Mapping Peering Interconnections to a Facility

Vasileios Giotsas
CAIDA / UC San Diego
vgiotsas@caida.org

Georgios Smaragdakis
MIT / TU Berlin
gsmaragd@csail.mit.edu

Bradley Huffaker
CAIDA / UC San Diego
bhuffake@caida.org

Matthew Luckie
University of Waikato
mjl@wand.net.nz

kc claffy
CAIDA / UC San Diego
kc@caida.org

ABSTRACT

Annotating Internet interconnections with robust physical coordinates at the level of a building facilitates network management including interdomain troubleshooting, but also has practical value for helping to locate points of attacks, congestion, or instability on the Internet. But, like most other aspects of Internet interconnection, its geophysical locus is generally not public; the facility used for a given link must be inferred to construct a macroscopic map of peering. We develop a methodology, called *constrained facility search*, to infer the *physical interconnection facility* where an interconnection occurs among all possible candidates. We rely on publicly available data about the presence of networks at different facilities, and execute traceroute measurements from more than 8,500 available measurement servers scattered around the world to identify the technical approach used to establish an interconnection. A key insight of our method is that inference of the technical approach for an interconnection sufficiently constrains the number of candidate facilities such that it is often possible to identify the specific facility where a given interconnection occurs. Validation via private communication with operators confirms the accuracy of our method, which outperforms heuristics based on naming schemes and IP geolocation. Our study also reveals the multiple roles that routers play at interconnection facilities; in many cases the same router implements both private interconnections and public peerings, in some cases via multiple Internet exchange points. Our study also sheds light on peering engineering strategies used by different types of networks around the globe.

CoNEXT '15 December 01-04, 2015, Heidelberg, Germany
 ISBN 978-1-4503-3412-9/15/12…$15.00
DOI: 10.1145/2716281.2836122

CCS Concepts

•**Networks** → **Network measurement;** *Physical topologies;*

Keywords

Interconnections; peering facilities; Internet mapping

1. INTRODUCTION

Measuring and modeling the Internet topology at the logical layer of network interconnection, i. e., autonomous systems (AS) peering, has been an active area for nearly two decades. While AS-level mapping has been an important step to understanding the uncoordinated formation and resulting structure of the Internet, it abstracts a much richer Internet connectivity map. For example, two networks may interconnect at multiple physical locations around the globe, or even at multiple locations in the same city [58, 52].

There is currently no comprehensive mapping of interconnections to physical locations where they occur [63]. There are good reasons for the dearth of this information: evolving complexity and scale of networking infrastructure, information hiding properties of the routing system (BGP), security and commercial sensitivities, and lack of incentives to gather or share data. But this opacity of the Internet infrastructure hinders research and development efforts as well as network management. For example, annotating peering interconnections with robust physical coordinates at the level of a building facilitates network troubleshooting and diagnosing attacks [45] and congestion [48]. Knowledge of geophysical locations of interconnections also enables assessment of the resilience of interconnections in the event of natural disasters [56, 22], facility or router outages [7], peering disputes [48], and denial of service attacks [24, 62]. This information can also elucidate the role of emerging entities, e. g., colocation facilities, carrier hotels, and Internet exchange points (IXP), that enable today's richly interconnected ecosystem [46, 8, 20, 21, 16]. It also increases traffic flow transparency, e. g., to identify unwanted transit paths through specific

countries, and inform peering decisions in a competitive interconnection market.

In this paper we describe a measurement and inference methodology to map a given interconnection to a physical facility. We first create and update a detailed map of interconnection facilities and the networks present at them. This map requires manual assembly, but fortunately the information is increasingly publicly available in recent years, partly due to the fact that many networks require it be available in order to establish peering [4], and many IXPs publish information about which networks are present at which of their facilities in order to attract participating networks [20]. Interconnection facilities also increasingly make the list of participant members available on their website or in PeeringDB [47]. While it is a substantial investment of time to keep such a list current, we find it is feasible.

However, a well-maintained mapping of networks to facilities does not guarantee the ability to accurately map all interconnections involving two ASes to specific physical facilities, since many networks peer at multiple locations even within a city. Mapping a single interconnection to a facility is a search problem with a potentially large solution space; however, additional constraints can narrow the search. The contributions of this work are as follows:

- We introduce and apply a measurement methodology, called *constrained facility search*, which infers the physical facilities where two ASes interconnect from among all (sometimes dozens of) possible candidates, and also infers the interconnection method, e.g. public peering at an IXP, private peering via cross-connect, point-to-point connection tunnelled over an IXP, or remote peering.

- We validate the accuracy of our methodology using direct feedback, BGP communities, DNS records, and IXP websites, and find our algorithm achieves at least 90% accuracy for each type of interconnection and outperforms heuristics based on naming schemes and IP geolocation.

- We demonstrate our methodology using case studies of a diverse set of interconnections involving content providers (Google, Akamai, Yahoo, Limelight, and Cloudflare) as well as transit providers (Level3, Cogent, Deutsche Telekom, Telia, and NTT). Our study reveals the multiple roles that routers play at interconnection facilities; frequently the same router implements both public and private peering in some cases via multiple facilities.

2. BACKGROUND AND TERMINOLOGY

Interconnection is a collection of business practices and technical mechanisms that allows individually managed networks (ASes) to exchange traffic [12]. The two primary forms of interconnection are *transit*, when one AS sells another ISP access to the global Internet, and *peering*, when two ISPs interconnect to exchange customer traffic, although complicated relationships exist [30, 33]. Whether and how to interconnect requires careful consideration, and depends on traffic volume exchanged between the networks, their customer demographics, peering and security policies, and the cost to maintain the interconnection [53].

Interconnection Facility. An *interconnection facility* is a physical location (a building or part of one) that supports interconnection of networks. These facilities lease customers secure space to locate and operate network equipment. They also provide power, cooling, fire protection, dedicated cabling to support different types of network connection, and in many cases administrative support. Large companies such as Equinix [29], Telehouse [61], and Interxion [38] operate such facilities around the globe. Smaller companies operate interconnection facilities in a geographic region or a city. Most interconnection facilities are carrier-neutral, although some are operated by carriers, e. g., Level3. In large communication hubs, such as in large cities, an interconnection facility operator may operate multiple facilities in the same city, and connect them, so that networks participating at one facility can access networks at another facility in the same city.

Internet Exchange Point. An Internet Exchange Point (IXP) is a physical infrastructure composed of layer-2 Ethernet switches where participating networks can interconnect their routers using the *switch fabric*. At every IXP there is one or more (for redundancy) high-end switches called *core switches* (the center switch in Figure 1). IXPs partner with interconnection facilities in the city they operate and install *access switches* there (switches at facilities 1 and 2 in Figure 1). These switches connect via high bandwidth connections to the core switches. In order to scale, some IXPs connect multiple access switches to back-haul switches. The back-haul switch then connects to the core switch. All IXP members connected to the same access switch or back-haul switch exchange traffic locally if they peer; the rest exchange traffic via the core switch. Thus, routers owned by members of IXPs may be located at different facilities associated with the same IXP [20].

Popular peering engineering options today are:

Private Peering with Cross-connect. A cross-connect is a piece of circuit-switched network equipment that physically connects the interfaces of two networks at the interconnection facility. It can be either copper or fiber with data speeds up to tens of Gbps. Cross-connects can be established between members that host their network equipment in different facilities of the same interconnection facility operator, if these facilities are interconnected. The downside of a cross-connect is operational overhead: it is largely a manual process to establish, update, or replace one.

Some large facilities have thousands of cross-connects, e. g., Equinix reported 161.7K cross-connects across all its colocation facilities, with more than half in the Amer-

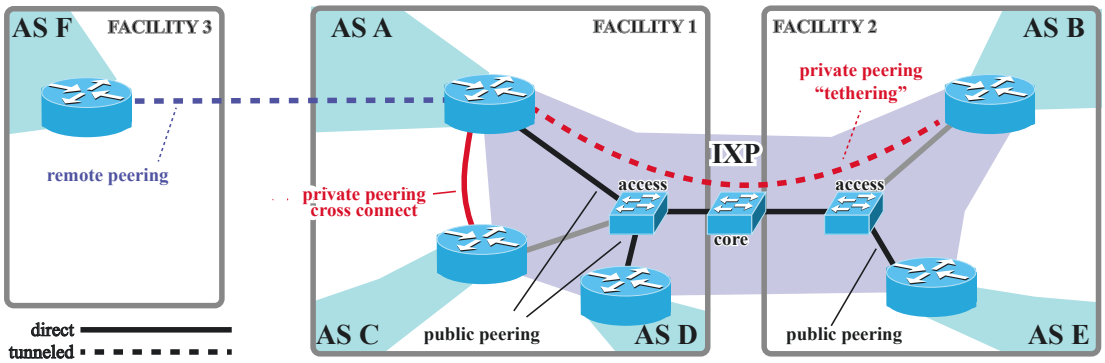

Figure 1: Interconnection facilities host routers of many different networks and partner with IXPs to support different types of interconnection, including cross-connects (private peering with dedicated medium), public peering (peering established over shared switching fabric), tethering (private peering using VLAN on shared switching fabric), and remote peering (transport to IXP provided by reseller).

icas (Q2 2015) [3]. Cross-connects are physically installed by interconnection facility operators. But IXPs can leverage their large membership to purchase at wholesale prices a large number of cross-connects at partnered interconnection facilities; members then purchase these cross-connects directly from the IXPs. For example, the IXP DE-CIX has facilitated more than 900 cross-connects across its partnered facilities in Frankfurt as of February 2015 [2].

Public Peering. Public peering, also referred to as public interconnect, is the establishment of peering connections between two members of an IXP via the IXP's switch fabric. IXPs are allocated IP prefix(es) and often an AS number by a Regional Internet Registry. The IXP assigns an IP from this range to the IXP-facing router interfaces of its IXP members to enable peering over its switch fabric [11]. One way to establish connectivity between two ASes is to establish a direct BGP session between two of their respective border routers. Thus, if two IXP member ASes wanted to exchange traffic via the IXP's switching fabric, they establish a *bi-lateral* BGP peering session at the IXP. An increasing number of IXPs offer their members the use of route server to establish *multi-lateral* peering to simplify public peering [34, 57]. With multi-lateral peering an IXP member establishes a single BGP session to the IXP's route server and receives routes from other participants using the route server. The advantage of public peering is that by leasing one IXP port it is possible to exchange traffic with potentially a large fraction of the IXP members [60].

Private Interconnects over IXP. An increasing number of IXPs offer private interconnects over their public switch fabric. This type of private peering is also called *tethering* or IXP metro VLAN. With tethering, a point-to-point virtual private line is established via the already leased port to reach other members of the IXP via a virtual local area network (VLAN), e. g., IEEE 802.1Q. Typically there is a setup cost. In some cases this type of private interconnect enables members of an IXP to privately reach networks located in other facilities where those members are not present, e. g., transit providers or customers, or to privately connect their infrastructure across many facilities.

Remote Peering. Primarily larger IXPs, but also some smaller ones, have agreements with partners, e. g., transport networks, to allow *remote peering* [15]. In this case, the router of the remote peer can be located anywhere in the world and connects to the IXP via an Ethernet-over-MPLS connection. An advantage of remote peering is that it does not require maintaining network equipment at the remote interconnection facilities. Approximately 20% (and growing) of AMS-IX participants were connected this way [20] in 2013. Remote peering is also possible between a remote router at the PoP of an ISP and a router present at an interconnection facility.

3. DATASETS AND MEASUREMENTS

To infer details of a given interconnection, we need information about the prefixes of the two networks and physical facilities where they are present. This section describes the publicly available data that we collected and analyzed for this study, and the publicly available measurement servers (vantage points) we utilized.

3.1 Data Sources

3.1.1 Facility Information

For a given network we developed (and continue to maintain to keep current) a list of the interconnection facilities where it is present. Despite the fact that facilities for commercial usage must be known to the network operators to facilitate the establishment of new peering links and to attract new customers, and in some cases it is required to be public (e. g., for facilities that partner with IXPs in Europe), the information is not available in one form.

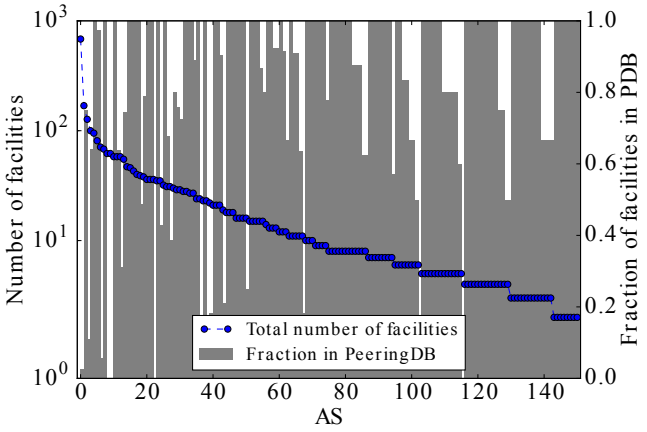

Figure 2: Number of interconnection facilities for 152 ASes extracted from their official website, and the associated fraction of facilities that appear in PeeringDB.

We started by compiling an AS-to-facilities mapping using the list of interconnection facilities and associated networks (ASNs) available in PeeringDB [47]. Although this list is maintained on a volunteer basis (operators contribute information for their own networks), and may not be regularly updated for some networks, it is the most widely used source of peering information among operators, and it allows us to bootstrap our algorithms. Due to its manual compilation process, there are cases where different naming schemes are used for the same city or country. To remove such discrepancies, we convert country and city names to standard ISO and UN names. If the distance between two cities is less than 5 miles, we map them to the same metropolitan area. We calculate the distance by translating the postcodes of the facilities to geographical coordinates. For example, we group Jersey City and New York City into the NYC metropolitan area.

To augment the list of collected facilities, we extracted colocation information from web pages of Network Operating Centers (NOCs), where AS operators often document their peering interconnection facilities. Extracting information from these individual websites is a tedious process, so we did so only for the subset of networks that we encountered in our traceroutes and for a network's PeeringDB data did not seem to reflect the geographic scope reported on the network's own web site. For example, we investigated cases where a NOC web site identified a given AS as global but PeeringDB listed facilities for that AS only in a single country.

Figure 2 summarizes the additional information obtained from NOC websites. The gray bars show the fraction of facilities found in PeeringDB. We checked 152 ASes with PeeringDB records, and found that PeeringDB misses 1,424 AS-to-facility links for 61 ASes; for 4 of these ASes PeeringDB did not list any facility. Interestingly, the ASes with missing PeeringDB information provided detailed data on their NOC websites, i.e., they were not intending to hide their presence.

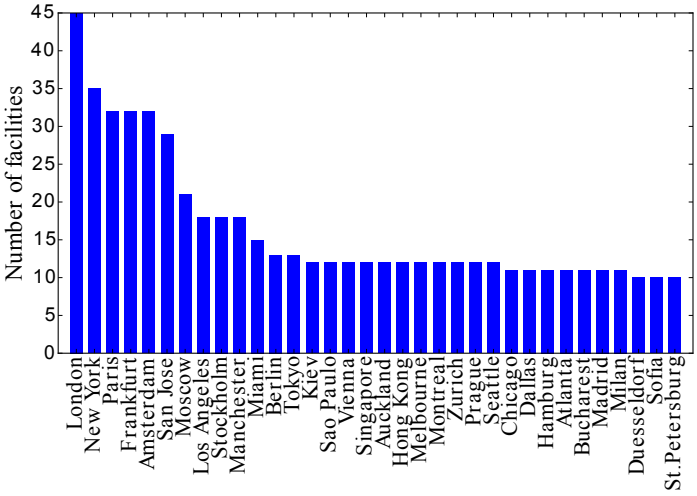

Figure 3: Metropolitan areas with at least 10 interconnection facilities.

3.1.2 IXP Information

We use various publicly available sources to get an up-to-date list of IXPs, their prefixes, and associated interconnection facilities. This information is largely available from IXP websites. We also use lists from PeeringDB and Packet Clearing House (PCH). Useful lists are provided by regional consortia of IXPs such as Euro-IX (also lists IXPs in North America), Af-IX, LAC-IX, and APIX that maintain databases for the affiliated IXPs and their members. Some IXPs may be inactive; PCH regularly updates their list and annotates inactive IXPs. To further filter out inactive IXPs, for our study, we consider only IXPs that (i) we were able to confirm the IXP IP address blocks from at least three of these data sources, and (ii) we could associate at least one active member from at least two of the above data sources. We ended up with 368 IXPs in 263 cities in 87 countries. IXPs belonging to the same operators in different cities may be different entries, e. g., DE-CIX Frankfurt and DE-CIX Munich.

We then create a list of IXPs where a network is a member, and annotate which facilities partner with these exchange points. For private facilities, we use PeeringDB data augmented with information available at the IXP websites and databases of the IXP consortia. We again encountered cases where missing IXP information from PeeringDB was found on IXP websites. For example, the PeeringDB record of the JPNAP Tokyo I exchange does not list any partner colocation facilities, while the JPNAP website lists two facilities [5]. Overall, we extracted additional data from IXP websites for 20 IXPs that we encountered in traces but for which PeeringDB did not list any interconnection facilities. PeeringDB was not missing the records of the facilities, only their association with the IXPs.

By combining all the information we collected for facilities, we compiled a list of 1,694 facilities in 95 countries and 684 cities for April 2015. The regional distribution of these facilities is as follows: 503 in North

America, 860 in Europe, 143 in Asia, 84 in Oceania, 73 in South America, and 31 in Africa. Notice that these facilities can be operated by colocation operators or by carriers. Figure 3 shows the cities with at least 10 colocation facilities. It is evident that for large metropolitan areas the problem of pinpointing a router's PoP at the granularity of interconnection facility is considerably more challenging than determining PoP locations at a city-level granularity.

On average a metropolitan area has about 3 times more interconnection facilities than it has IXPs, because an IXP's infrastructure may span multiple facilities in a city, or even multiple cities, for redundancy and expanded geographical coverage. For example, the topology of DE-CIX in Frankfurt spans 18 interconnection facilities. ASes tend to connect to more interconnection facilities than to IXPs, with 54% of the ASes in our dataset connected to more than one IXPs and 66% of the ASes connected at more than one interconnection facilities, which is consistent with the fact that connectivity to an IXP requires presence at one or more facility that partners with the IXP. However, we observe the opposite behavior for a relatively small number of ASes that use fewer than 10 interconnection facilities. This behavior is consistent with two aspects of the peering ecosystem: (i) an interconnection facility may partner with multiple IXPs, so presence at one facility could allow connectivity to multiple IXPs, and (ii) remote peering allows connectivity to an IXP through an IXP port reseller, in which case presence at an IXP does not necessarily require physical presence at one of its partner facilities. For instance, about 20% of all AMS-IX participants connect remotely [20].

3.2 Vantage Points and Measurements

To perform targeted traceroute campaigns we used publicly available traceroute servers, RIPE Atlas, and looking glasses. We augmented our study with existing daily measurements, from iPlane and CAIDA's Archipelago infrastructures, that in some cases had already traversed interconnections we considered. Table 1 summarizes characteristics of our vantage points.

RIPE Atlas. RIPE Atlas is an open distributed Internet measurement platform that relies on measurement devices connected directly to home routers, and a smaller set of powerful measurement collectors (anchors) used for heavy measurements and synchronization of the distributed measurement infrastructure. The end-host devices can be scheduled to perform traceroute, ping, and DNS resolution on the host. We employed ICMP Paris (supported by RIPE Atlas) traceroute to mitigate traceroute artifacts caused by load balancing [10]. We also used existing public measurements gathered in May 2015 by RIPE Atlas nodes (e. g., periodic traceroute queries to Google from all Atlas nodes).

Looking Glasses. A looking glass provides a web-based or telnet interface to a router and allows the execution of non-privileged debugging commands. In many cases a looking glass provides access to routers in different cities, as well multiple sites at the same city. Many looking glasses are also colocated with IXPs. Often looking glass operators enforce probing limitations through mandatory timeouts or by blocking users who exceed the operator-supported probing rate. Therefore, looking glasses are appropriate only for targeted queries and not for scanning a large range of addresses. To conform to the probing rate limits, we used a timeout of 60 seconds between each query to the same looking glass.

	RIPE Atlas	LGs	iPlane	Ark	Total unique
Vantage Pts.	6385	1877	147	107	8517
ASNs	2410	438	117	71	2638
Countries	160	79	35	41	170

Table 1: Characteristics of the four traceroute measurement platforms we utilized.

We extracted publicly available and traceroute-capable looking glasses from PeeringDB, *traceroute.org* [41], and previous studies [43]. After filtering out inactive or otherwise unavailable looking glasses, we ended up with 1877 looking glasses in 438 ASes and 472 cities including many in members of IXPs and 21 offered by IXPs. An increasing number of networks run public looking glass servers capable of issuing BGP queries [34], e. g., "show ip bgp summary", "prefix info", "neighbor info". We identified 168 that support such queries and we used them to augment our measurements. These types of looking glasses allow us to list the BGP sessions established with the router running the looking glass, and indicate the ASN and IP address of the peering router, as well as showing metainformation about the interconnection, e. g., via BGP communities [33].

iPlane. The iPlane project [50] performs daily IPv4 traceroute campaigns from around 300 PlanetLab nodes. iPlane employs Paris traceroute to target other PlanetLab nodes and a random fraction of the advertised address space. We used two daily archives of traceroute measurements, collected a week apart, from all the active nodes at the time of our measurements.

CAIDA Archipelago (Ark). CAIDA maintains Ark, a globally distributed measurement platform with 107 nodes deployed in 92 cities (as of May 2015 when we gathered the data). These monitors are divided into three teams, each of which performs Paris traceroutes to a randomly selected IP address in every announced /24 network in the advertised address space in about 2-3 days. We analyzed one dataset collected when we performed the traceroute campaigns with RIPE Atlas and the looking glasses.

Targeted traceroutes. It takes about 5 minutes for a full traceroute campaign using more than 95% of all active RIPE Atlas nodes for one target. The time required by each looking glass to complete a traceroute measurement to a single target depends on the number of locations provided by each looking glass. The largest

looking glass in our list has 120 locations. Since we wait 60 seconds between queries, the maximum completion time is about 180 minutes, assuming that a traceroute takes about 30 seconds to complete.

4. METHODOLOGY

Next we describe the technique we designed and implemented to infer the location of an interconnection. Figure 4 depicts the overall methodology and datasets used at each step of the inference process. For our experiment, all traceroute measurements we used were collected in May 2015.

4.1 Preparation of traceroute data

Interconnections occur at the network layer when two networks agree to peer and exchange traffic. To capture these interconnections, we performed a campaign of IPv4 traceroute measurements from RIPE Atlas and looking glass vantage points, targeting a set of various networks that include major content providers and Tier-1 networks (see section 5). We augmented this data with other traceroute measurements performed by iPlane and CAIDA Ark, and when relevant from RIPE Atlas archived measurements (Table 1).

We first mapped each IP router interface to an ASN using Team Cymru's IP-to-ASN service [23], which utilizes multiple BGP sources to construct this mapping. Mapping IP addresses to ASNs based on longest prefix matching is prone to errors caused by IP address sharing between siblings or neighboring ASes [65]. Such errors can reduce the accuracy of our methodology since they can lead to inference of incorrect candidate facilities for an IP interface. To reduce common errors, we detected potentially erroneous IP to ASN mappings by performing alias resolution to group IP interfaces into routers. We resolved 25,756 peering interfaces and found 2,895 alias sets containing 10,952 addresses, and 240 alias sets that included 1,138 interfaces with conflicting IP to ASN mapping. We mapped alias sets with conflicting IP interfaces to the ASN to which the majority of interfaces are mapped, as proposed in [18].

We used the MIDAR system [42] to infer which aliases belong to the same router. MIDAR uses the monotonic bounds test on a sequence of collected IP-ID values to infer which IP addresses are aliases, and has been shown to produce very few false positives. However, some routers were unresponsive to alias resolution probes (e. g., Google) or sent constant or random IP-ID values, so false negatives are possible. Alias resolution improved the accuracy of our IP-to-ASN mappings, but more importantly provided additional constraints for mapping interfaces to facilities.

4.2 Constrained Facility Search

At the end of the previous step we obtained three representations of the routing paths between the vantage points and our targets: the IP-level paths as well as the corresponding router-level and AS-level abstractions. We combine this topology data with the mapping of ASes and IXPs to facilities that we constructed in section 3.1.1. We use the combined data to infer the location of the targeted peering interconnections as follows. We progressively constrain the possible facilities where an IP interface is located, through a process of triangulation similar to those used in RTT-based geolocation [35, 39], but instead of delay data we rely on facility information data. Figure 4 provides an overview of the Constrained Facility Search (CFS) algorithm. We use the notation in table 2 to describe this algorithm.

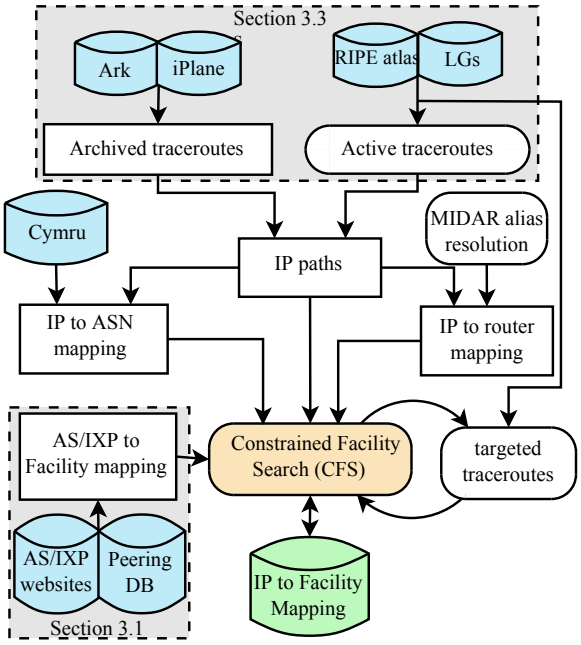

Figure 4: Overview of our interconnection-to-facility mapping process. Using a large set of traceroutes toward the target ASes, we first resolve IP addresses to routers [42], and map IP addresses to ASes [23]. We feed this data, along with a constructed list of interconnection facilities for each AS and IXP, to our *Constrained Facility Search (CFS)* algorithm. The CFS algorithm iteratively constrains the possible interconnection facilities for inferred peerings, using targeted traceroutes as necessary to narrow the possible facilities for a router until it converges.

Step 1: Identifying public and private peering interconnections. Consider the case where we want to infer the facilities where peers of AS B interconnect. We start by searching recently collected traceroute data for peering interconnections involving B. If we find such an interconnection, we then identify the peering interface of the neighbor AS involved in the interconnection and whether the peering is public or private, using the following technique.

If we observe a sequence of IP hops (IP_A, IP_e, IP_B), in a traceroute path, we check if interface IP_e belongs to the address space of an IXP that is used for public

Notation	Meaning
IP_x^i	The ith IP interface that is mapped to ASN x.
(IP_x, IP_y, IP_z)	Sequence of IP hops in a traceroute path.
$\{F_A\}$	The set of interconnection facilities where ASN A is present.
$IP_x \rightarrow \{f_1, f_2\}$	The IP interface IP_x is mapped to either facility f_1 or facility f_2

Table 2: Notation used in Constrained Facility Search.

peering, assembled as explained in section 3.1.2. If IP_e belongs to IXP address space, we infer that the peering link (A, B) is public and is established over the IXP that owns IP_e [11]. If IP_e is an unresolved (no mapping to AS) or an unresponsive interface, we discard the path. If we observe a sequence of IP hops (IP_A, IP_B), then we infer that the peering interconnection (A, B) is private, since there is no intermediate network between AS A and AS B. This peering interconnection can be either cross-connect, tethering, or remote.

Step 2: Initial facility search. After we determine the public and private peering interconnections, we calculate the possible locations where each interconnection could be established. This step allows us to create an initial set of candidate locations for each peering interface, and helps us to distinguish cross-connects from remote peering and tethering. For a public peering (IP_A, IP_{IXP}, IP_B) we compare the set of facilities $\{F_A\}$ where AS A has presence with the IXP's set of interconnection facilities $\{F_E\}$. Note that we can compare the facilities between AS A and IXP, but not the facilities between IXP and AS B, because typically the traceroute response returns from the ingress interface and therefore the interface of AS B at the IXP is not visible in the traceroute paths. From this comparison we have three possible outcomes regarding the resolution of an IP interface to facility:

1. *Resolved interface:* If AS A has only one common facility with the IXP, we infer that AS A is not remotely interconnected to the IXP, and that its interface IP_A is located in the common facility.

2. *Unresolved local interface:* If AS A has multiple common facilities with the IXP, then we infer that AS A is not remotely interconnected to the IXP, and that its interface IP_A is located in one of the common facilities, i. e., $IP_A \rightarrow \{\{F_A\} \cap \{F_E\}\}$.

3. If AS A has no common facility with the IXP, then we have two possibilities: (a) *Unresolved remote interface:* AS A is remotely connected to the IXP through a remote peering reseller. For these interfaces the set of possible facilities includes all facilities where AS A is present, i. e., $IP_A \rightarrow \{F_A\}$. (b) Missing data: We have incomplete facility data about AS A or about the IXP that prevents inference of the location of the interconnection.

We use the methodology developed in [15] to infer remote peering. We use multiple measurements taken at different times of the day to avoid temporarily elevated RTT values due to congestion.

We perform a similar process for private peering interconnections (IP_A, IP_B), but this time we calculate the common facilities between private peers AS A and AS B. Again, there are three possible outcomes: (1) a single common facility in which we infer IP_A to be located, (2) multiple common facilities where IP_A may be located, or (3) no common facilities, meaning that the interconnection is remote private peering or tethering, or we have missing data.

Step 3: Constraining facilities through alias resolution. Identifying the facility of an interface means that all aliases of that interface should be located in the same facility. This observation allows us to further constrain the set of candidate facilities for unresolved interfaces in the previous step (*unresolved local* or *remote*). Even if none of a router's aliases were resolved in the previous step to a single router, it is possible that by cross-checking the candidate facilities of the aliases we will converge to a single facility for all of the aliases. For example, consider two unresolved interfaces IP_A^1 and IP_A^2, with $IP_A^1 \rightarrow \{f_1, f_2\}$ and $IP_A^2 \rightarrow \{f_2, f_3\}$. Since IP_A^1 and IP_A^2 are aliases, it means that they can only be located at the common facilities, hence we infer that both aliases are located in facility f_2.

Step 4: Narrowing the set of facilities through follow-up targeted traceroutes. For the remaining unresolved interfaces, we perform additional traceroute measurements in order to further constrain the set of possible facilities [13]. For an unresolved interface, our goal is to find different peering connections involving the interface that reduce the set of possible candidate facilities. We carefully select targets of these traceroutes to increase the likelihood of discovering additional constraints. Selection of targets depends on the type of unresolved interface, and the already inferred possible facilities, both of which we determined in Step 2.

For an *unresolved local* peering interface IP_A^x we target other ASes whose facilities overlap with at least one candidate facility of IP_A^x. The candidate facilities of IP_A^x must be a superset of the target's facilities, otherwise, comparison of the common facilities between A and the target will not further constrain the possible facilities for IP_A^x. We select as follow-up traceroute targets IP addresses in ASes with $\{F_{target}\} \subset \{F_A\}$, and we launch follow-up traceroutes starting from the target with the smallest facility overlap. The resulting traceroute will contribute constraints only if it does not cross the same IXP against which we compared the facilities of A in Step 1. Therefore, we need to find paths that cross private peering interconnections or previously unseen IXPs, which means that we prioritize targets that are not colocated in the already queried IXP.

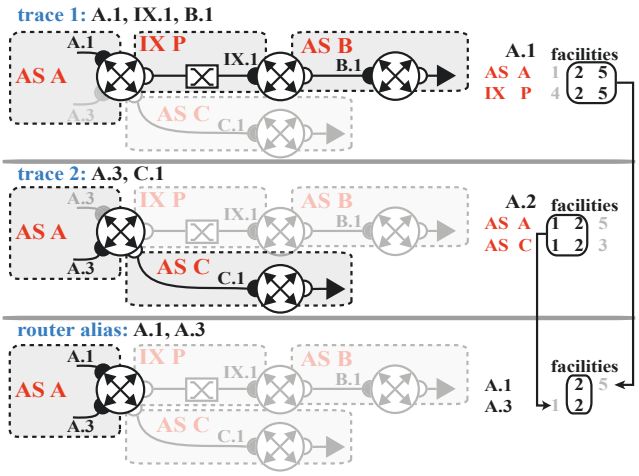

Figure 5: Toy example of how we use Constrained Facility Search (CFS) method to infer the facility of a router by probing the interconnection between peers with known lists of colocation facilities (described in detail at end of Section 4.2).

An *unresolved remote* interface IP_A^y occurs when Step 1 does not provide any constraints, meaning that the possible facilities for IP_A^y are the entire set of facilities where A is present. In this case, we intend the targeted traceroutes to find local peering interconnections (public or private) that involve the router of IP_A^y. Again, we begin the measurements from the ASes with the smallest possible non-empty overlap of facilities.

After we launch the additional targeted traceroute measurements, we repeat Steps 2 to 4 until each interface converges to a single facility, or until a timeout set for searching expires. To illustrate the execution of our algorithm consider the example in Figure 5. Using *trace* 1 and by comparing the common facilities between AS A and IXP we find that the interface $A.1$ is located in Facility 2 or Facility 5. Similarly, using *trace* 2 and by comparing the common facilities between AS A and AS B we find that the interface $A.3$ is located in Facility 1 or Facility 2. To further narrow the potential facilities where the interfaces $A.1$ and $A.3$ are located, we de-alias the collected interfaces and map the resulting router to the intersection of the candidate facilities for each interface. At the end of this process we infer that the interfaces $A.1$ and $A.3$ are located in facility 2.

4.3 Facility search in the reverse direction

So far we have located the peering interconnections from the side of the peer AS that appears first in the outgoing direction of the traceroute probes. In some cases, due to the engineering approach to interconnection (i. e., private cross-connect), we expect that the second peer (the other side of the interconnection) is in the same facility or building. Furthermore, in many cases of public peering interconnections over IXPs, the unresolved peer is connected to only a single IXP facility.

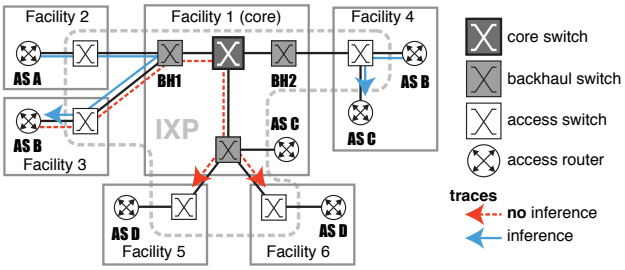

Figure 6: Toy example to illustrate the execution of the Switch Proximity Heuristic (Section 4.4) to infer the interconnection facility of the peer at the far end of an IXP peering link when the peer is connected in more than one IXP facility.

However, in remote peering, tethering, and public peering at IXPs, where the second peer is connected at multiple facilities, the two peers may be located at different facilities. For example, in Figure 5 the CFS algorithm will infer the facility of A.1's router but not the facility of IX.1's router. This outcome arises because traceroute replies typically return from the ingress, black, interface of a router and therefore do not reveal the router's egress, white, interfaces.

To improve our visibility, we repeat Steps 1–4 on the reverse paths, if we have a monitor at the side of the second peer. But in many cases we do not have such a monitor, and obtaining reverse paths using the record route option and correlating traceroutes [40] is not a general solution, and in particular cannot be applied to interconnections with several popular content providers who do not support that option. To improve visibility of the far end interface, we apply the following heuristic.

4.4 Proximity Heuristic

As a fallback method to pinpoint the facility of the far end interface, we use knowledge of common IXP practices with respect to the location and hierarchy of switches. We confirmed with operators via private communication that networks connected to the same switch, or connected to switches attached with the same backhaul switch, exchange traffic locally and not via the core switch. For example, consider the toy IXP setup of Figure 6, over which AS A establishes a public peering with AS B. AS A will send its traffic to the router of AS B in Facility 3 instead of Facility 4, because Facilities 2 and 3 are connected to the same backhaul switch (BH1), while Facilities 2 and 4 would exchange traffic over the Core switch. Consequently, we develop the *switch proximity* heuristic. For a public peering link $(IP_A, IP_{IXP,B}, IP_B)$ for which we have already inferred the facility of IP_A, and for which IP_B has more than one candidate IXP facility, we require that IP_B is located in the facility proximate to IP_A.

Because a detailed switch topology of an IXP is not always available, we infer the proximity of the IXP fa-

cilities through probabilistic ranking based on the IP-to-facility mapping performed in previous steps. More specifically, for each IXP facility that appears at the near end of a public peering link (e.g. the facility of A_1 in Figure 5), we count how often it traverses a certain IXP facility at the far end (the facility of B_1 in Figure 5) whenever the far end has more than one candidate facility, and we rank the proximity of IXP facilities using this metric. Based on the inferred proximities we then try to determine the facilities of public peering links for which we do not have traceroute paths from the reverse direction. If we have pinpointed the facility of the near-end peering router, we require that the far-end router will be located in the most proximate facility to the near-end router.

We validated inferences from the *switch proximity* heuristic against ground-truth data from AMS-IX [1], which publishes the interfaces of connected members and corresponding facilities of those interfaces. We executed an additional traceroute campaign from 50 AMS-IX members who are each connected to a single facility of AMS-IX, targeting a different set of 50 AMS-IX members who are each connected to two facilities. We found that in 77% of the cases the *switch proximity* heuristic finds the exact facility for each IXP interface. When it fails, the actual facility is in close proximity to the inferred one (e. g., both facilities are in the same building block), which is because (per the AMS-IX web site) the access switches are connected to the same backhaul switch. Moreover, the heuristic cannot make inferences when the potential facilities are connected to the same backhaul or core switch. For example, for traffic between AS B and AS D in Figure 6, we cannot infer the facility of AS D because both facilities of AS D have the same proximity to the facilities of AS B.

5. RESULTS

To evaluate the feasibility of our methodology, we first launched an IPv4 traceroute campaign from different measurement platforms targeting a number of important groups of interconnections, and tried to infer their locations. We considered a number of popular content providers whose aggregated traffic is responsible for over half the traffic volume in North America and Europe by some accounts [32, 54]: Google (AS15169), Yahoo! (AS10310), Akamai (AS20940), Limelight (AS22822) and Cloudflare (AS13335). For these networks we maintain a list of their IP prefixes via their BGP announcements (in some cases a content provider uses more than one ASN) as well as whitelists that they publish to avoid blocking by firewalls [19] or whitelists provided by previous studies [14]. We also collected a list of URLs served by these networks [9]; we converted the domain names to IPs which became candidate traceroute targets. We prioritized traceroutes to IP addresses that were on the list from ZMap [28] and also ICMP-reachable, followed by addresses not on the Zmap list but ICMP-reachable.

Second, we considered four large transit providers (the main ASN that they use to peer is in parenthesis) with global footprints: NTT (AS2914), Cogent (AS174), and Deutsche Telekom (AS3320), Level3 (AS3356) and Telia (AS1299). We collected the list of all their peers from [49], and augmented this list with the names of PoPs available on the networks' web sites. We selected one active IP per prefix for each peer.

In total we were able to map 9,812 router interfaces to a single interconnection facility, after completing 100 iterations of CFS.[1] Figure 7 shows that over 70% of interfaces resolve to a facility after 100 iterations of the CFS algorithm when using all of our available datasets.

At the end of the first iteration, the CFS algorithm obtains the interface-to-facility resolutions that correspond to peering ASes with only a single common facility. Most remote peering interconnections are resolved in step 2, as a result of CFS changing the traceroute target to facilities that are local to the remote peer. In our experiment, about 40% of observed interfaces were resolved after the first 10 iterations of the algorithm, with diminishing returns after 40 iterations (Figure 7). We defined the timeout at 100 rounds, after which we managed to pinpoint 70.65% of the observed peering interfaces. For about 9% of unresolved interfaces, we constrained the location of the interface to a single city. We also studied the convergence rate when we used only a single platform for targeted measurements, either RIPE Atlas or Looking Glasses (but all of the archived data). Figure 7 shows that the CFS algorithm inferred twice as many interfaces per iteration when using RIPE Atlas than when using the Looking Glasses for targeted measurements. However, 46% of the interfaces inferred through Looking Glasses traces were not visible from the Atlas probes due to fact the that we had Looking Glass vantage points in 236 ASes that were not covered by RIPE Atlas.

To put our convergence rate into context, we tried to geolocate the collected interfaces using DRoP [36], a DNS-based geolocation technique that extracts geographical information from DNS hostnames, such as airport codes, city names, and CLLI codes. From the 13,889 peering interfaces in our traceroute data that belonged to the targeted networks, 29% had no associated DNS record, while 55% of the remaining 9,861 interfaces did not encode any geolocation information in their hostname. Ultimately, we could geolocate only 32% of the peering interfaces using DNS hostname information. Compared to DNS-based geolocation, CFS resolved about 40% more interfaces at finer-grained geolocation (facility-level instead of city-level).

For 33% of the interfaces that did not resolve to a facility, we did not have any facility information for the AS that owns the interface address. To better understand the effect of missing facility data on the fraction of resolved interfaces, we iteratively executed CFS while removing 10 facilities from our dataset in random order

[1]Each iteration of the CFS algorithm repeats steps 2–4 as explained in section 4.2.

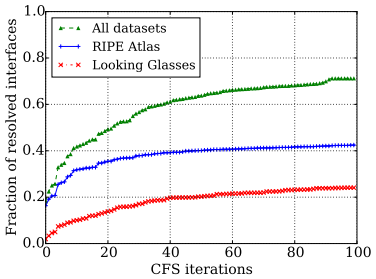

Figure 7: Fraction of resolved interfaces versus number of CFS iterations when we use all, RIPE Atlas, or LG traceroute platforms.

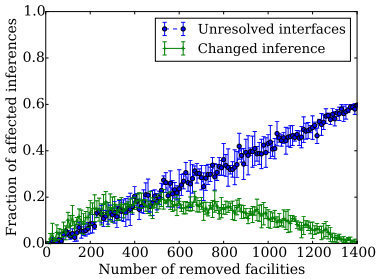

Figure 8: Average fraction of unresolved interfaces, and interfaces with changed facility inference by iteratively removing 1400 facilities.

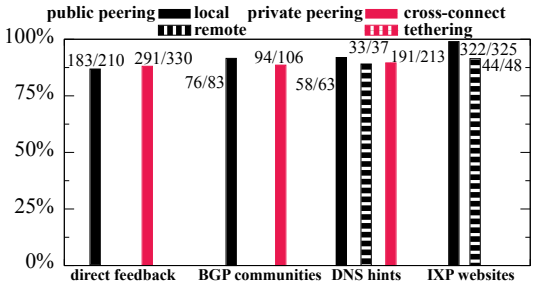

Figure 9: Fraction of ground truth locations that match inferred locations, classified by source of ground truth and type of link inferred. CFS achieves 90% accuracy overall.

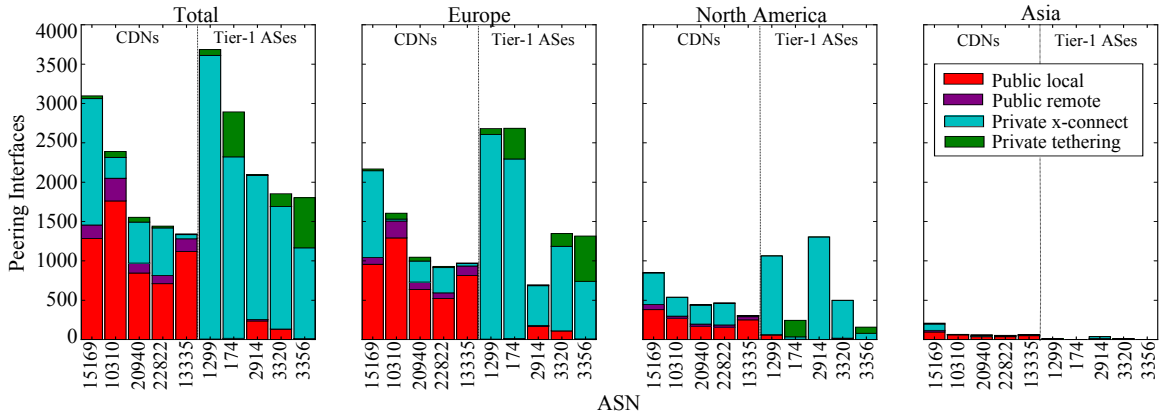

Figure 10: Number of peering interfaces inferred and distribution by peering type for a number of networks in our study around the globe and per region.

at each iteration, until we had removed 1,400 facilities. We repeated this experiment 20 times. Figure 8 shows that removing 850 facilities (50% of the total facilities in our dataset) causes on average 30% of the previously resolved interfaces to become unresolved, while when we remove 1,400 (80%) facilities 60% of the resolved interfaces become unresolved.

Incomplete data can also affect the correctness of our inferences. Missing facility information can cause the CFS algorithm to incorrectly converge to a single facility, by cross-referencing incomplete datasets. For instance, if in Figure 5 AS C is also present in Facility 5, then it is possible that the interfaces A.1 and A.2 are located in Facility 5 but the algorithm converges to Facility 2 because it does not have this information. Figure 8 shows several effects of incomplete data on our inferences of interface-to-facility mappings. First, the blue line shows that as we remove knowledge of facilities, we also reduce the number of interfaces we can map to a specific facility; the relationship is perhaps intuitively linear. Less intuitive is the non-monotonic effect of removing facility knowledge on which facility an interface maps to. Removing 500 (30% of the) facilities from our dataset caused the algorithm to place 20% of the interfaces in a different facility (changed inference), but after a certain threshold (about 500) of facility removal, the CFS algorithm has so few facilities to select from (or change to), that it cannot effectively narrow the search to converge to single a facility.

An interesting outcome of our measurements is that 39% of the observed routers implemented both public and private peering. Although we cannot generalize this finding since our traceroute campaign did not aim at exhaustive discovery of peering interconnections, the large fraction of the observed multi-role routers implies that private and public peering interconnections often rely on the same routing equipment and thus may have common points of congestion or failure. Therefore, public and private peering interconnections are more interdependent than previously believed. We also find that 11.9% of the observed routers used to implement public peering establish links over two or three IXPs. As explained in section 3.1.1, an interconnection facility can be used by more than one IXP, therefore a router can establish links with peers across all IXPs colocated at the same facility. This heterogeneity helps our algorithm resolve more interfaces to facilities, since we can use a mix of IXPs and private peering facilities to constrain the possible facilities of multi-role routers.

Figure 10 presents the total number of peering in-

terfaces per target AS in three major regions (Europe, North America, and Asia). Different peering practices affect our inferences of facility and location. For example, European IXPs tend to be more transparent than U.S. IXPs about their facility locations and interconnection relationships, which makes our mappings of European interconnections to facilities likely more complete and more accurate. The set of vantage points available will also affect the geographic coverage of CFS inferences. For example, RIPE Atlas probes have a significantly larger footprint in Europe than in Asia, allowing inference of more interfaces in Europe. The type of network also plays a role; CDNs establish most interconnections via public peering fabrics, in contrast to Tier-1 ASes (Figure 10, Total).

6. VALIDATION

Due to its low-level nature, ground truth on interconnection to facility mapping is scarce. We tried to validate our inferences as extensively as possible by combining four different sources of information:

Direct feedback: We obtained direct validation from two CDN operators we used as measurement targets. The operators offered validation only for their own interfaces but not the facilities of their peers due to lack of data. Overall, we validated 88% (474/540) of our inferences as correct at the facility level, and 95% as correct at the city level. Missing facilities from our dataset were responsible for 70% of the wrong inferences.

BGP communities: AS operators often use the BGP communities attribute [17] to tag the entry point of a route in their network. The entry point to the AS network is at the near end of the peering interconnection, for which we made facility inferences, meaning that the communities attribute is a source of validation. We compiled a dictionary of 109 community values used to annotate ingress points, defined by four large transit providers. For our validation we used only data from looking glasses that provide BGP and traceroute vantage points from the same routers, to avoid path disparities due to potential path diversity between different PoPs of an AS. We queried the BGP records of addresses that we used as destinations in our traceroute measurements, and we collected the communities values attached to the BGP routes. We correctly pinpointed 76/83 (92%) of public peering interfaces and 94/106 (89%) of cross-connect interfaces.

DNS records: Some operators encode the facility of their routers in the hostnames of the router interfaces. For example the hostname `x.y.rtr.thn.lon.z` denotes that a router is located in the facility Telehouse-North in London. We compiled a list of naming conventions that denote interconnection facilities from 7 operators in the UK and Germany, and we confirmed with them that the DNS records were current. Of the interfaces validated, we correctly pinpointed 91/100 (91%) of public peering interfaces and 191/213 (89%) of cross-connect interfaces.

IXP websites: A few IXPs list on their websites the exact facilities where and the IP interfaces with which their members are connected. We collected data from 5 large European IXPs (AMS-IX, NL-IX, LINX, France-IX and STH-IX) and compared them against our inferences. AMS-IX and France-IX also distinguished between local and remote peers. Although they provided the location of their reseller, we used the data to verify that our remote-peering inferences were correct. We correctly pinpointed 322/325 (99.1%) of public peering interfaces correctly inferred 44/48 (91.7%) of remote peers. We achieved higher accuracy for this validation subset because we collected from IXP websites complete facilities lists for the IXPs and their members.

Figure 9 shows that the CFS algorithm correctly pinpointed correctly over 90% of the interfaces. Importantly, when our inferences disagreed with the validation data, the actual facility was located in the same city as the inferred one (e. g., Telecity Amsterdam 1 instead of Telecity Amsterdam 2).

7. RELATED WORK

Several research efforts have mapped peering interconnections to specific regions using a variety of data sources. Augustin et al. [11] used traceroute measurements to infer peering interconnections established at IXPs. Dasu [59] used BitTorrent clients as vantage points to accomplish a similar mapping. Follow-up work [34] used public BGP information from IXP route servers to infer a rich set of additional peerings. These studies map interconnections to a specific city where an IXP operates. Castro et al. [15] provided a delay-based method to infer remote peerings of IXP members. Giotsas et al. [33] used BGP communities information, DNS hostname information [36], and Netacuity [6] to map interconnections at the city level. Calder et al. [14] provided novel techniques based on delay measurements to locate peerings and PoPs of a large content provider at the city level. Motamedi et al. [51] proposed a methodology that combines public BGP data, targeted traceroutes, and target BGP Looking Glass queries to to map cross-connects of all tenants in two commercial colocation facilities.

Two other methods are widely used to infer the location of an interconnection: reverse DNS lookup and IP geolocation. But DNS entries are not available for many IP addresses involved in interconnections, including Google's. Even when hostnames exist, it is challenging to infer possible naming conventions that may enable mapping the hostnames to geolocations. Furthermore, many providers do not regularly maintain or update DNS entries [64, 31]. IP geolocation of core router infrastructure has similar problems: studies have shown that it is reliable only at the country or state level [55, 37, 35].

Another recent study [27] provided techniques to infer all intra-ISP links at the PoP level, combining archived traceroutes (from CAIDA Ark) with topology maps pub-

lished on ISP web sites. This probing technique maps collected IP interfaces to city-level PoPs using the dataset in [26] to extract geolocation hints from DNS hostname. While this study did not try to identify the location of peering interconnections, it provided useful insights related to the design and execution of traceroute campaigns. Research projects have also assembled physical Internet maps of ISPs at the PoP level [44] and of long-haul fiber-optic network in the U.S. [25].

8. CONCLUSION

The increasing complexity of interconnection hinders our ability to answer questions regarding their physical location and engineering approach. But this capability – to identify the exact facility of a given interconnection relationship, as well as its method – can enhance if not enable many network operations and research activities, including network troubleshooting, situational awareness and response to attacks, and many Internet cartography challenges.

In this paper we presented a measurement-driven methodology, called *constrained facility search*, to infer the physical facility where a target interconnection occurs from among all possible candidates, as well as the type of interconnection used. Our process narrows the number of candidate facilities for a given interconnection to those consistent with other known interconnections involving the same routers. Eventually the multiple sources of constraints leads to a small enough set of possible peering locations that in many cases, it becomes feasible to identify a single location that satisfies all known constraints. We believe this is the first time that these types of constraints have been used to infer where an interconnection physically occurs. We achieved over 90% accuracy in our application of this method to a large set of traceroute data collected in May 2015 (both historial archives and targeted measurements). This level of accuracy significantly outperforms heuristics based on naming schemes and IP geolocation.

We emphasize that discovery of all interconnections in the Internet is a far-reaching goal; our method can infer the location and type of given interconnections. Nevertheless, by utilizing results for individual interconnections and others inferred in the process, it is possible to incrementally construct a more detailed map of interconnections. Our data is available at http://www.caida.org/publications/paper/2015/constrained_facility_search/.

9. ACKNOWLEDGMENTS

This work was supported in part by NSF CNS-1414177. Georgios Smaragdakis was supported by the EU Marie Curie IOF "CDN-H" (PEOPLE-628441). The work was also funded by the Department of Homeland Security (DHS) Science and Technology Directorate, Cyber Security Division BAA 11-02 and SPAWAR Systems Center Pacific via contract number N66001-12-C-0130, and by Defence Research and Development Canada (DRDC) pursuant to an Agreement between the U.S. and Canadian governments for Cooperation in Science and Technology for Critical Infrastructure Protection and Border Security. The work represents the position of the authors and not necessarily that of NSF, DHS, or DRDC.

10. REFERENCES

[1] AMS-IX Connected Parties. https://ams-ix.net/connected_parties.
[2] DE-CIX quick facts. http://www.de-cix.net/about/quick-facts.
[3] Equinix Investor Relations: Annual and Quarter Results. http://investor.equinix.com/.
[4] Google Peering Policy (accessed 2013-4). https://peering.google.com/about/peering_policy.html.
[5] JPNAP Tokyo I Service. http://www.jpnap.net/english/jpnap-tokyo-i/index.html.
[6] Netacuity. http://www.digitalelement.com/our_technology/our_technology.html.
[7] *The Internet Under Crisis Conditions: Learning from September 11*. The National Academy Press, 2003.
[8] B. Ager, N. Chatzis, A. Feldmann, N. Sarrar, S. Uhlig, and W. Willinger. Anatomy of a Large European IXP. In *ACM SIGCOMM*, 2012.
[9] B. Ager, W. Mühlbauer, G. Smaragdakis, and S. Uhlig. Web Content Cartography. In *ACM IMC*, 2011.
[10] B. Augustin, X. Cuvellier, B. Orgogozo, F. Viger, T. Friedman, M. Latapy, C. Magnien, and R. Teixeira. Avoiding traceroute anomalies with Paris traceroute. In *ACM IMC*, 2006.
[11] B. Augustin, B. Krishnamurthy, and W. Willinger. IXPs: Mapped? In *ACM IMC*, 2009.
[12] Broadband Internet Technical Advisory Group Report (BITAG). Interconnection and Traffic Exchange on the Internet, 2014.
[13] R. Bush, O. Maennel, M. Roughan, and S. Uhlig. Internet Optometry: Assessing the Broken Glasses in Internet Reachability. In *ACM IMC*, 2009.
[14] M. Calder, X. Fan, Z. Hu, E. Katz-Bassett, J. Heidemann, and R. Govindan. Mapping the Expansion of Google's Serving Infrastructure. In *ACM IMC*, 2013.
[15] I. Castro, J. C. Cardona, S. Gorinsky, and P. Francois. Remote Peering: More Peering without Internet Flattening. In *CoNEXT*, 2014.
[16] I. Castro and S. Gorinsky. T4P: Hybrid Interconnection for Cost Reduction. In *NetEcon*, 2012.
[17] R. Chandra, P. Traina, and T. Li. BGP Communities Attribute, 1996.
[18] H. Chang, S. Jamin, and W. Willinger. Inferring AS-level Internet topology from router-level path traces. In *ITCom*, 2001.
[19] N. Chatzis, G. Smaragdakis, J. Boettger, T. Krenc, and A. Feldmann. On the benefits of using a large IXP as an Internet vantage point. In *ACM IMC*, 2013.
[20] N. Chatzis, G. Smaragdakis, A. Feldmann, and W. Willinger. There is More to IXPs than Meets the Eye. *ACM CCR*, 43(5), 2013.
[21] N. Chatzis, G. Smaragdakis, A. Feldmann, and W. Willinger. Quo vadis Open-IX? Trying to boost public peering in the US. *ACM CCR*, 45(1), 2015.
[22] K. Cho, C. Pelsser, R. Bush, and Y. Won. The Japan

Earthquake: the impact on traffic and routing observed by a local ISP. In *ACM CoNEXT SWID workshop*, 2011.

[23] Cymru Team. IP to ASN mapping. *http://www.team-cymru.org/IP-ASN-mapping.html*.

[24] J. Czyz, M. Kallitsis, M. Gharaibeh, C. Papadopoulos, M. Bailey, and M. Karir. Taming the 800 Pound Gorilla: The Rise and Decline of NTP DDoS Attacks. In *ACM IMC*, 2014.

[25] R. Durairajan, P. Barford, J. Sommers, and W. Willinger. InterTubes: A Study of the US Long-haul Fiber-optic Infrastructure. In *ACM SIGCOMM*, 2015.

[26] R. Durairajan, S. Ghosh, X. Tang, P. Barford, and B. Eriksson. Internet atlas: A Geographic Database of the Internet. In *Proc. of HotPlanet*, 2013.

[27] R. Durairajan, J. Sommers, and P. Barford. Layer 1-Informed Internet Topology Measurement. In *ACM IMC*, 2014.

[28] Z. Durumeric, E. Wustrow, and J. A. Halderman. ZMap: Fast Internet-Wide Scanning and its Security Applications. In *USENIX Security Symposium*, 2013.

[29] Equinix. Global Data Centers and Colocation Services. http://www.equinix.com/locations/.

[30] P. Faratin, D. Clark, S. Bauer, W. Lehr, P. Gilmore, and A. Berger. The Growing Complexity of Internet Interconnection. *Communications and Strategies*, 2008.

[31] M. J. Freedman, M. Vutukuru, N. Feamster, and H. Balakrishnan. Geographic Locality of IP Prefixes. In *ACM IMC*, 2005.

[32] A. Gerber and R. Doverspike. Traffic Types and Growth in Backbone Networks. In *OFC/NFOEC*, 2011.

[33] V. Giotsas, M. Luckie, B. Huffaker, and kc claffy. Inferring Complex AS Relationships. In *ACM IMC*, 2014.

[34] V. Giotsas, S. Zhou, M. Luckie, and kc claffy. Inferring Multilateral Peering. In *CoNEXT*, 2013.

[35] B. Gueye, A. Ziviani, M. Crovella, and S. Fdida. Constraint-Based Geolocation of Internet Hosts. *IEEE/ACM Trans. Networking*, 14(6), 2006.

[36] B. Huffaker, M. Fomenkov, et al. DRoP: DNS-based router positioning. *ACM CCR*, 44(3), 2014.

[37] B. Huffaker, M. Fomenkov, and k. claffy. Geocompare: A Comparison of Public and Commercial Geolocation Databases. Technical report, CAIDA, May 2011.

[38] Interxion. Locations. http://www.interxion.com/locations/.

[39] E. Katz-Bassett, J. P. John, A. Krishnamurthy, D. Wetherall, T. Anderson, and Y. Chawathe. Towards IP geolocation using delay and topology measurements. In *ACM IMC*, 2006.

[40] E. Katz-Bassett, H. Madhyastha, V. Adhikari, C. Scott, J. Sherry, P. van Wesep, A. Krishnamurthy, and T. Anderson. Reverse Traceroute. In *NSDI*, 2010.

[41] T. Kernen. traceroute.org. http://www.traceroute.org.

[42] K. Keys, Y. Hyun, M. Luckie, and k claffy. Internet-Scale IPv4 Alias Resolution with MIDAR. *IEEE/ACM Trans. Networking*, 21(2), 2013.

[43] A. Khan, T. Kwon, H. C. Kim, and Y. Choi. AS-level Topology Collection through Looking Glass Servers. In *ACM IMC*, 2013.

[44] S. Knight, H. X. Nguyen, N. Falkner, R. Bowden, and M. Roughan. The Internet Topology Zoo. *IEEE J. on Sel. Areas in Comm.*, 29(9), 2011.

[45] A. Kumar, V. Paxson, and N. Weaver. Exploiting Underlying Structure for Detailed Reconstruction of an Internet Scale Event. In *ACM IMC*, 2005.

[46] C. Labovitz, S. Lekel-Johnson, D. McPherson, J. Oberheide, and F. Jahanian. Internet Inter-Domain Traffic. In *ACM SIGCOMM*, 2010.

[47] A. Lodhi, N. Larson, A. Dhamdhere, C. Dovrolis, and K. Claffy. Using PeeringDB to Understand the Peering Ecosystem. *ACM CCR*, 44(2), 2014.

[48] M. Luckie, A. Dhamdhere, D. Clark, B. Huffaker, and kc claffy. Challenges in Inferring Internet Interdomain Congestion. In *ACM IMC*, 2014.

[49] M. Luckie, B. Huffaker, A. Dhamdhere, V. Giotsas, and kc claffy. AS Relationships, Customers Cones, and Validations. In *ACM IMC*, 2013.

[50] H. V. Madhyastha, T. Isdal, M. Piatek, C. Dixon, T. Anderson, A. Kirshnamurthy, and A. Venkataramani. iPlane: An information plane for distributed systems. In *ACM OSDI*, 2006.

[51] R. Motamedi, B. Chandrasekaran, B. Maggs, R. Rejaie, and W. Willinger. On the Geography of X-Connects. U. Oregon, CIS-TR-2014-1, May 2015.

[52] W. Muhlbauer, A. F. O. Maennel, M. Roughan, and S. Uhlig. Building an AS-Topology Model that Captures Route Diversity. In *ACM SIGCOMM*, 2006.

[53] W. B. Norton. The Art of Peering: The Peering Playbook, 2010.

[54] I. Poese, B. Frank, G. Smaragdakis, S. Uhlig, A. Feldmann, and B. Maggs. Enabling Content-aware Traffic Engineering. *ACM CCR*, 42(5), 2012.

[55] I. Poese, S. Uhlig, M. A. Kaafar, B. Donnet, and B. Gueye. IP Geolocation Databases: Unreliable? *ACM CCR*, 41(2), 2011.

[56] L. Quan, J. Heidemann, and Y. Pradkin. Trinocular: Understanding Internet Reliability Through Adaptive Probing. In *ACM SIGCOMM*, 2013.

[57] P. Richter, G. Smaragdakis, A. Feldmann, N. Chatzis, J. Boettger, and W. Willinger. Peering at Peerings: On the Role of IXP Route Servers. In *ACM IMC*, 2014.

[58] M. Roughan, W. Willinger, O. Maennel, D. Pertouli, and R. Bush. 10 Lessons from 10 Years of Measuring and Modeling the Internet's Autonomous Systems. *IEEE J. on Sel. Areas in Comm.*, 29(9), 2011.

[59] M. A. Sánchez, J. S. Otto, Z. S. Bischof, D. R. Choffnes, F. E. Bustamante, B. Krishnamurthy, and W. Willinger. Dasu: Pushing Experiments to the Internet's Edge. In *NSDI*, 2013.

[60] J. H. Sowell. Framing the Value of Internet Exchange Participation. In *Proc. of TPRC*, 2013.

[61] Telehouse. Colocation Services. http://www.telehouse.com/facilities/colocation/.

[62] R. van Rijswijk-Deij, A. Sperotto, and A. Pras. DNSSEC and its Potential for DDoS Attacks – A Comprehensive Measurement Study. In *ACM IMC*, 2014.

[63] W. Willinger and M. Roughan. Internet Topology Research Redux. *Recent Advances in Networking*, 1(1), 2013.

[64] M. Zhang, Y. Ruan, V. Pai, and J. Rexford. How DNS Misnaming Distorts Internet Topology Mapping. In *USENIX ATC*, 2006.

[65] Y. Zhang, R. Oliveira, H. Zhang, and L. Zhang. Quantifying the pitfalls of traceroute in AS connectivity inference. In *PAM*, 2010.