

traIXroute: Detecting IXPs in traceroute paths

George Nomikos and Xenofontas Dimitropoulos

Foundation of Research and Technology Hellas (FORTH), Greece
{gnomikos, fontas}@ics.forth.gr

Abstract. Internet eXchange Points (IXP) are critical components of the Internet infrastructure that affect its performance, evolution, security and economics. In this work, we introduce techniques to augment the well-known `traceroute` tool with the capability of identifying if and where exactly IXPs are crossed in end-to-end paths. Knowing this information can help end-users have more transparency over how their traffic flows in the Internet. Our tool, called `traIXroute`, exploits data from the PeeringDB (PDB) and the Packet Clearing House (PCH) about IXP IP addresses of BGP routers, IXP members, and IXP prefixes. We show that the used data are both rich, i.e., we find 12,716 IP addresses of BGP routers in 460 IXPs, and mostly accurate, i.e., our validation shows 92-93% accuracy. In addition, 78.2% of the detected IXPs in our data are based on multiple diverse evidence and therefore help have higher confidence on the detected IXPs than when relying solely on IXP prefixes. To demonstrate the utility of our tool, we use it to show that one out of five paths in our data cross an IXP and that paths do not normally cross more than a single IXP, as it is expected based on the valley-free model about Internet policies. Furthermore, although the top IXPs both in terms of paths and members are located in Europe, US IXPs attract many more paths than their number of members indicates.

1 Introduction

A few hundred IXPs worldwide host more than one hundred thousand interconnections between Autonomous Systems (ASes) [10], [14], [20]. As critical components of the Internet infrastructure, IXPs influence its expansion [16], performance [11], and security [7]. However, their centralized nature is also a limitation that can be exploited for mass surveillance of Internet users or for targeted attacks. Although IXPs exist since the early days of the Internet, they have recently attracted intense interest from the academic community in part because the last decade the Internet topology is flattening [16], [18], [21], [23], which implies an even more central role for IXPs.

In this work we extend the well-known and widely-used `traceroute` tool with the capability of inferring if and where an IXP was crossed. This is useful not only for end-users in having more transparency over where their traffic goes, but also for operators in troubleshooting end-to-end paths and for researchers in understanding the evolving IXP ecosystem. Our tool, called `traIXroute`, detects IXPs based on data from the PeeringDB (PDB) and the Packet Clearing House (PCH). In particular, it uses the (i) exact IP addresses of BGP routers connected to IXP subnets; (ii) IXP member ASes; (iii) IXP prefixes; and (iv) IP addresses to AS mappings; and combines multiple information to detect IXPs with higher confidence than simply relying on IXP prefixes.

Our second contribution is that we evaluate the coverage and accuracy of the IXP router IP addresses, which we denote with a triplet $\{IP\ address \rightarrow IXP, AS\}$, in PDB and PCH. We find in total 12,716 triplets for 460 IXPs worldwide. Using the exact router IXP addresses along with checking the IXP membership of the two adjacent ASes, we classify 78.2% of the IXP paths. Therefore, in most cases we can detect an IXP with strong evidence. In addition, we find that 92-93% of the triplets $\{IP\ address \rightarrow IXP, AS\}$ extracted from PDB and PCH are consistent with the corresponding information extracted from live BGP sessions of route collectors at IXPs.

Third, to illustrate how `traIXroute` can be useful, in particular for researchers in Internet measurement studies, we use it to answer the following questions: (i) how often paths cross IXPs? (ii) which IXPs attract most paths? and (iii) how many IXPs are encountered per path? We apply `traIXroute` on 31.8 million traceroute probes collected from the ark measurement infrastructure [1]. We find that approximately one out of five paths crossed an IXP and that IXP-paths normally cross no more than a single IXP. The IXP hop is located on average near the 6th hop at the middle of the route. Finally, we show that the top IXPs in terms of paths differ in part from the top IXPs in terms of AS members.

The rest of this paper is structured as follows. In the next section, we discuss the related work and provide background into the problem of detecting IXPs in traceroute paths. Next, in Section 3 we describe `traIXroute` and its IXP detection techniques. In Section 4, we evaluate the coverage and accuracy of the data used by `traIXroute` and discuss the hit rate of its detection rules. Finally, in Section 5 we outline our IXP measurement study using `traIXroute` and in Section 6 we conclude.

2 Related Work and Background

Previous studies have examined the problem of mapping traceroute paths to AS-level paths [15], [25]. Mapping IP addresses to ASes is not straightforward because routers can reply with source IP addresses numbered from a third-party AS. These studies ignore hops with IXP IP addresses. These addresses are used to number BGP router interfaces connected to the IXP subnet and it is hard to identify to which AS they belong.

Besides, a group of previous studies, starting with Xu *et al.* [27] and then followed by He *et al.* [22] and Augustin *et al.* [13], focus on inferring participating ASes and peerings at IXPs from *targeted* traceroute measurements. Compared to these studies, our goal is different: we build a general-purpose traceroute tool, while they aim at discovering as many peering links as possible. The basic methodology developed in [27] and then significantly extended in [22] and [13] detects IXPs based on assigned IP address prefixes and uses various heuristics to infer peering ASes. The seminal work of Augustin *et al.* [13] exploited also data for BGP routers at IXP, but by querying 1.1K BGP Looking Glass servers, which had significant processing cost. In contrast, we extract corresponding data from PDB and PCH, with low processing cost, and show that they are both rich and mostly accurate.

Recently, Giotsas *et al.* [19] introduced techniques to identify the physical facility where ASes interconnect using targeted traceroute measurements and a combination of publicly available facility and IXP based information.

Our starting point in this work is that **observing an IP address from an IXP prefix is not sufficient evidence to conclude that the IXP was crossed**. This happens for multiple reasons: (i) the available IXP IP address prefix data may be inaccurate; (ii) IXPs could use allocated addresses not only in the IXP subnet but also in other operational subnets; and (iii) third-party IP addresses from IXP subnets. To illustrate the latter consider the following example (cf. Figure 1). A router connected to the IXP fabric could reply to traceroute probes using a source IP address from any of its interfaces, including the interface on the IXP subnet. Traceroute paths that do not cross the IXP, like the dotted one in Figure 1, can include a reply with a source IP address from the IXP subnet. Therefore, the path appears to have an IP address from an IXP subnet, even if the IXP is not crossed. Our goal is to detect paths that cross the IXP fabric, like the dashed one in Figure 1.

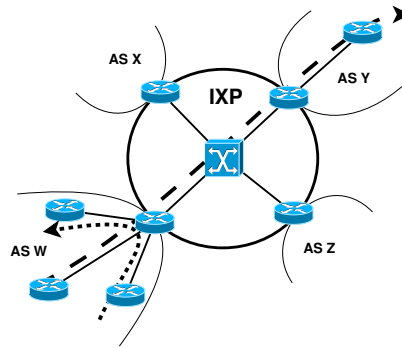


Fig. 1: Example IXP connected to four ASes. The dotted traceroute path could include a reply with an IXP IP address, even if the IXP is not crossed. Our goal is to identify paths that cross the IXP, like the dashed one.

To be more confident that an IXP is crossed, we exploit specific information about the IP addresses of BGP router interfaces connected to the IXP subnet. This data enable us also to associate IP addresses to ASes and IXPs. Furthermore, we check if the ASes before and after the IXP IP address are members of the candidate IXP based on the IXP membership data from PCH and PDB, which have not been explored in the previous studies for this purpose.

3 TRAIXROUTE Design and Heuristics

In this section, we first outline the design of `traIXroute` and then its IXP detection heuristics.

3.1 TRAIXROUTE Design

`traIXroute` is written in python and operates like `traceroute`. It can be configured to use either the standard `traceroute` tool in the background or the `scamper` tool

```

$ traIXroute de-cix.net
traIXroute to de-cix.net (80.81.196.█), 30 hops max, 60 byte packets
 1 AS8522      139.91.68.253 (139.91.68.█) 0.564 ms 0.544 ms 0.579 ms
 2 AS8522      139.91.34.85 (139.91.34.█) 0.478 ms 0.545 ms 0.627 ms
 3 AS5408      forth-her-4-gw.eier.access-link.grnet.gr (62.217.98.█) 7.028 ms 7.037 ms 7.027 ms
 4 AS20965     grnet.mx2.ath.gr.geant.net (62.40.124.█) 7.061 ms 7.061 ms 7.049 ms
 5 AS20965     ae8.mx1.vie.at.geant.net (62.40.112.█) 37.316 ms 37.324 ms 37.312 ms
 6 Vienna IX->AS6939  10gigabitethernet1-3.core1.vie1.he.net (193.203.0.█) 43.740 ms 41.824 ms 41.898 ms
 7 AS6939      10ge1-4.core1.prg1.he.net (184.105.222.█) 50.897 ms 49.737 ms 49.754 ms
 8 AS6939      100ge8-1.core1.fra1.he.net (184.105.213.█) 79.408 ms 75.336 ms 75.328 ms
 9 AS6939      sgw2-te-0-0-2-0-v1210.fra.de-cix.net (216.66.80.█) 50.939 ms 51.273 ms 50.928 ms
10 AS51531     fw-ext-v190.fra.de-cix.net (46.31.120.█) 50.443 ms 50.322 ms 50.312 ms
11 AS51531     web1.de-cix.net (80.81.196.█) 50.767 ms 50.462 ms 50.479 ms
IXP hop detected:
1) 62.40.112.█->193.203.0.█, hop 5->6

```

Fig. 2: Example output of traIXroute.

[24], which implements the Paris traceroute technique [12]. It has a modular design and can be easily extended with new IXP data and detection rules. An example of the output of traIXroute is shown in Figure 2. In this example the Vienna IX is detected between hops 5 and 6. The tool also prints the AS that corresponds to each hop based on simple origin AS lookups. traIXroute exploits three datasets to identify IXPs in traceroute paths which can be updated automatically from the command line:

1. **IXP Memberships Dataset:** We use IXP membership data from the PEERINGDB (PDB) [4] and the PACKET CLEARING HOUSE (PCH) [3]. They provide: 1) exact IP addresses of router interfaces connected to the IXP network; and 2) the ASes which these routers belong to. Therefore, this dataset provides an association from IXP IP addresses to ASes and IXPs, i.e., a triplet of the form $\{IP\ address \rightarrow IXP, AS\}$, which we mainly exploit in our heuristics.
2. **IXP IP Address Prefixes Dataset:** We use, in addition, two datasets of IPv4 address prefixes assigned to IXPs. The first is provided by PDB, while we extract the second from PCH. These addresses are typically used to number the interfaces of the BGP routers connected to the IXP subnet. We organize the dataset in the form $\{IP\ prefix \rightarrow IXP\}$ to map IP addresses to IXPs.
3. **Routeviews Prefix to AS mappings Dataset:** We use IP address prefix to AS mappings, i.e., $\{IP\ prefix \rightarrow AS\}$, provided by CAIDA [5] based on data from RouteViews [9], to associate IP addresses to ASes. Also, we filter the IANA reserved IP addresses, which should not be announced to BGP, to protect from route leaks and other misconfigurations. When encountering multi-origin-as [28] IP addresses, we check the IXP membership of all the ASes.

PCH and PDB do not use consistent identifiers for IXPs and therefore if one naively matched the IXP identifiers would introduce artifacts. For this reason, we merge the two datasets by matching the IXP IP addresses, prefixes and names. We ignore matched records that include inconsistent attributes. In addition, we filter data for IXPs marked as inactive.

3.2 IXP detection

Next, we describe our methodology to detect and identify at which hop we cross an IXP in traceroute paths. When observing an IP address from an IXP subnet, we ask what information we know, based on our data, for this and the adjacent IP addresses. In particular, to infer an IXP crossing we follow three steps:

(Step 1) - Does the IP address match an exact BGP router IP address from an IXP subnet? In this case, we have a specific triplet $\{IP\ address \rightarrow IXP, AS\}$, which gives us also additional information about the AS of the router on the IXP. If an exact router IP address is not matched, then we check if an IXP prefix is matched, like in previous works [13] [22]. However, in this case we do not have any information about the AS that owns the router. If an IP address in the k -th hop of a traceroute path IP_k belongs to the interface of a router connected to the IXP subnet, then we denote this with $IP_k \xrightarrow{inf} IXP, AS_k$, where IXP is the IXP and AS_k the AS of the router. Otherwise, if we can associate IP_k only with an IXP IP prefix, then we denote this with $IP_k \xrightarrow{prf} IXP$.

(Step 2) - Are the adjacent ASes members of the IXP? We map the IP addresses 1-hop adjacent to the observed IXP IP address to ASes and, considering also the AS of the IXP IP address (if this information is available), we check the IXP membership of the ASes. We distinguish four possible cases: (i) both ASes are members, (ii) - (iii) only the AS in the left or right of the IXP IP address is a member; and (iv) none of the ASes is an IXP member. Our assessment is based on the available data about the ASes from triplets and from mapping IP addresses to ASes using the Routeviews Prefix to AS mappings Dataset. Such mappings could be wrong [25], therefore we do not consider this evidence alone conclusive. In addition, if AS_k is a member of the IXP based on IXP membership data then we denote this with $AS_k \in IXP$.

(Step 3) - Is the IXP link crossed before or after the IXP IP address? We check this when sufficient information about the ASes is available.

Our heuristics are applied on a traceroute path in a sliding window fashion, where the length of the window is three. By carefully reasoning about all possible combinations of evidence from Steps 1 and 2 that exist for three subsequent hops, we formulated 16 cases. Each case corresponds to a detection rule. For brevity, we next discuss only the cases (8 in total) that appeared with frequency higher than 1% in the matched IXP paths. The remaining cases are still supported in `traIXroute`. In Table 1 we show our detection rules for the most typical scenario, when we observe a single IXP IP address between two non-IXP IP addresses. We also consider the special case, shown in Table 2, when we observe two adjacent IP addresses from an IXP subnet. In most cases, we can deduce the exact link where the IXP was crossed, which we denote in Tables 1 and 2 as a or b . We split the rules into *strong* and *weak* evidence rules and order them based on their frequency, as shown in the last column of the tables (cf. Section 4).

Rules 1.1 to 1.3 match the IP addresses of routers on the IXP subnet, extract information about the adjacent ASes, and find that both ASes are members of the IXP. In the Rules 1.1 and 1.2 the IXP is crossed in the first hop. The Rule 1.2 is otherwise the same with the Rule 1.1, but without information for AS_{k+2} . Finally, the Rule 1.3 is also identical otherwise, but with $AS_{k+2} \neq AS_{k+1}$. These three rules check multiple criteria and exploit data about triplets, which give also an association from IP addresses

One IXP IP Address between two non-IXP IP addresses					
Rules	Hop Window			Assessment	Hit Rate
1.1	$AS_k \in IXP$	$IP_{k+1} \xrightarrow{inf} IXP, AS_{k+1}$ $AS_{k+1} = AS_{k+2} \neq AS_k$	$AS_{k+2} \in IXP$	$a \rightarrow IXP$	65.57%
1.2	$AS_k \in IXP$	$IP_{k+1} \xrightarrow{inf} IXP, AS_{k+1}$ $AS_{k+1} \neq AS_k \neq AS_{k+2}$	$AS_{k+2} \notin IXP$	$a \rightarrow IXP$	8.79%
1.3	$AS_k \in IXP$	$IP_{k+1} \xrightarrow{inf} IXP, AS_{k+1}$ $AS_{k+1} \neq AS_k \neq AS_{k+2}$	$AS_{k+2} \in IXP$	a or $b \rightarrow IXP$	2.5%
1.4	$AS_k \in IXP$	$IP_{k+1} \xrightarrow{prf} IXP$	$AS_{k+2} \notin IXP$	$a \rightarrow IXP$	7.7%
1.5	$AS_k \notin IXP$	$IP_{k+1} \xrightarrow{prf} IXP$	$AS_{k+2} \in IXP$	$b \rightarrow IXP$	5.55%
1.6	$AS_k \notin IXP$	$IP_{k+1} \xrightarrow{inf} IXP, AS_{k+1}$ $AS_{k+1} = AS_{k+2} \neq AS_k$	$AS_{k+2} \in IXP$	$b \rightarrow IXP$	4.56%
1.7	$AS_k \notin IXP$	$IP_{k+1} \xrightarrow{inf} IXP, AS_{k+1}$ $AS_k \neq AS_{k+1} \neq AS_{k+2}$	$AS_{k+2} \notin IXP$	a or $b \rightarrow IXP$	1.21%

Table 1: IXP detection rules for a single IXP IP address, based either on IXP interface (inf) or prefix-level (prf) data, between two non-IXP addresses. The rows give the data attributes per hop to check in order to detect an IXP. Rules 1.1 to 1.3 use stronger evidence than Rules 1.4 to 1.7.

Two Consecutive IXP IP Addresses				
Rules	Hop Window		Assessment	Hit Rate
2.0	$IP_k \xrightarrow{inf} IXP, AS_k$	$IP_{k+1} \xrightarrow{inf} IXP, AS_{k+1}$ $AS_{k+1} \neq AS_k$	$a \rightarrow IXP$	1.36%

Table 2: IXP detection rule for two subsequent IXP IP addresses based on IXP interface (inf) data. The rows give the data attributes per hop which are checked to deduce an IXP.

to ASes with high accuracy (cf. Section 4.2). We therefore consider that these rules rely on stronger evidence than the Rules 1.4 to 1.7.

The Rules 1.4 and 1.5 do not match a triplet, but only an IXP prefix. In addition, we find that one of the two adjacent ASes is a member of the IXP. Based on this evidence, we consider that an IXP may have been crossed. However, we have much weaker evidence than when Rules 1.1-1.3 hold. `traIXroute` marks these cases as potential IXP crossing. Similarly, the Rules 1.6 and 1.7 match an IP address from a triplet, however only one or none of the adjacent ASes is a member of the IXP. We also have weaker evidence in these detections.

Finally, the Rule 2 in Table 2 finds two consecutive IP addresses that match triplets from the same IXP. The ASes in the triplets are also found members of the IXP. We consider this also as strong evidence for IXP detection, since multiple evidence indicate so. This is a particularly interesting case, as it indicates that the IXP fabric may have been crossed twice. In other words, we observe in few cases a type of "ping pong" routing over the IXP fabric.

Statistics	PDB	PCH
# of IXPs	509	466
# of IXP address prefixes	312	343
# of IXP membership triplets	12,323	3,580
# of IXPs with membership data	448 (88%)	343 (74%)
% of IXPs in top-50 with membership data	100%	62%
# of IXPs with IP prefix data	272 (53%)	299 (64%)
% of IXPs in top-50 with IP prefix data	92%	96%

Table 3: Various statistics about the PDB and PCH IXP datasets.

4 Evaluation

In this section, we evaluate and validate our methodology. We downloaded the IXP Memberships Dataset and the IXP IP Address Prefixes Dataset from PDB and PCH on January, the 10th 2015. Our Routeviews Prefix to AS mappings Dataset was downloaded from CAIDA on January, the 20th 2015.

4.1 Data Coverage and Hit Rates

PDB includes membership data for 448 (88%) out of the 509 IXPs in the database. Similarly, PCH provides membership data for 343 (74%) out of the 466 IXPs it includes. PDB and PCH provide membership data for 100% and 62%, accordingly, out of the top-50 IXPs (sorted by the number of their AS members). Besides, 312 of the IXPs in PDB and 343 of the IXPs in PCH provide IXP IP address prefixes. After merging, the combined dataset has 475 address prefixes for 417 IXPs and a total of 12,716 IXP membership triplets $\{IP\ address \rightarrow IXP, AS\}$ for 460 IXPs, i.e., an increase of 38.5% and 3.2%, correspondingly, with respect to the largest individual dataset. These statistics along with other details are summarized in Table 3. For comparison, the April 2009 experiment reported by Augustin *et al.* [13] found triplets for 119 IXPs by querying 1.1K BGP Looking Glass servers.

We then discuss the hit rate of the rules in Tables 1 and 2 in our `traIXroute` probes to shed more light onto the methodology. The strong evidence Rules 1.1 to 1.3 collectively account for 76.86% of the detected IXPs, which shows that in most cases we can detect IXPs, while satisfying multiple criteria: (i) we observe an exact IP address of a BGP router on the IXP subnet; and (ii) we find that both ASes are members of the candidate IXP. Rule 1.1 is by far the most frequent as it matches 65.57% of the detected IXPs. This indicates that the available datasets from PDB and PCH about exact IXP router addresses are rich enough to match most IXP addresses observed in traceroute measurements.

Rules 1.4 to 1.7 collectively account for 19.02% of the matches. These rules rely on weaker evidence. The Rules 1.4 and 1.5, in particular, which rely on IXP prefixes match 13.25% of the cases. We observe that IXP prefixes add a moderate amount of weak evidence matches compared to the IXP membership data.

Rule 2 hits in 1.36% of the detected IXPs. This illustrates that in a few cases, the IXP fabric maybe crossed twice. This points to inefficient routing due to the BGP path

Statistics	PDB	PCH
# of <i>(IXP-AS)</i> tuples in intersection with BGP	4,655	3,073
% of tuples <i>(IXP-AS)</i> with consistent IP addresses	93.4%	92.1%

Table 4: Consistency of IXP router IP addresses in PDB and PCH with data from 87 BGP Route Collectors located at IXPs

selection process that relies on AS-level paths and ignores layer-2 topologies. In this case, the layer-2 IXP fabric is likely crossed back and forth, consuming resources.

Besides, we explored a number of other rules, which we do not show in Tables 1 and 2 because they matched in less than 1% of the cases. From these rules, we confirmed (as expected) that the IXP link is almost always before the observed IXP address. This is because routers typically reply with the IP address of the inbound interface. In just 0.71% of the cases we observed the IP address, which matched an IXP triplet, to belong to the same AS with the preceding IP address. Another interesting observation is that when an IP address matches an IXP prefix, but not an IXP triplet, then in only 2.98% of the matches both of the adjacent ASes are members of the IXP. In contrast, the corresponding number for matched IXP triplets is 81.79%. This supports further the point that triplets help to detect IXPs more reliably than IXP prefixes.

4.2 Data Accuracy and Validation

The data in PDB are primarily self-reported by IXP and ISP operators, while the data in PCH are based primarily on live BGP Route Collectors that PCH operates in multiple IXP sites, where it is an IXP member and peers with other ASes. The PDB data are often used by network operators for checking and configuring their routers. A recent study [26] showed that 99% of the valid (i.e., that conform to the correct format) IP addresses reported in PDB matched the IP addresses used by BGP routers, based on a sample submitted by network operators for 256 routers. We validate further the accuracy of the used PDB and PCH IXP membership data based on BGP feeds from the Route Collectors of PCH.

We parse BGP routing table dumps downloaded on January, the 31st 2015 from 87 Route Collectors operated by PCH. Route Collectors on IXPs peer with members of the IXP to provide a live view of their routing announcements. They are therefore an excellent reference for validation because their attributes, e.g. IP addresses and AS numbers, are used in live BGP sessions. For each routing table entry, we extract the next hop IP address and the first AS in the AS path. We then compare the extracted data with the corresponding information from PDB and PCH. We find that 93.4% of the 4,655 *{IXP-AS}* tuples, which are common between PDB and BGP, have consistent IP addresses. Accordingly, 92.1% of the 3,073 *{IXP-AS}* tuples, which are common between PCH and BGP, have consistent IP addresses. This data is summarized in Table 4. This high degree of consistency shows that triplets $\{IP\ address \rightarrow IXP, AS\}$ from PDB and PCH are a valid source of information for detecting IXPs in traceroute paths. The inconsistent part could result from stale or incomplete information in PDB and PCH. Triplets with stale IP addresses will not help, but will not also introduce problems in detecting IXPs with our methodology. Finally, we note that although the triplets we

exploit have a reasonable level of accuracy, their completeness is hard to assess. This is a limitation for our work. However, our analysis is encouraging because we find 12,716 triplets for 460 IXPs after merging the PDB and PCH data.

Finally, as an extra validation step we cross-checked the Routeviews Prefix to AS mappings Dataset from CAIDA with the IP to ASN mapping service of Team Cymru [6] and found that the two mappings were fully consistent.

5 Use Case: IXPs in Traceroute Paths

Having evaluated and validated our approach, we next do a preliminary analysis of what we can learn about IXPs using an IXP-informed traceroute tool. We use traceroute paths collected from CAIDA’s Ark measurement infrastructure [8], which at the time of our experiments had 107 monitors distributed around the globe (split into three teams of similar size). The monitors rely on the scamper tool [24] configured with the Paris traceroute technique [12] to mitigate artifacts due to load balancing. We use one full cycle of measurements collected on January, the 20th 2015, which includes an ICMP-paris probe to each globally routed /24 block. Each probe is assigned to a team. We process the output of scamper with `traIXroute` to detect IXPs. We repeat our experiments with data from the three teams to check for the consistency of our results across different vantage points. In addition, we process the collected paths to remove probes without any reply or with loops. The number of probes after pre-processing dropped from 31.8 million to 27.8 million probes.

In Table 5 we first report the fraction of traceroute paths which go through an IXP. The monitors are located in a mix of academic and corporate institutions [2]. We first observe that the fraction of paths that cross an IXP is 17.44%, 17.65% and 23.64% in the three teams. We observe a slightly larger fraction in the 3rd team, because one of the monitors in this team is located in an IXP (AMS-IX). Despite this, our results are mostly consistent across the three teams: Approximately one out of five paths in our datasets go through an IXP. Furthermore, in paths that go through an IXP we observe 1 to 1.05 IXPs per path. This is interesting because it confirms the expectation based on the valley-free model [17] that up to one peering link, and therefore one IXP¹, is crossed in an end-to-end path. Even if BGP allows much more complex policies and the Internet IXP ecosystem evolves continuously, Internet paths in our measurements largely conform to the well-known valley-free model. Furthermore, we observe that paths cross on average between 14.06 to 14.77 hops, and the IXP hop is located near the middle, i.e., on average between hop 5.4 and 6.68 for the different teams. For completeness, we also compute the number of ASes the paths cross, which ranges between 4.17 and 4.48 ASes.

Top IXPs in terms of paths. We next analyze which IXPs attract most paths and how the number of paths an IXP attracts compares with the number of their member ASes. In Table 6 we show the top-10 IXPs in terms of paths, the min and max numbers of paths over the three teams, and number of their members. We first observe that the top-3 IXPs, namely AMS-IX, LINX, and DE-CIX, are the same both in terms of paths and members. These IXPs are located in Europe; 5 of the following IXPs are located in the

¹ IXPs links are typically used for settlement-free peering relationships.

Statistics	Team 1	Team 2	Team 3
%Paths with IXPs	17.65%	17.44%	23.64%
Avg. # of IXPs per IXP path	1.02	1	1.05
Avg. # of hops per path	14.77	14.37	14.06
Avg. IXP hop	6.68	6.35	5.40
Avg. # of ASes per path	4.48	4.17	4.33

Table 5: Statistics about IXPs in 27.85 million probed traceroute paths. The results are grouped into teams to show the consistency of the computed statistics across vantage points.

IXP Name	Min-max # of paths over teams	# of member ASes
1. AMS-IX	277K - 570K	630
2. LINX	182K - 234K	526
3. DE-CIX Frankfurt	133K - 215K	520
4. Equinix Palo Alto	119K - 134K	116
5. Equinix Chicago	73K - 80K	145
6. Equinix Ashburn	43K - 91K	217
7. NAP of The Americas	45K - 90K	112
8. Equinix Los Angeles	37K - 60K	76
9. CoreSite - California	30K - 58K	195
10. Netnod Stockholm	33K - 44K	104

Table 6: Top IXPs sorted by the number of paths that cross them. For each IXP, we show the minimum and maximum number of paths that cross it over the three probing teams; and the number of AS members.

US and 4 of these are run by Equinix, i.e., the largest IXP corporation in the US. Finally, one IXP in South America and one more European close the top-10. We note that in Table 6 the 570K paths that cross the AMS-IX, is an outlier due to a single ark monitor located in AMS-IX. Despite this, the ranking does not change if we only consider the other teams of monitors.

Besides, below the top-3 IXPs we observe significant variance between the number of IXP members and the number of IXP paths. Figure 3 illustrates how the number of IXP members correlates with the number of paths. The overall correlation coefficient is 0.8. We observe that the top-3 IXPs are close to the 95-percentile confidence intervals, which means that compared to the average they have more members than paths. In contrast, many US IXPs have more paths than their number of members indicates. Notably, Equinix Palo Alto is in the 4th position with a small difference in terms of paths from DE-CIX, although the latter has 520 members and the former only 116.

6 Conclusions

Internet users, network operators, and researchers would benefit if they were able to know from which IXPs packets go through. To help towards this goal, in this paper we introduce a tool that extends the commonly used `traceroute` with techniques to detect IXPs. Our techniques rely on data about the exact IP addresses of BGP router interfaces connected to the IXP subnet, i.e., triplets $\{IP\ address \rightarrow IXP, AS\}$, extracted from the PEERINGDB and the PACKET CLEARING HOUSE. This data has not been previously explored for identifying IXPs. We show that they are both rich, i.e., we find 12,716

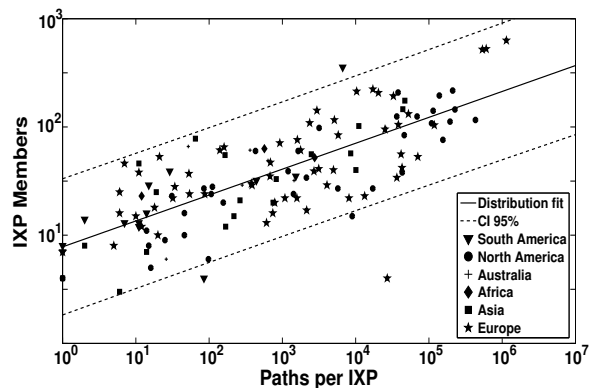


Fig. 3: Scatterplot of number of AS members vs. number of paths per IXP along with fitted line and 95% confidence intervals (CI). IXPs are grouped by continent. The correlation is 0.8.

triplets for 460 IXPs, and accurate, i.e., our validation shows 92-93% accuracy. We also incorporate in our heuristics an IXP membership check for the adjacent ASes to have stronger evidence that an IXP was crossed. To demonstrate the utility of `traIXroute`, we use it to show that approximately one out of five paths cross an IXP in our data. In addition, in most cases, we observe not more than one IXP per path, which is located near the middle. Furthermore, we observe that although the top IXPs both in terms of paths and members are located in Europe, US IXPs attract many more paths than their number of members indicates. In the future, we plan to investigate how `traIXroute` could help Internet users to have more control over their paths.

Acknowledgements

This work has been funded by the European Research Council Grant Agreement no. 338402. We would like to thank Pavlos Sermpezis, Laurent Vanbever, Michalis Bamiedakis and the anonymous reviewers for their helpful comments.

References

1. Archipelago Measurement Infrastructure. <http://www.caida.org/projects/ark/>
2. CAIDA Monitors: The Archipelago Measurement Infrastructure. <http://www.caida.org/data/monitors/monitor-map-ark.xml>
3. Packet Clearing House - Internet Exchange Directory. <https://prefix.pch.net>
4. PeeringDB. <http://www.peeringdb.com>
5. Routeviews Prefix to AS mappings Dataset (pfx2as) for IPv4. <http://www.caida.org/data/routing/routeviews-prefix2as.xml>
6. Team Cymru, IP to ASN mapping. <http://www.team-cymru.org/IP-ASN-mapping.html>
7. The DDoS That Almost Broke The Internet. <http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet>

8. The IPv4 Routed /24 Topology Dataset. http://www.caida.org/data/active/ipv4_routed_24_topology_dataset.xml
9. The Route Views Project. www.routeviews.org
10. Ager, B., Chatzis, N., Feldmann, A., Sarrar, N., Uhlig, S., Willinger, W.: Anatomy of a large european ixp. In: Proc. ACM SIGCOMM (2012)
11. Ahmad, M.Z., Guha, R.: Studying the effect of internet exchange points on internet link delays. In: Proc. Spring Simulation Multiconference (2010)
12. Augustin, B., Friedman, T., Teixeira, R.: Multipath tracing with paris traceroute. In: Proc. IEEE End-to-End Monitoring Techniques and Services Workshop (2007)
13. Augustin, B., Krishnamurthy, B., Willinger, W.: Ixps: mapped? In: Proc. ACM IMC (2009)
14. Chatzis, N., Smaragdakis, G., Feldmann, A., Willinger, W.: There is more to ixps than meets the eye. Proc. SIGCOMM CCR (2013)
15. Chen, K., Choffnes, D.R., Potharaju, R., Chen, Y., Bustamante, F.E., Pei, D., Zhao, Y.: Where the sidewalk ends: Extending the internet as graph using traceroutes from p2p users. In: Proc. ACM SIGCOMM CoNEXT (2009)
16. Dhamdhere, A., Dovrolis, C.: The internet is flat: modeling the transition from a transit hierarchy to a peering mesh. In: Proc. ACM ICPS (2010)
17. Gao, L., Rexford, J.: Stable Internet Routing Without Global Coordination. In: Proc. ACM SIGMETRICS (2000)
18. Gill, P., Arlitt, M., Li, Z., Mahanti, A.: The flattening internet topology: Natural evolution, unsightly barnacles or contrived collapse? In: Proc. PAM. Springer (2008)
19. Giotsas, V., Smaragdakis, G., Huffaker, B., Luckie, M., claffy, k.: Mapping peering interconnections to a facility. In: Proc. ACM SIGCOMM CoNEXT (2015)
20. Giotsas, V., Zhou, S., Luckie, M., claffy, k.: Inferring multilateral peering. In: Proc. ACM SIGCOMM CoNEXT (2013)
21. Gregori, E., Improta, A., Lenzini, L., Orsini, C.: The impact of ixps on the as-level topology structure of the internet. Computer Communications (2011)
22. He, Y., Siganos, G., Faloutsos, M., Krishnamurthy, S.: Lord of the links: A framework for discovering missing links in the internet topology. IEEE/ACM ToN (2009)
23. Labovitz, C., Iekel-Johnson, S., McPherson, D., Oberheide, J., Jahanian, F.: Internet inter-domain traffic. ACM SIGCOMM CCR (2011)
24. Luckie, M.: Scamper: a scalable and extensible packet prober for active measurement of the internet. In: Proc. ACM IMC (2010)
25. Mao, Z.M., Rexford, J., Wang, J., Katz, R.H.: Towards an accurate as-level traceroute tool. In: Proc. ACM SIGCOMM (2003)
26. Snijders, J.: PeeringDB Accuracy: Is blind faith reasonable? NANOG 58 (2013)
27. Xu, K., Duan, Z., Zhang, Z.L., Chandrashekar, J.: On properties of internet exchange points and their impact on as topology and relationship. In: Networking. Springer (2004)
28. Zhao, X., Pei, D., Wang, L., Massey, D., Mankin, A., Wu, S.F., Zhang, L.: An analysis of bgp multiple origin as (moas) conflicts. In: Proc. ACM SIGCOMM Internet Measurement Workshop (2001)