Analyzing Remote Peering Deployment and Its Implications for Internet Routing

Fabricio Mazzola, Augusto Setti, Pedro Marcos, and Marinho Barcellos

***Abstract*— Internet eXchange Points (IXPs) have significantly transformed the structure and economics of the Internet by allowing many nearby networks to connect directly, avoiding the need for service providers. These large IXPs are so beneficial that they are not just used by nearby networks, but also by far away Autonomous Systems (AS). This is made possible by Remote Peering (RP), which typically involves the use of RP resellers to access remote IXPs. In this paper, we evaluate the effects of RP on four different routing aspects, using a representative group of IXPs located on three continents: (a) growth of RP deployment over one and a half years; (b) presence of route announcement mispractices (when networks prioritize the remote IXP over the local IXP), which are associated to routing anomalies; (c) reliability of RP interfaces and (d) adoption of RP-related BGP communities, i.e. to perform traffic engineering to remote peers. We make our data and results available to the community via a web portal.**

***Index Terms*— Computer networks, internet.**

I. Introduction

INTERNET eXchange Points (IXPs) increase connectivity by concentrating together a large number of networks. IXPs shorten Internet paths, improve performance, and reduce interconnection cost to its members [1], [2], [3], [4]. In recent years, *Remote Peering (RP)* has enhanced the importance and footprint of IXPs, by allowing ASes to reach a remote IXP, typically replacing the physical presence at the IXP facility with the services of a layer-2 provider. RP benefits include a quicker setup, no additional hardware, and lower installation costs when compared to local peering [5], [6], [7].

Despite being widely deployed at IXPs around the world, the community is still trying to understand the usage of RP, how/if it is still expanding, and the implications to Internet routing [8], [9], [10], [11], [12], [13], [14]. The precursory investigations about RP focused on methods to identify which networks remotely connect at different IXPs [7], [15]. Later studies have provided preliminary insights about the impacts of RP, such as introducing undesired latency to anycast [16], making it harder to detect peering infrastructure outages [17] and performing worse than local routes to reach specific prefixes on IXPs [18].

In this work, we perform a comprehensive measurement study of different routing impacts of RP in the wild, including its impacts on IXP growth, prefix announcement mispractices, IXP member's connectivity and operation time, and usage of BGP communities to perform traffic engineering (TE). For three months, we infer RP interfaces and announced prefixes on seven IXPs (identified in Table I), including five of the world's ten-largest IXPs by membership, to shed light on how RP evolves in different IXPs. Using these inferences, we investigated how prefix announcement mispractices for ASes connected on multiple IXPs via RP and local peering could introduce routing problems, inadvertently steering their traffic to the remote IXP. Next, we looked at the BGP session status of ASes in IXP route servers (RS) and evaluated the reliability and stability of remote connections. Lastly, we analyze the popularity and usage patterns of BGP communities explicitly created by three IXPs to perform TE on networks connecting via RP. Our contributions are as follows.

1) We investigate the evolution of RP deployment on IXPs with varying characteristics, such as the number of members and traffic exchanged (§III). To enable the study, we perform active latency measurements and collect BGP data from seven IXPs worldwide between August and October 2022. To widen our observation window, we compare our results with Mazzola et. al. [18]. Our results show that the number of remote interfaces has expanded faster than local ones since 2021. We also observed that newer, less established IXPs tend to lead the growth of RP use. We also noted that although the number of remote members grew over time, there was an unexpected decrease in the number of remote prefixes announced.
2) We select ASes connecting to IXPs via different connection methods (i.e., RP and local peering) to further investigate their prefix announcement practices (§IV). We identified more than 60 distinct ASes announcing their most specific prefixes (therefore preferential) on the remote IXP instead of prioritizing their local IXP connection, accounting for more than 37000 affected prefixes. These practices are highly likely to introduce *trombone paths*, impairing peering performance and connectivity.
3) We investigate the connection characteristics of remote and local IXP members on a subset of IXPs that enabled data collection for every IXP interface individually (§V).

Manuscript received 26 March 2023; revised 30 October 2023; accepted 11 February 2024; approved by IEEE/ACM Transactions on Networking Editor D. Malone. This work was supported in part by LACNIC through FRIDA Program and in part by LACNIC Applied Research Program. *(Corresponding author: Fabricio Mazzola.)*

Fabricio Mazzola is with the Institute of Informatics, Universidade Federal do Rio Grande do Sul, Porto Alegre 90040-060, Brazil (e-mail: fmmazzola@inf.ufrgs.br).

Augusto Setti and Pedro Marcos are with Center for Computational Science, Universidade Federal do Rio Grande, Rio Grande 96201-900, Brazil.

Marinho Barcellos is with the School of Computer and Mathematical Sciences, University of Waikato, Hamilton 3240, New Zealand.

Digital Object Identifier 10.1109/TNET.2024.3375898

Our fine-grained data collection of the ASes connected to the IXP RS (every 15 minutes over one and a half months) allows us to evaluate the connection stability and reliability between remote and local interfaces through different metrics, such as the uninterrupted time they stay with an active BGP session and the number of BGP session state changes. We found that RP connections to the IXP RS are consistently less stable than local ones for all IXPs and that BGP sessions in RP interfaces not only stay online less time in total but also change state more frequently.

4) We collect and analyze the usage of BGP communities specifically created to perform TE to remote peers on three IXPs (§VI). Our findings show that, despite created and made available for more than one year in the three IXPs, the usage of these communities is still negligible, with less than 1.11% of IXP members applying them to their routes. We also identify the ASes with the highest use of RP BGP communities and highlight their usage patterns.
5) We contribute a web portal with interactive analysis and plots to the community, making our results publicly accessible (§VII).

II. Measurement Architecture

In this section, we explain the measurement architecture used to infer remote interfaces and prefixes for our intended analysis in four parts: we justify the selection of IXPs considered (§II-A), the control plane datasets (with BGP information) we collected for the study (§II-B), and the methodology used to infer RP (§II-C). In the subsequent sections (§III, §IV, and §V), we provide further details about the specific methodology and metrics used in each corresponding analysis.

A. Peering Infrastructure Selection

To identify networks connected via RP, and prefixes and routes announced via RP, we required peering infrastructures that had (i) publicly available BGP routing data, and (ii) an active measurement vantage point (VP) attached to the IXP switching fabric. We consider an active measurement VP as the IXPs with the availability of RouteViews collectors capable of performing active measurements [19]. We use the RouteViews measurement infrastructure (as we will mention in the following section) because of the VP's location and lack of measurement limitations (such as Looking Glasses tools).[1]

Table I presents the seven selected IXPs where we had both BGP routing data and active measurement capability among the existing 20 IXPs which offer the necessary combination of RouteViews and Scamper [20]. Among the selected IXPs, we analyze five of the world's ten largest IXPs by membership [21], [22], deployed in five different countries. The three Brazilian IXPs (i.e., PTT sites) are part of the largest ecosystem of public IXPs in the world (IX.br) and are the leading Latin American IXPs in terms of average traffic volumes (≈12.9, 9.2, and 1.4 Tbps, respectively) [23], [24], [25].

[1] We tried using AMS-IX for our analysis, which had the required measurement infrastructure, but its VP was unavailable for maintenance during the time of our data collection.

TABLE I

Seven Analyzed IXPs in Our Work, Along With the Number of Interfaces Observed on 2022-10-14 (2022-10-17 for PTT-RJ) and the BGP Data Availability in Each Peering Infrastructure. These Dates Represent the Days With the Maximum Number of Interfaces at Each IXP

IXP	Location	Observed Interfaces	BGP VPs LG	PCH
PTT-SP	Sao Paulo, BR	2,163	✓	✗
LINX	Londres, UK	876	✓	✓
NAPAfrica	Johannesburg, ZA	611	✗	✓
PTT-RJ	Rio de Janeiro, BR	418	✓	✗
PTT-CE	Fortaleza, BR	419	✓	✗
Eq-Ash	Ashburn, VA, US	375	✗	✓
Eq-Chi	Chicago, IL, US	265	✗	✓

B. Datasets

To identify the peering router's IP and ASN of all members at each IXP, we combine multiple public data sources for all IXPs except for LINX, which publishes this information through their member portal [26]. We collected membership data and subnet information from Euro-IX [21] and the publicly available databases of Hurricane Electric (HE) [22], PeeringDB (PDB) [27], and Packet Clearing House (PCH) IXP Directory [28]. In cases of conflicts, we followed the preference ordering described in Nomikos et al. [15]: *Euro-IX > HE > PDB > PCH*. According to the authors, Euro-IX is the most reliable data source since its information is provided directly by the IXPs. The additional sources are potentially more inaccurate and outdated since they depend on ASes providing timely and accurate information.

To address cases of conflicting data, we consider IXP websites as the most reliable source of information since the data are directly provided by the IXP operators; in fact, while websites may share peering policy information with e.g., PeeringDB, they maintain their own IXP-related information, such as membership lists

We used two sources of BGP routing data: (i) Looking Glass (LG) of the IXP which observes routes from the IXP's Route Server and (ii) routes from the archive collected by PCH [29]. For IXPs with both PCH and LG views, we used data archived by PCH because it has greater visibility of routes advertised by IXP members. For example, when comparing both datasets for LINX, we observed 3.9x more routes and 2.0x more prefixes from PCH than from LG views. We discarded: (i) routes with artifacts, such as reserved/unassigned ASes [30] and loops; (ii) prefixes shorter than /8 or longer than /24.

At each IXP listed in Table I, we used RouteViews collectors which were directly connected to the IXP LAN to conduct active measurements using scamper [31]. Figure 1 illustrates the measurement architecture of each RouteViews collector and how we used them to conduct active measurements.

To identify which networks are connected remotely at IXPs, we conduct active latency measurements to each IXP member's peering router. These measurements use the IP address that the collector has in the IXP LAN (X.1), so that probes and responses cross the IXP LAN, as in when we probe X.2

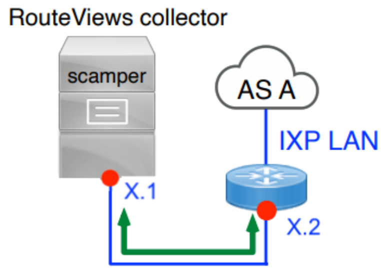


Fig. 1. Architecture of our data plane measurements (similar to Mazzola et.al. [18]). We used RouteViews collectors with an interface in the IXP LAN as VPs for data plane measurements. Delay measurements to the peering router of each IXP member (e.g., X.2) used the collector's IP address in the IXP LAN (X.1), so the probes and responses crossed the IXP LAN.

in Figure 1. The *ping* responses help us to understand the geographic distance between the IXP and the IXP member's peering router and, consequently, infer how far they are from the analyzed peering infrastructures.

C. Distinguishing Remote From Local Peering

To infer members using RP at all seven IXPs, we used the method of Castro et al. [7], which uses latency measurements and empirically obtained thresholds as a proxy of physical distance, with the following approach. For each IXP, we associated IXP member ASes and their assigned IXP IP addresses using the datasets mentioned in §II-B. We performed latency measurements to these addresses between 2022-08-01 and 2022-10-31. From each RouteViews scamper instance, we probed each interface with 20 *pings* per day and used the minimum latency for each address to account for cases of transient congestion. To ensure that the ping replies returned directly over the peering infrastructure, we discarded measurements where the replies had an IP-TTL value that appeared to have been decremented (i.e., not 64 or 255). If the minimum latency from a given interface was 10ms or higher, we classified the member's router as remotely connected to the IXP; a latency of 10ms would roughly correspond to a distance of up to 1000km from the IXP [32], [33]. By having an interface with latency consistently higher than 10ms over the 20 probes, we can guarantee that this behaviour is exclusively related to propagation delay and has no potential implications from other delay types (e.g., queuing delay). We adopted the method in Castro et al. [7] because its latency threshold alone yielded accurate results for single metropolitan area peering infrastructures [34], which is the case of the analyzed IXPs in our work (see §II-A).

To further assess the correctness of our inferences – and similar to step 2 in Giotsas et al. [34] (*colocation-informed RTT interpretation*) – we obtained the colocation facilities of each of the seven analyzed IXPs in public data sources (IXP websites and PeeringDB) and computed the distance between them. We observed that Equinix Ashburn has the largest distance between facilities (i.e., 80km), which corresponds to a latency of ≈1ms. Therefore, any IXP peer interface with latency consistently higher than 10ms is unlikely to be a local peer at the IXPs we examined.

III. RP Analysis over Time

RP is widely deployed in IXPs around the world nowadays, representing up to 40% of the member base in the largest IXPs [18], [34]. According to Giotsas et al. [34], as of mid-2018, the deployment of new RP connections had been major factor in the recent IXP growth.

Methodology. We pose two questions: (i) are RP connections still a major contributor to the growth of IXPs? (ii) How does the prevalence of RP changes over time in IXPs? We answer these questions in three steps, as follows. To infer RP at IXPs, we use a methodology similar to Mazzola et al. [18]: during three months, we continuously collect IXP membership data, announced routes at IXPs, and latency measurements from a VP inside the IXP to each member interface (§II-C). Then, we compare our results regarding remotely inferred interfaces (§III-A) and prefixes (§III-B) with the most recent results from the literature.

A. How Does Remote Membership Vary With Time?

First, we investigate how the prevalence of RP (in terms of member interfaces) changes with time, as shown in Table II. During a preliminary investigation, we analyzed every daily measurement collected to identify change patterns on the numbers of remote and local member interfaces. As described by [3] and confirmed by our data (less than 1% of change), the churn in IXP membership and peering interfaces is negligible in daily time scales and is better observable in weekly terms. As our primary goal is to observe trends in the deployment of RP, we selected two measurement samples (one day in the first month and one in the third) instead of analyzing the whole three-month dataset collected. To choose both days, we selected the ones that showed the highest numbers of prefixes and connected interfaces at IXPs for each month to increase the visibility of the IXP routing data. To further extend our analysis and provide richer insights, we compare the results with the numbers obtained by Mazzola et al. [18] in May 2021, extending the analysis period from 3 months to 1.5 years.

We found that remote member interfaces' deployment has grown since 2021 in almost all IXPs (6/7) and that the amount of (aggregated) growth varied according to the characteristics of the IXP. The numbers indicate that well-established IXPs, such as LINX and PTT-SP, have grown less, which conforms intuition: these massive IXPs already have a widespread member base and less space to grow in local and remote networks compared to emergent infrastructures, such as NAPAfrica and PTT-CE. The growth ranged between 4.4% (681 to 711 interfaces in PTT-SP) and 22.5% (40 to 49 interfaces in NAPAfrica). The odd case, Equinix Ashburn, actually had a decrease in the number of remote member interfaces (-17.1%), showing that the RP growth cannot be simply assumed (35 to 29 remote interfaces).

We contrast our findings with earlier work of Giotsas et al. [34], whose authors looked at the RP evolution at five IXPs between 2017 and 2018. They concluded that remote member interfaces on the five IXPs grew 20% over one year, but this analysis was for all IXPs combined

TABLE II

NUMBER OF INTERFACES CONNECTED VIA RP AT IXPS.THE PREVALENCE OF RP GREW SLIGHTLY 6 OF 7 IXPS BETWEEN 05-2021 AND 10-2022 (MATCHED BY AN INCREASE IN THE ABSOLUTE NUMBER OF REMOTE INTERFACES).EQ-ASH SHOWED A DECREASE IN REMOTE INTERFACES, BOTH ABSOLUTELY AND IN PREVALENCE

	Remote Interfaces		
	05-05-2021 [18]	16-08-2022	14-10-2022 (17-10-2022 for RJ)
PTT-SP	681 of 2,169 (31.4%)	729 of 2,156 (33.4%)	711 of 2,163 (32.9%)
LINX	121 of 911 (13.3%)	129 of 878 (14.7%)	128 of 876 (14.6%)
NAPAfrica	40 of 542 (7.4%)	52 of 612 (8.5%)	49 of 612 (8.0%)
PTT-RJ	61 of 462 (13.2%)	67 of 427 (15.7%)	66 of 443 (14.9%)
PTT-CE	139 of 395 (35.2%)	169 of 423 (39.9%)	165 of 419 (39,4%)
Eq-Ash	35 of 365 (9.6%)	31 of 375 (8.3%)	29 of 375 (7.7%)
Eq-Chi	17 of 259 (6.6%)	18 of 265 (6.8%)	18 of 265 (6.8%)

aggregated. We look in more depth and find that this growth is not equally distributed, being influenced by basic properties of the IXP (e.g., size, traffic, location).

We can also observe (from Table II) that the fraction of remote interfaces remained relatively stable, with changes under 5% (in PTT-CE, it went from 35.2% to 39.4%, having 139 remote interfaces in 2021 and 165 in the end of 2022). This is so because the number of local interfaces fell in some IXPs *despite* the growth in RP. For PTT-RJ and LINX, the number of local interfaces has decreased -5.2% and -5.3%, respectively. In virtually all IXPs (6/7), the number of remote interfaces increased, reaching up to 10× when compared than local interfaces. NAPAfrica, the younger/smaller IXP in our set, had a subtle difference (1.8×), hinting that for emergent IXPs the accelerated grow may happen similarly for both remote and local interfaces.

B. How Do Remotely Announced Prefixes Vary With Time?

To answer the question, first we combine the information about remote interfaces with IXP BGP routing data to identify the prefixes announced by these members. To classify a *prefix* as local or remote, we tag it according to the nextHop interface of the BGP route, which refers to the IXP member announcing it at the IXP. A prefix that has routes being announced by *both* remote *and* local members is denoted as *hybrid*. We highlight that the prefixes observed were not converted to /24 prefixes and all numbers shown in the results reflects the prefixes as seen on the IXP BGP routing tables.

Table III shows the results obtained for the three-month data collection compared with data from 2021 of Mazzola et al. [18]. For most IXPs (5/7), the number of remote prefixes decreased from 2021 to 2022. The reasons for this, according to our private talks with network operators,

TABLE III

NUMBER AND % OF REMOTE PREFIXES AT IXPS. REMOTE PREFIXESDECREASED IN FOUR IXPS EVEN THOUGH THEY SHOWED A GROWTH IN REMOTE MEMBERS OVER TIME

	Remote Prefixes		
	05-05-2021 [18]	16-08-2022	14-10-2022 (17-10-2022 - RJ)
PTT-SP	19,612 of 154,561 (12.7%)	13,764 of 127,285 (10.8%)	12,453 of 132,550 (9.4%)
LINX	71,452 of 482,643 (14.8%)	67,794 of 472,746 (14.3%)	67,663 of 463,036 (14.6%)
NAPAfrica	7,252 of 144,513 (5.0%)	8,301 of 174,449 (4.8%)	8,435 of 175,797 (4.8%)
PTT-RJ	3,850 of 128,652 (3.0%)	2,654 of 98,176 (2.7%)	1,640 of 96,805 (1.7%)
PTT-CE	6,869 of 26,597 (25.8%)	5,356 of 28,017 (19.1%)	5,367 of 27,137 (19.7%)
Eq-Ash	46,752 of 525,688 (8.9%)	21,698 of 600,632 (3.6%)	21,679 of 597,586 (3.6%)
Eq-Chi	8,120 of 271,855 (3.0%)	8,686 of 344,233 (2.5%)	8,745 of 344,312 (2.5%)

is that networks use RP more often to fetch/download content (faster) from remote locations (via more established IXPs) than to deliver/upload content to distant networks. We did not observe a change pattern in terms of remote prefix prevalence, ranging broadly between -53,6% (25,073 fewer prefixes in Equinix-Ash) and 16.3% (1,183 more prefixes in NAPAfrica). One might expect that an increase in the number of remote members would lead to an increase in remote prefixes, but we found no correlation: the four IXPs with a reduction in remote prefixes *actually increased* the number of remote members in the same period (as shown in §III-A). In nearly half of the IXPs (4/7), we saw a shift in the prevalence of prefixes, from remote to local ones.

IV. ROUTING MISPRACTICES CAUSED BY RP

If operators do not correctly configure their deployment of RP, ASes connected to multiple IXPs using different types of peering (i.e., local in some IXPs and remote at others) may introduce *trombone paths* to other peers. This section investigates likely routing mispractice cases associated with RP misconfiguration. Trombone paths, in this context, happen when two networks locally connected in a location (e.g., London) end up exchanging traffic via a distant peering facility (e.g., Chicago) that both are also members of, but via RP, causing poor routing performance and impaired connectivity.

The Internet routing best practices indicate that more specific prefixes have a preference (as the intended destination for packets) over less specific prefixes. For example, a prefix 1.0.0.0/24 will be preferred over 1.0.0.0/16. In a peering scenario, the more specific prefixes (routes) announced by one AS in one IXP will be preferred for traffic exchange over less specific prefixes that can be announced at one transit provider. As reported by [9], an AS (in São Paulo) that has peering connections to a local IXP and a remote IXP can damage its peering connection performance if the operator does not correctly configure its prefix announcements in both

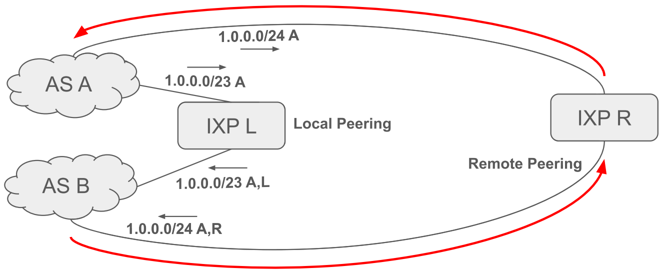


Fig. 2. Routing mispractice behavior when announcing at remote and local IXPs. AS A announces a more specific prefix to the IXP it connects via RP and a less specific prefix to the IXP it connects via Local Peering. When AS B receives both routes, it will give preference to the one via IXP R (red path) considering Internet routing best practices.

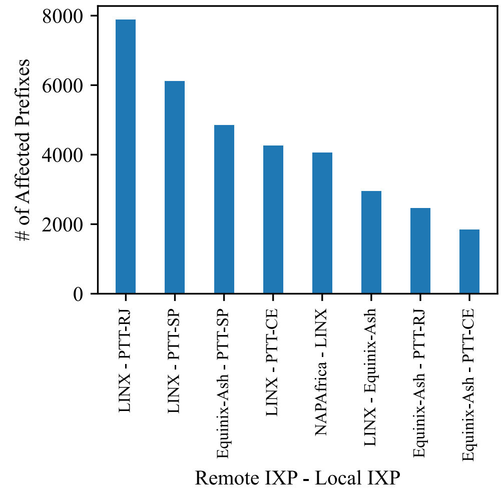


Fig. 3. IXPs involved in the identified prefixes with route announcements mispractices.

IXPs. We exemplify this scenario in Figure 2, where an AS A connects to an IXP nearby (i.e. local peering on IXP X) and to a distant IXP (i.e. RP on IXP Y). By wrongly announcing more specific prefixes to the remote IXP instead of the local IXP, it can inadvertently steer its traffic exchange thousands of kilometres away (green path) from the optimal peering infrastructure (IXP X). For example, if an AS B also connected at IXP X via local peering and IXP Y via RP, the more specific prefix wrongly announced would lead the traffic exchange between them to go via the distant IXP Y, even though the better option (IXP X) is where both ASes are locally connected. In the rest of this section, we denote these likely problematic cases as *trombone prefixes*.

Methodology. We use the BGP data collected between 2022-08-01 and 2022-10-31 along with ping measurements performed from VPs in IXPs to corresponding IXP member interfaces (§ III). The data allows us to identify the ASes that are present in multiple IXPs (in our set), by definition with one local connection and two or more, remote. For these ASes, we check the set of prefixes they announce in more than one IXP. The last step is to verify the of trombone prefix cases, that is, where a more specific prefix is announced at the remote IXP while a less specific prefix is announced at the local IXP.

We quantify the daily number of trombone prefixes and identify the ASes that announce them. We observed more than 480 trombone prefixes/day, with a peak of 1069/day. The daily number of ASes varied between 4 and 31, with an average of 17 ASes daily over the entire period; the 31 ASes were responsible for 1408 prefixes. We discover that both the number of trombone prefixes and ASes responsible for them can vary over time, indicating that they usually represent a *transient* routing problem that ASes fix in a matter of days. Looking further at the ASes that own such prefixes, we see just two ASes being accountable for 56.8% of all the overall trombone prefixes on average in the two-month period (AS52320 and AS262589, with 12616 and 8417 occurrences each). Not surprisingly, perhaps, we find that these two ASes were also the ones responsible for the peak occurrences (representing 78.6% of the prefixes on this day). Both ASes are continental networks offering IP transit, cloud and RP services for Latin American customers. We believe these prefixes represent routes from these ASes' customers that were improperly announced by the transit provider and subsequentially fixed.

IX.br and LINX are involved in most cases identified. Here we shift the analysis to the *IXPs* most commonly involved in the trombone prefixes. Figure 3 shows the most relevant combinations of IXPs for two months; we only display the IXP pairs with more than 1000 occurrences, which represent 93.0% of the total. The order is relevant, such that the first and second IXPs of the pair are, respectively, announcing the most specific prefix and the less specific prefix. We can observe in the figure that 50% of the cases are due to less specific prefixes being announced locally by networks connected at one of the IX.br IXPs (i.e., PTT-SP, PTT-RJ, and PTT-CE) and more specific versions of it announced remotely at LINX. Five ASes were responsible for more than 86.8% of the cases on the three IXPs: the previously mentioned AS52320 and AS262589, and AS28329, AS14840, and AS267613. The latter three are Brazilian networks with continental coverage, also offering IP transit and cloud services to Latin American clients.

Even though looking only at control plane data cannot guarantee that these cases represent actual routing problems, anedoctally, they often do. Our study reveals that there is a considerable number of occurrences happening over time. If these cases are not dealt with properly, they may affect the performance and connectivity of these networks and their customers and impose financial losses.

V. Connection Stability of IXP Members

In this section, we investigate to which extent RP can affect the stability of IXP members' interface connections to the IXP route server. Understanding how much a peering connection type is less stable than others can be helpful since downtime can cause significant financial, performance and reputational loss for ASes [35]. Based on earlier work [36], we expect to see remote interfaces being less stable than local ones because they are not physically connected at the IXPs and rely on a third-party infrastructure in which they do not have control to reach the peering facilities. Besides, since many RP resellers usually connect multiple remote networks through shared logical ports, in which higher instability to one physical interface can affect many clients.

Methodology. As mentioned by Ager et al. [3], analyzing large IXPs is a complex task of constantly looking at a moving target. On weekly/monthly time scales, it is possible to observe changes in the IXP membership, number of switch ports, and peerings. In contrast, traffic variations and disconnections are the main causes for changing IXP conditions on daily or hourly time scales. To analyze the connection stability of remote and local interfaces at IXPs, we collected membership data from IXP LGs every 15 minutes over two months (2022-11-19 to 2023-01-23). The 15-minute granularity over the two months allows us to eliminate cases of transient or short-lasting instability for the different types of peering.

Our analysis is only feasible in IXPs with publicly available LGs, which enables real-time data collection of the current BGP tables of members individually, allowing us to classify each of the IXP interfaces according to their remoteness: LINX, PTT-SP, PTT-RJ, and PTT-RJ. For NAPAfrica, Equinix-Ash, and Equinix-Chi, there was no LGs offering open access to BGP data (see §I). Our results are especially relevant despite having only 4 of the 7 IXPs in the study analyzed, given that no previous study has performed such a data collection and analysis over a similar period extension. Besides, collecting these data is complex since they are not usually publicly available or have collection limitations on the VPs. We exclude from the analysis a small fraction of IXP interfaces (1.6%) which either changed from remote to local and vice-versa or were not present during the entire collection period. We collected 7008 samples of the connected interfaces to RS on four IXPs (LINX, PTT-SP, PTT-RJ e PTT-CE) between 2022-11-19 and 2023-01-23 (see § II-B).

Interfaces switch between two states, up or down, which we use to compute the following metrics:

- **Median Uptime Between Failures.** It represents the stability of a connection and is computed by the median of all the hours one interface stayed in the up state uninterruptedly during the collection period. If the interface remains up between data collection X and $X+1$, we add 15 minutes of uptime to the interface.
- **State changes.** The metric indicates how common errors are on IXP's interfaces. We compute it as the sum of state changes (up to down, and vice-versa), between all data collections.
- **Mean Time Between Failures.** MTBF is (a well-known metric) that we use to indicate the level of availability of interfaces. We compute it by dividing the total uptime by the number of failures.
- **Reliability.** Measures the ability of a system or component to perform its intended function for a specified period. The system's reliability can be calculated using various methods, including reliability models, failure data analysis, and reliability testing. We computed it using the MTBF metric and two different intervals, day and month: $Reliability = e^{-\frac{1}{MTBF} \times Time}$

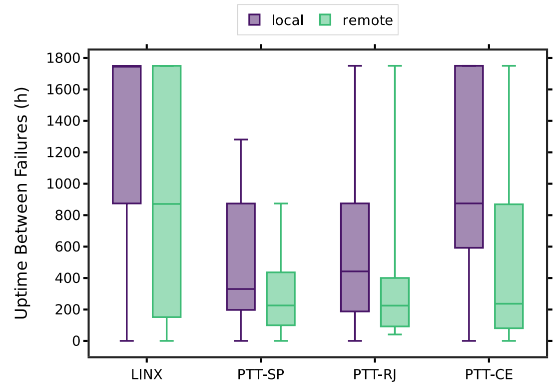


Fig. 4. Median uptime between failures per IXP interface. Remote interfaces stay less time continuously without failures.

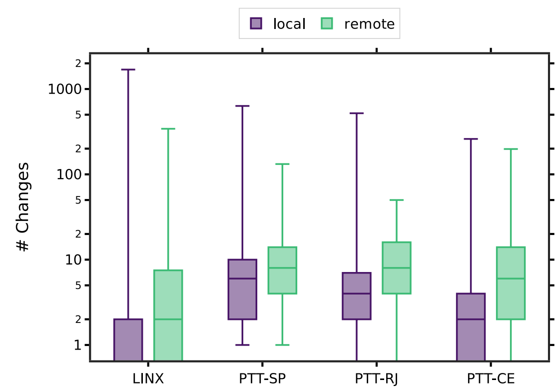


Fig. 5. Number of state changes per IXP interface; the y axis is in log scale. Remote interfaces are subject to many more state changes.

RP interfaces stay less time continuously functioning than local ones. We first evaluate whether the connection type affects the interfaces' stability, by comparing the median uptime between failures for remote and local interfaces. Figure 4 shows that the uptime for local interfaces is considerably higher than remote ones. In other words, remote interfaces tend to stay less time continuously functioning before a change of state (e.g., failure, BGP session issue). This difference is striking in the case of LINX and PTT-CE. For LINX, the disparity reaches two times higher uptime for local members (1749 hours to local vs 871 hours to remotes) when considering at least 50% of the interfaces. For PPT-CE, at least 50% of the local interfaces have uptime higher than 874 hours, while the uptime of at least 50% of the remote ones does not reach 236 hours (3.7 times lower).

Local interfaces suffer fewer state changes. Next, we look at the state change number for each connection type. Too many state changes indicate lower stability, since the members' BGP session is constantly shutdown and re-established. Figure 5 shows the results using a Y-axis log-scale. We observe that remote interfaces consistently present more state transitions than local ones, reaching up to 3.5× more changes. While 75% of the local members in each IXP have no more than between 10 and 2 changes, depending on the IXP, the corresponding values for remote connections were between 16 and 5. Combined with the uptime hours previously presented, these numbers strongly indicate less connection stability for RP.

Local peers are greatly more reliable than RP. Finally, we compare the metric Reliability for the IXP interfaces, for periods of different durations, day and month. Members with higher reliability also present higher availability and less time between intermittent failures. Figures 6a and 6b show the results 1-day and 1-month, respectively. Even though reliability is directly related to the time interval, remote interfaces have lower reliability than local ones in both scenarios for all IXPs. However, the results vary considerably depending on the duration of the period considered. While in the 1-day analysis, there was little difference between local and remote (the median differences varied between 1.37% and 3.98%), in the 1-month, there are massive differences (reaching 47.05% and 33.85% for PTT-CE and LINX, respectively).

As mentioned in previous work [15], [17], [36], the usage of RP can introduce interconnection drawbacks such as loss of resilience and difficulty for layer-3 management. Besides, as remote interfaces represent geographically distant ASes connected through longer chains of involved third-party hardware, it is easier for localized failures in the IXP and colocation facilities to become widespread, pottentially affecting many other networks. Our results combined showed that, in addition to having less uptime and more state changes, remote interfaces also show less reliability over time and are less stable when compared to local ones in the analyzed IXPs. Such results benefit not only for the networks connectd via RP but also ASes interconnecting with remote peers. While for the first it can shed light on ways to improve the interconnection stability of their resellers and their own networks, for the latter can represent a better perspective on more stable and reliable peers to exchange traffic.

This confirms our expectations and shows there can be a substantial difference considering in some large IXPs.

VI. Usage of RP BGP Communities for TE

BGP communities have been used in IXP to tag routes and help with traffic engineering [37]. Communities can also be used to perform TE in RP connections, such as tagging connections whose latency exceeds some threshold. IX.br started supporting BGP communities targetting remote networks in March 2022. This was accomplished with two changes: the RS in IXPs started tagging remote routes with *informational communities* to assist ASes in making traffic engineering decisions; and IXPs started supporting *action communities* added by the IXP members to impose their routing policies on their routes. We look at which communities networks add when sharing routes with the IXP.

Methodology. We analyze the usage of RP-related BGP communities for the three IXPs among our set that have support for such communities (PTT-SP, PTT-RJ, and PTT-CE). RP-related communities can be used to avoid route exports and to add different levels of prepending for ASes when matching certain conditions, such as RTT thresholds, packet loss thresholds, or announcement within some RIR region. The IX.br is responsible for measuring both latency and packet loss and marking up the routes with such characteristics.

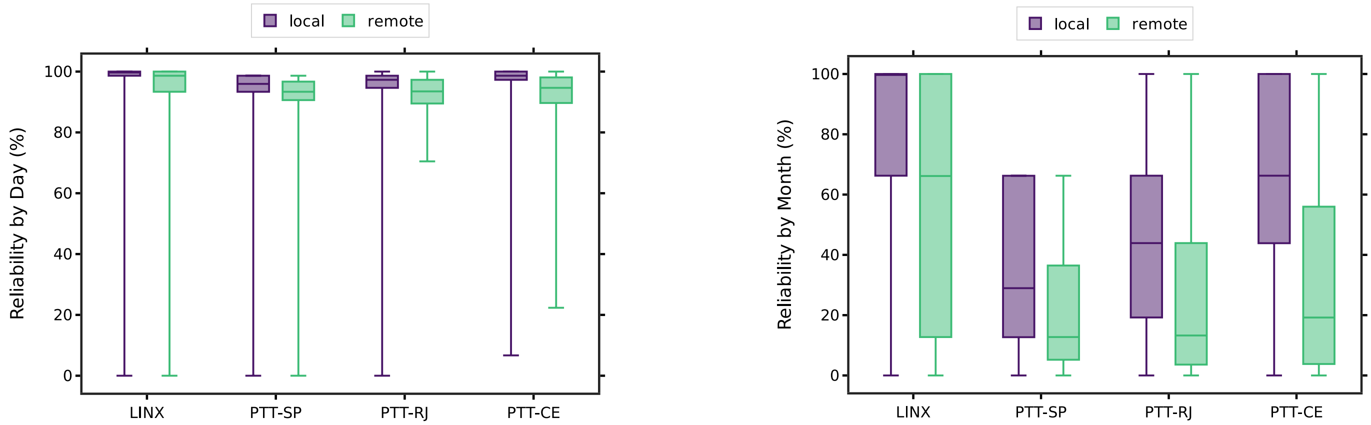
Using the LG API in each IXP, we collected a routing data snapshot on 2023-01-17 from their primary IPv4 RS. The information captured for every route includes a prefix, next-hop address, AS-Path, and lists of BGP communities. We also fetched the RS configuration file containing the semantics of available informational and action BGP communities. To identify the communities defined by the IXPs, we build a *dictionary* using the LG API. We identified 96 communities related to RP on IX.br, out of the total 649 available. Their actions allow ASes to avoid route export and path-prepend once, twice or thrice to peers with RTT higher than 10, 50, 100, 150, 200 and 250 ms.

We process every route observed in the IXP BGP data for our analyses and compare the BGP communities in it with our community dictionary. We then counted the number of RP communities used in each route by each AS (i.e., if a route have two RP communities, we add two to the AS count).

Which types of BGP communities are more popular? First, we identify which specific RP-related communities are prevalent in the IXP route server member's routes. On PTT-SP, the most common actions are *adding a single prepend* to members with RTT higher than 10ms and 50ms (4911 and 3860 instances, respectively). In contrast, the most common action in PTT-CE and PTT-RJ was to *avoid route export* for ASes with RTT higher than 10ms (2024 and 188 occurrences, respectively).

Are RP-related BGP Communities used? These fine-grained traffic engineering BGP communities for RP were introduced in March 2022 to all the 35 Brazilian IXPs. According to network operators from IX.br, this was prompted by a broad request from the network operation community. The general understanding has been that the communities would be widely used, and to confirm whether this was true or not, and to which extent, we examined the usage of RP BGP communities. Surprisingly, we discover that they are still not so widespread, at least when compared to the rest of BGP communities. For example, in PTT-SP, the fraction of RP-related action communities was under 0.27%.

We believe the low usage is because of two main reasons: the lack of knowledge about the potential impacts that remote peers may cause on performance; and the lack familiarity with the communities available at the IXPs. According to network operators, measurements to evaluate the peering performance are not proactively and regularly done to every individual peer. Instead, networks generally perform more detailed traffic engineering analysis when clients complain of reduced connectivity or performance. Unfortunately, the lack of periodic analysis and the opportunity to use RP-related BGP communities may hinder optimal peering decisions overall. As shown in Mazzola et al. [18], using remote connections to deliver traffic can impose latency penalties compared to using a local route alternative for many cases. With respect to the lack of familiarity, given that different IXPs provide different services and deploy distinct BGP communities, network operators may still need to learn about the possibility of fine-grained traffic engineering. We discussed this with the operational community, and learned that often they deploy



(a) Interface's reliability considering 1-day period.

(b) Interface's reliability considering 1-month period.

Fig. 6. Level of reliability using the reliability metric. Results show that remote interfaces are less reliable than local ones, reaching a difference up to 47.05%.

a single configuration model: a configuration is performed considering communities that are available at every IXP (e.g., avoid export to ASN, export only to ASN) and then replicated to all other IXPs.

Do ASes apply different RP communities in distinct IXPs to steer traffic? We now examine the numbers and characteristics of the ASes that are using RP BGP communities to their routes. We found that only a tiny number of ASes use these communities, representing 0.5% (11 ASes' interfaces out of 2175) in PTT-SP and 1.1% (5 ASes' interfaces out of 471) in PTT-CE. When looking further at these ASes, we can highlight that one AS (AS7195) uses RP communities for its routes on the three IXPs examined, and three ASes (AS61832, AS53202, and AS61568) use them in two IXPs (PTT-SP and PTT-CE). AS7195 (i.e., EdgeUno) is a continental company focusing on IP transit, RP, and cloud hosting services. It adds the community to avoid route export to ASes with RTT $>$ 10 to, on average, 2.5% of their announced prefixes. They could represent prefixes needing better performance, which would not benefit from having long-distance networks redistributing them to their customers. The other three ASes, AS61832, AS53202, and AS61568, are ISPs connected to multiple IXPs worldwide. AS53202 and AS61568 add communities to avoid route export for ASes with RTT $>$ 50ms to 7.4% and 0.4%, respectively, of their announced prefixes in both IXPs. AS61832, in contrast, makes a distinguished use of these actions against remote peers: in PTT-CE, AS61832 uses the "No export to RTT $>$ 10ms" action on 74.4% of its prefixes, but on PTT-SP, it applies the community "Add one prepend to RTT $>$ 10ms" to all its announced routes. This approach inflates the AS-Path of the routes distributed in PTT-SP and forces traffic for some of its routes to go preferably via its connection in PTT-CE.

VII. Web Portal

We created a web portal to the community, making our results publicly accessible and enabling users to interactively dissect the results.[2] The portal allows users to view the analyses we conducted on RP deployment between August

[2]Our portal can be accessed at http://remotepeeringportal.c3.furg.br [38].

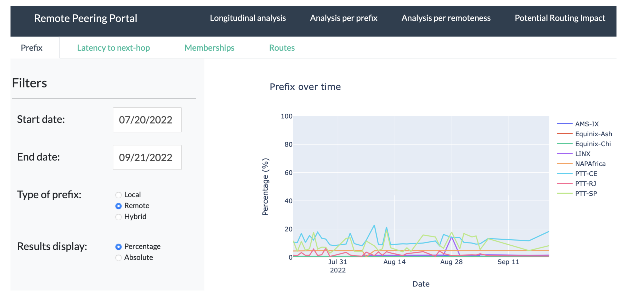


Fig. 7. Example of analysis in the portal's GUI.

and October 2022. For each IXP, we provide results over time for the number and type of IXP interfaces, announced prefixes, routes, and the minimum/average RTT for each IXP member (see Figure 7). Additionally, users can obtain a detailed view of the announced BGP routes at IXPs, including prefix, next-hop, and AS Path information per day. Furthermore, we present results that demonstrate the potential routing impacts caused by prefixes announced by ASes connected via RP or local peering at IXPs. Users can interact with and query all of the results using a variety of selectable options.

We plan to enable data download for the community to encourage reproducibility. We invite interested IXPs to contact us if they want to have their peering infrastructure on the portal.

VIII. Related Work

With the growing deployment of RP, there have been several efforts to investigate this interconnection practice. We divide related work into three categories: (1) methods to identify RP at IXPs, (2) studies to explore implications of RP on the Internet, and (3) work investigating the characteristics and usage patterns of BGP communities at IXPs.

Inferring Remote Peering. Two main related methodologies have been proposed in the literature. In 2014, Castro et al. [7] introduced a conservative inference method based on measuring propagation delay to IXP interfaces connected to it via pings and identifying RP via a empirically obtained 10ms latency threshold. Results showed that 91% of the 22 studied IXPs showed networks connecting via RP, with potential to offload up to 25% of its transit-provider traffic via

RP. In 2018, Nomikos et al. [15] also proposed a methodology to infer RP, combining latency measurements with additional RP features, such as port capacity and AS presence at colocation facilities. They inferred that 90% of the analyzed IXPs had more than 10% of their members using RP, with a few having up to 40% of their members as remote. In 2021, the authors extended the previous work [34], with changes in the methodology and additional analysis on Wide-Area IXPs.

Implications of Remote Peering. In 2017, Giotsas et al. [17] showed that the rise of RP made it easier for localized failures in IXP and colocation facilities to become widespread. Bian et al. [16] proposed a methodology to characterize anycast based on archived BGP routing information collected globally. While trying to infer anycast prefixes, the authors found that RP peering could potentially affect 38% of anycast prefixes with an average latency increase of 35.1ms. Bertholdo et al. [36] analyzed the stability of participants' connections to IXP route-servers. Their results show that unstable interfaces were mainly caused by large regional ASes connected in just one IXP or ASes connected via RP at IXPs. Finally, Mazzola et al. [18] compared the latency impact to reach prefixes announced by remote peers at eight different IXPs using routes from remote peers, local peers, and transit providers. Results showed that despite remote routes being generally preferred by BGP given their shorter AS path, the local routes had lower latency than the remote route in the majority of cases.

Usage of BGP Communities. In [39], Giotsas et al. collected communities from router server with semantics defined by the IXP in order to infer p2p links. In [40], Philipp et al. examined the role of route servers in IXPs, using communities for some inferences. Krenc et al. [41] observed announcements at BGP collectors (e.g. RIPE and RouteViews) aiming to understand better community usage, but limited to when/how ASes *add* communities to announcements and when they *remove*. Mazzola et al. [37], on the other hand, evaluated how action communities used for traffic engineering are used by ASes in IXPs and performed a characterization about BGP communities usage patterns.

IX. Conclusion

IXPs are critical infrastructures that support ever-increasing data volumes and service requirements of modern Internet services. However, the recent growth of RP introduces new challenges for traffic engineering because peering may no longer keep local traffic local. Our paper sheds light on the RP growth over the last year in seven IXPs and explores some of the implications on the use of RP on the Internet. We highlight some of the following key findings.

RP growth varies according to IXP characteristics. Using results from a three-month data collection and comparisons with state-of-the-art data, we found that remote interfaces have grown since 2021 in almost all IXPs evaluated. The growth was directly related to how developed and prevalent the peering infrastructure was. While the growth was lower in well-established IXPs, RP development was predominant in more emergent peering infrastructures.

Undesirable trombone prefixes may be common, due to route announcements mispractices. ASes connected to multiple IXPs with a combination of local and remote connections may unintentionally occur in route announcements mispractices. Our analysis showed that more than 60 distinct ASes announced most specific prefixes on the remote IXP instead of prioritizing their local IXP connection. We found over 37k prefixes with highly likely trombone paths, impairing peering performance.

Remote interfaces are consistently more unstable than local ones. A concern about RP growth at IXPs is that networks using a shared port or being geographically distant would impose higher instability on their connection to the IXP RS, affecting other members. Our results indicate that this is indeed the case in all analyzed IXPs. Remote interfaces seemed to be less reliable, presenting differences to local peers that reach up to 47.05% on a monthly analysis. Besides, the remote interfaces remain less time in `up` state between failures, with local interfaces staying up to 3.7× more active. Lastly, remote interfaces showed up to 3.5× more state changes (from `up` to `down`) than local peers.

BGP communities' usage to perform TE on remote peers is still not widespread. Many modern IXPs started to offer specific BGP communities to filter route export or perform some action (e.g., prepend) to networks connected remotely. Our analysis of these communities at three IXPs (PTT-SP, PTT-RJ, and PTT-CE) revealed that they are still negligible, representing less than 0.27% of all the action communities seen at the IXP routes.

Our findings helped characterize some of the RP implications to Internet routing and its growth in different IXPs. We believe that considering additional IXPs, and analyzing IPv6 prefixes would improve the community's understanding of the RP evolution and deployment. Besides, even though our analysis was comprehensive in including some of the largest IXPs, in Internet measurements we say it is virtually always possible to grow the dataset to include more VPs (IXPs) and for longer periods, so "it is never enough". Improving current methodologies is also crucial to promote further research on RP implications to performance and security.

References

[1] Internet Society. (2021). *IXPs Make the Internet Faster and More Affordable*. [Online]. Available: https://www.internetsociety.org/issues/ixps/

[2] N. Chatzis, G. Smaragdakis, A. Feldmann, and W. Willinger, "There is more to IXPs than meets the eye," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 43, no. 5, pp. 19–28, Nov. 2013.

[3] B. Ager, N. Chatzis, A. Feldmann, N. Sarrar, S. Uhlig, and W. Willinger, "Anatomy of a large European IXP," in *Proc. ACM SIGCOMM Conf. Appl., Technol., Architectures, Protocols Comput. Commun.*, Aug. 2012, pp. 163–174.

[4] B. Augustin, B. Krishnamurthy, and W. Willinger, "IXPs: Mapped?" in *Proc. 9th ACM SIGCOMM Conf. Internet Meas.*, Nov. 2009, pp. 336–349.

[5] DE-CIX. (2021). *Connect to DE-CIX via a Reseller*. [Online]. Available: https://www.de-cix.net/en/access/how-to-connect/connect-via-reseller

[6] AMS-IX. (2021). *Pricing*. [Online]. Available: https://www.ams-ix.net/ams/pricing

[7] I. Castro, J. C. Cardona, S. Gorinsky, and P. Francois, "Remote peering: More peering without Internet flattening," in *Proc. 10th ACM Int. Conf. Emerg. Netw. Experiments Technol.*, Dec. 2014, pp. 185–198.

[8] M. J. Levy. (2019). *Peer Locally, With Local Network on Local IXs or Not! (Alternate Title: Remote Peering is Bad for Content)*. [Online]. Available: https://www.globalpeeringforum.org/pastEvents/gpf14/presentations/Wed_2_MartinLevy_remote_peering_is_bad_for.pdf

[9] L. Almeida, "Good practices for ISP connection to international IXPs," in *Proc. 9th Forum*, 2019. [Online]. Available: https://youtu.be/bIfwuFVm0iI

[10] A. Nipper, B. Hedges, E. Verhoef, and J. Sirota, "Remote peering panel—Providers," in *Proc. 9th Forum*, 2018. [Online]. Available: https://www.youtube.com/watch?v=HQZY-DJNlxU&ab_channel=NICbrvideos

[11] European Peering Forum. (2016). *Panel: What Are the Challenges of Remote Peering*. [Online]. Available: https://www.peering-forum.eu/agenda?year=2016

[12] "Panel: Remote peering, with a look at resellers as well," in *Proc. 29th Euro-9th Forum*, Krakow, Poland, 2016. [Online]. Available: https://www.euro-ix.net/media/filer_public/ba/61/ba61bc32-f506-4ac7-b037-4dab8549c8a2/e-an-20161108-remote_peering.pdf

[13] Z. Ali. (2012). *Panel: Remote Peering, Ripe 65*. Amsterdam, The Netherlands. [Online]. Available: https://ripe65.ripe.net/presentations/196-RIPE65_EIXWG_ZA.pdf

[14] W. B. Norton. (2012). *The Great Remote Peering Debate*. [Online]. Available: http://drpeering.net/AskDrPeering/blog/articles/Ask_DrPeering/Entries/2012/9/18_The_Great_Remote_Peering_Debate.html

[15] G. Nomikos et al., "O peer, where art thou? Uncovering remote peering interconnections at IXPs," in *Proc. Internet Meas. Conf.*, New York, NY, USA, Oct. 2018, pp. 265–278.

[16] R. Bian, S. Hao, H. Wang, A. Dhamdere, A. Dainotti, and C. Cotton, "Towards passive analysis of anycast in global routing: Unintended impact of remote peering," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 49, no. 3, pp. 18–25, Nov. 2019.

[17] V. Giotsas, C. Dietzel, G. Smaragdakis, A. Feldmann, A. Berger, and E. Aben, "Detecting peering infrastructure outages in the wild," in *Proc. Conf. ACM Special Interest Group Data Commun.*, Aug. 2017, pp. 446–459.

[18] F. Mazzola, P. Marcos, I. Castro, M. Luckie, and M. Barcellos, "On the latency impact of remote peering," in *Passive and Active Measurement*, O. Hohlfeld, G. Moura, and C. Pelsser, Eds. Cham, Switzerland: Springer, 1007, pp. 367–392.

[19] (2020). *University of Oregon Route Views Project*. [Online]. Available: http://www.routeviews.org/routeviews/

[20] (2023). *Routeviews Collector Map*. [Online]. Available: https://www.routeviews.org/routeviews/index.php/map/

[21] Euro-IX. (2021). *The IXP Database*. [Online]. Available: https://ixpdb.euro-ix.net/en/

[22] Hurricane Electric. (2021). *Internet Exchange Report*. [Online]. Available: https://bgp.he.net/report/exchanges

[23] (2020). *IX.br—Brazilian Public IXP Project*. [Online]. Available: https://ix.br/intro

[24] E. Carisimo, J. M. D. Fiore, D. Dujovne, C. Pelsser, and J. I. Alvarez-Hamelin, "A first look at the Latin American IXPs," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 50, no. 1, pp. 18–24, Mar. 2020.

[25] S. H. B. Brito, M. Santos, R. dos Reis Fontes, D. A. L. Perez, and C. E. Rothenberg, "Dissecting the largest national ecosystem of public Internet eXchange points in Brazil," in *Passive and Active Measuremen*. Heraklion, Greece, 2016.

[26] LINX. (2021). *Members by IP/ASN*. [Online]. Available: https://portal.linx.net/members/members-ip-asn

[27] PeeringDB. (2020). *IXPs and Colocation Database*. [Online]. Available: https://www.peeringdb.com

[28] Packet Clearing House. (2020). *Internet Exchange Directory*. [Online]. Available: https://www.pch.net/ixp/dir

[29] PCH. (2021). *Daily Routing Snapshots*. [Online]. Available: https://www.pch.net/resources/

[30] IANA. (2020). *IANA Autonomous System (AS) Numbers*. [Online]. Available: https://www.iana.org/assignments/as-numbers/as-numbers.xml

[31] M. Luckie, "Scamper: A scalable and extensible packet prober for active measurement of the Internet," in *Proc. 10th ACM SIGCOMM Conf. Internet Meas.*, Nov. 2010, pp. 239–245.

[32] E. Katz-Bassett, J. P. John, A. Krishnamurthy, D. Wetherall, T. Anderson, and Y. Chawathe, "Towards IP geolocation using delay and topology measurements," in *Proc. 6th ACM SIGCOMM Conf. Internet Meas.*, Oct. 2006, pp. 71–84.

[33] B. Trammell and M. Kühlewind, "Revisiting the privacy implications of two-way Internet latency data," in *Passive and Active Measuremen*. Berlin, Germany, 2018, pp. 73–84.

[34] V. Giotsas et al., "O peer, where art thou? Uncovering remote peering interconnections at IXPs," *IEEE/ACM Trans. Netw.*, vol. 29, no. 1, pp. 1–16, Feb. 2021.

[35] T. Holterbach, S. Vissicchio, A. Dainotti, and L. Vanbever, "SWIFT: Predictive fast reroute," in *Proc. Conf. ACM Special Interest Group Data Commun.* New York, NY, USA: Association for Computing Machinery, Aug. 2017, p. 460, doi: 10.1145/3098822.3098856.

[36] L. M. Bertholdo, J. M. Ceron, L. Z. Granville, and R. van Rijswijk-Deij, "Forecasting the impact of IXP outages using anycast," in *Proc. TMA*, 2021.

[37] F. Mazzola, P. Marcos, and M. Barcellos, "Light, camera, actions: Characterizing the usage of IXPs' action BGP communities," in *Proc. 18th Int. Conf. Emerg. Netw. EXperiments Technol.* New York, NY, USA: Association for Computing Machinery, Nov. 2022, p. 196, doi: 10.1145/3555050.3569143.

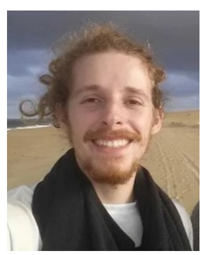
[38] (2024). *RP Portal*. [Online]. Available: http://remotepeeringportal.c3.furg.br

[39] V. Giotsas, S. Zhou, M. Luckie, and K. Claffy, "Inferring multilateral peering," in *Proc. 9th ACM Conf. Emerg. Netw. Experiments Technol.*, Dec. 2013, pp. 247–258.

[40] P. Richter, G. Smaragdakis, A. Feldmann, N. Chatzis, J. Boettger, and W. Willinger, "Peering at peerings: On the role of IXP route servers," in *Proc. Conf. Internet Meas. Conf.*, Nov. 2014, pp. 31–44.

[41] T. Krenc, R. Beverly, and G. Smaragdakis, "AS-level BGP community usage classification," in *Proc. 21st ACM Internet Meas. Conf.*, Nov. 2021, pp. 577–592.

Fabricio Mazzola received the B.S. degree in computer science and the Ph.D. degree from UFRGS, in 2019 and 2023, respectively. His research interests include internet measurements, internet routing, networking, and distributed systems.



Augusto Setti received the B.S. degree in computer science from FURG in 2023. His research interests include internet measurements, internet routing, networking, and distributed systems.

Pedro Marcos is currently an Assistant Professor with the Federal University of Rio Grande (FURG), Brazil. His research interests include the internet interconnection and routing aspects, focusing on measuring the interactions between the different entities that compose the internet and extracting valuable information to improve internet operations. His research has been funded by LACNIC through FRIDA Program and LACNIC Applied Research Program, and by FAPESP/MCTI/MCom/CGI.br.

Marinho Barcellos has been with the University of Waikato, New Zealand, since 2019. Before, he was an Associate Professor with UFRGS, Brazil. He has contributed with research in topics, including network security, internet measurements, and programmable data planes. He was the Program Chair of ACM CoNEXT 2022, the General Chair of ACM SIGCOMM 2016, and a member of the SIGCOMM Executive Committee 2017–2021. He is currently the Chair of the Advisory Board of PACMNET and the SIGCOMM CARES Committee.