On The IPv4/IPv6 Internet. *Computer Networks* 221 (2023), 109500. https://doi.org/10.1016/j.comnet.2022.109500

[24] MaxMind, Inc. 2025. MaxMind – GeoLite Country. https://dev.maxmind.com/geoip/geolite2-free-geolocation-data

[25] TU Munich. 2024. IPv6 Hitlist Service. https://ipv6hitlist.github.io

[26] Yevheniya Nosyk, Maciej Korczyński, and Andrzej Duda. 2022. Routing Loops As Mega Amplifiers For DNS-Based DDoS Attacks. In *Proc. of PAM Conf.* Springer, Springer, Berlin Heidelberg, 629–644. https://doi.org/10.1007/978-3-030-98785-5_28

[27] Long Pan, Jiahai Yang, Lin He, Zhiliang Wang, Leyao Nie, Guanglei Song, and Yaozhong Liu. 2022. Your Router Is My Prober: Measuring IPv6 Networks Via ICMP Rate Limiting Side Channels. In *Proc. of NDSS*. Internet Society, San Diego, CA, USA, 1–16. https://doi.org/10.14722/ndss.2023.23049

[28] Riccardo Ravaioli, Guillaume Urvoy-Keller, and Chadi Barakat. 2015. Characterizing ICMP Rate Limitation On Routers. In *Proc. of IEEE ICC*. IEEE, IEEE, Washington, DC, USA, 6043–6049. https://doi.org/10.1109/ICC.2015.7249285
[29] RIPE NCC. 2010. RIPE Atlas Built-In Measurements. https://atlas.ripe.net/docs/getting-started/built-in-measurements
[30] RIPE NCC. 2010. What is RIPE Atlas? https://atlas.ripe.net/about/
[31] Erik Rye and Dave Levin. 2023. IPv6 Hitlists at Scale: Be Careful What You Wish For. In *Proceedings of the ACM SIGCOMM 2023 Conference (ACM SIGCOMM '23)*. ACM, New York, NY, USA, 904–916. https://doi.org/10.1145/3603269.3604829
[32] Erik C Rye and Robert Beverly. 2020. Discovering The IPv6 Network Periphery. In *Proc. of PAM Conf.* Springer, Springer, Berlin Heidelberg, 3–18. https://doi.org/10.1007/978-3-030-44081-7_1
[33] Quirin Scheitle, Oliver Hohlfeld, Julien Gamba, Jonas Jelten, Torsten Zimmermann, Stephen D. Strowes, and Narseo Vallina-Rodriguez. 2018. A Long Way to the Top: Significance, Structure, and Stability of Internet Top Lists. In *Proc. of ACM IMC*. ACM, New York, NY, USA, 478–493. https://doi.org/10.1145/3278532.3278574
[34] Guanglei Song, Jiahai Yang, Lin He, Zhiliang Wang, Guo Li, Chenxin Duan, Yaozhong Liu, and Zhongxiang Sun. 2022. AddrMiner: A Comprehensive Global Active {IPv6} Address Discovery System. In *Proc. of USENIX ATC*. USENIX Association, San Diego, CA, USA, 309–326. https://doi.org/10.1109/TNET.2024.3406508
[35] Lion Steger, Liming Kuang, Johannes Zirngibl, Georg Carle, and Oliver Gasser. 2023. Target Acquired? Evaluating Target Generation Algorithms for IPv6. In *Proc. of TMA*. IEEE, Piscataway, NJ, USA, 1–10. https://doi.org/10.23919/TMA58422.2023.10199073
[36] Johanna Ullrich, Peter Kieseberg, Katharina Krombholz, and Edgar Weippl. 2015. On Reconnaissance with IPv6: A Pattern-Based Scanning Approach. In *10th International Conf on Availability, Reliability and Security*. IEEE, Piscataway, NJ, USA, 186–192. https://doi.org/10.1109/ARES.2015.48
[37] University of Oregon. 2017. Route Views Project. http://www.routeviews.org/.
[38] Grant Williams, Mert Erdemir, Amanda Hsu, Shraddha Bhat, Abhishek Bhaskar, Frank Li, and Paul Pearce. 2024. 6Sense: Internet-Wide IPv6 Scanning and its Security Applications. In *Proc. of the 33rd USENIX Security Symposium*. USENIX Association, San Diego, CA, USA.
[39] Tao Yang and Zhiping Cai. 2024. Efficient IPv6 Router Interface Discovery. In *IEEE INFOCOM 2024*. IEEE, Washington, DC, USA, 1641–1650. https://doi.org/10.1109/INFOCOM52122.2024.10621168
[40] Tao Yang, Zhiping Cai, Bingnan Hou, and Tongqing Zhou. 2022. 6Forest: An Ensemble Learning-Based Approach To Target Generation For Internet-Wide IPv6 Scanning. In *IEEE INFOCOM 2022*. IEEE, IEEE, Piscataway, NJ, USA, 1679–1688. https://doi.org/10.1109/INFOCOM48880.2022.9796925
[41] Johannes Zirngibl, Lion Steger, Patrick Sattler, Oliver Gasser, and Georg Carle. 2022. Rusty clusters? Dusting an IPv6 research foundation. In *Proc. of the ACM IMC*. ACM, New York, NY, USA, 395–409. https://doi.org/10.1145/3517745.3561440

A Ethics

In this work, we found critical router configurations and a software bug of major router vendors, both are deployed on the IPv6 Internet. We implemented a responsible disclosure policy by contacting all affected networks and router vendors. First networks started to correct their configuration and router vendors started to fix their software. Intentionally, we did not reveal networks and vendors in this paper.

We discovered these threats by active scanning, *i.e.,* sending standard ICMPv6 Echo requests with different hop limits. This method is a common Internet measurement method and does not introduce ethical concerns. As soon as we noticed the implications of our scans on some networks, we excluded the affected IP prefixes from subsequent scans. In addition, we excluded networks for which operators asked us to stop scanning—we received and processed a total of two opt-out requests.

B Artifacts

All artifacts of this paper are publicly available. These include (*i*) all raw measurement data that we used to analyze SRA probing; (*ii*) all routing loop and amplification data after a clearance process; (*ii*) all data derived from post-processing, *i.e.,* data that substantiate our arguments and serve as input for our figures; (*iii*) measurement scripts; (*iv*) post-processing scripts. All artifacts and details on how to use them are archived on https://doi.org/10.5281/zenodo.17210254.

Regular updates of our data are available on https://ipv6-sra.realmv6.org.

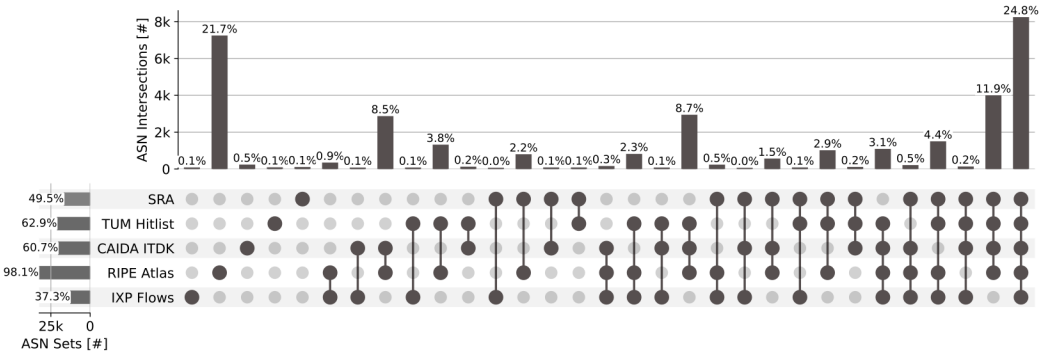


Fig. 9. Overlap between all collected data sources on AS level.

C Resolving Common Routing Loops

Internet routing loops often exist because a customer announces a covering prefix to its upstream provider but only maintains some routes to more specific prefixes of the overall announced address space. In addition, this customer configures a default route via its upstream. This makes parts of the address space that belong to the customer but are unused and locally unreachable accessible to the customer via the upstream. To prevent routing loops (*e.g.,* triggered by downstream peers of the customer), the customer router needs to drop packets destined to the unused address space. In many router implementations, this is achieved by using *null routes*. We now present necessary configurations to prevent routing loops on routers from Cisco and Juniper, two common router vendors.

For example, a customer that has been assigned the prefix 2001:db8::/32 but only uses the parts 2001:db8::/34 and 2001:db8:8000::/34 can exclude all traffic to 2001:db8:4000::/34 and 2001:db8:c000::/34 from further forwarding as follows.

Cisco IOS.

```
ipv6 route 2001:db8::/32 Null0
```

Juniper Junos OS.

```
set aggregate route 2001:db8::/32
```

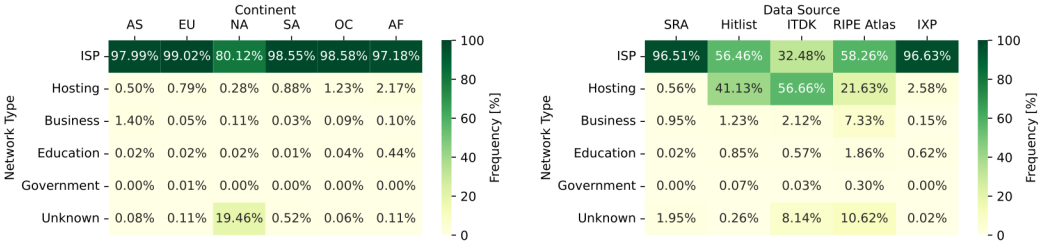
Note that these configurations are examples. The exact configuration syntax depends on the firmware deployed.

D Overlap on AS Level

Figure 9 shows the complete version of the UpSet plot presented in Figure 7, *i.e.,* all combinations of intersections between the datasets we analyzed. Additional combinations of intersections, however, do not change the overall picture of overlapping (and non-overlapping) ASNs that we discussed in Section 5.

E Distribution of IP Addresses Across Network Types

Figure 10 presents the distribution of discovered IP addresses per network type, further grouped geographically for our SRA dataset and in comparison with other data sources. Across all continents, the majority of router IP addresses we discovered using SRA probing belong to ISP networks (>80%). Comparing SRA probing with other datasets, passive IXP flow data shows similar results, mainly



(a) Router IP addresses per continent discovered using SRA probing .

(b) IP addresses per network type, comparing our SRA and other datasets.

Fig. 10. Distribution of IP addresses per network type. Columns are sorted in decreasing order by absolute values.

including IP addresses belonging to ISP networks (96%). All other sources contain, in addition to ISP networks, a significant fraction of IP addresses linked to hosting networks.

F Distribution of Routing Loops and Amplification

Table 4 shows the top 5 countries (Brazil, China, Czech Republic, Germany, Netherlands, and USA) that host the most /48 subnets affected by routing loops and amplification. In total, we observe routing loops in more than 5k autonomous systems, distributed across 155 countries. 54% relate to infrastructure located in only five countries, with Brazil alone accounting for 26%. Interestingly, the routing loops in Brazil are distributed over 9k router IP addresses, whereas the routing loops in Germany, Czech Republic, and the Netherlands are distributed between 388 and 1.2k router IP addresses (see Table 4(a)). In terms of maximum amplification factors, China is more relevant than the Netherlands (see Table 4(b)).

Table 4. Top 5 countries hosting infrastructure that triggers routing loops and amplification.

(a) Top 5 countries ranked by the number of /48 subnets that trigger a routing loop.

	Looping /48 subnets		Router
Country	[#]	[%]	IPs [#]
BRA	37,081,970	26.22	9329
DEU	13,273,666	9.39	1192
CZE	10,444,197	7.39	881
USA	7,613,551	5.38	4150
NLD	7,241,713	5.12	388

(b) Top 5 countries ranked by the number of /48 subnets that trigger amplification.

	Ampl. /48 subnets		Router	
Country	[#]	[%]	IPs [#]	Max. Ampl. [×]
BRA	4,674,687	23.35	2765	51
DEU	477,046	2.38	78	258,399
USA	247,736	1.24	577	109,385
CHN	245,546	1.23	4141	52
CZE	212,547	1.06	17	37

Received June 2025; accepted September 2025