The opacity of the Internet infrastructure limits the capability of research and development efforts to model network behavior and topology, design protocols and/or new architectures, and study real-world properties such as robustness, resilience, and economics. Overcoming these limitations is impossible without realistic and representative datasets, and measurement infrastructure on which to support sustained longitudinal measurements as well as new experiments. CAIDA has been navigating the interdisciplinary challenges of operating Internet measurement infrastructure for nearly 20 years: collecting, coordinating, curating, and sharing data sets for the network research and operational community in support of Internet science.

With previous CRI (and DHS) funding we have designed, implemented, deployed, and operated a secure measurement platform, Archipelago, that supports large-scale active measurement studies of the global Internet. Since 2007 Archipelago has gathered the largest set of network topology data used for a broad spectrum of scientific research, from physics to biology, from infrastructure vulnerability assessments to theory of complex networks.

Now that we have this intellectually fertile community research infrastructure firmly established, we want to focus on achieving greater involvement from a broader cross-section of the CISE and other research communities, by lowering the barrier to using the infrastructure and data products that we curate. We propose four infrastructure development tasks. First, we will deploy a new hardware architecture that expands the scale and manageability of the infrastructure. Second, we will integrate recent measurement technology advances to enable fundamentally new scientific experiments and data sets. Third, we will upgrade the functionality of our measurement-on-demand web interface to the Ark platform to enable richer scheduling of more complex measurements. Fourth, we will create a new interface for browsing, querying, and visualizing the data gathered.

Improving data curation and implementing a user-friendly web-based interface to the data products require significant software and systems experience, resources, and domain knowledge, and it is exactly the sort of activity researchers do not have resources to do themselves. The results of our project will amplify the impact of NSF's investment into this community infrastructure and will support CISE research by enabling new data products that are more compelling than before to a wide range of Internet and network research disciplines: from empirical assessments of global Internet security and stability vulnerabilities, to scientific modeling and mapping of complex networks, to retrospective and prospective studies of network architecture evolution.

Intellectual Merit. Ark is a unique laboratory in which researchers can quickly design, implement, and easily coordinate the execution of experiments across a globally distributed set of dedicated monitors. It supports precise time synchronization across monitors, continuous comprehensive global Internet topology measurements, and measurements-on-demand. Ark's enhanced capabilities and data products will support crucial transformative research in network and security, providing empirical grounding for study of: real-world Internet phenomena (e.g., TCP and middlebox (mis)behavior, outage analysis, BGP hijacking, congestion induced by commercial peering disputes, evolution of address space utilization and IPv6 evolution); theoretical and practical efforts in network modeling and mapping; longitudinal studies of the Internet's historical evolution, and evaluation of potential future network architectures.

Broader Impacts. We will disseminate the results of this project via conferences, web sites, blogs, and workshops. Our focus is on lowering the barrier to CISE community use of the infrastructure and data products for research and educational needs. We will also provide convenient and interactive public remote access to a massive volume of heavily curated topology data, enabling broad understanding by the general public of the most exciting critical infrastructure ever invented.

Keywords: active Internet measurement infrastructure; empirical network science; topology data analysis; curation

Contents

Internet Laboratory for Empirical Network Science - Next Phase (iLENS-NP)

1 Introduction: Expanding the Reach and Impact of Internet Topology Data

The best publicly available data about the global interconnection system that carries most of the world's communications traffic is incomplete and of unknown accuracy. There is no map of physical link locations, capacity, utilization, or interconnection arrangements. This opacity of the Internet infrastructure hinders research and development efforts to model network behavior and topology; design protocols and new architectures; and study real-world properties such as robustness, resilience, and economic sustainability. There are good reasons for the dearth of information: complexity and scale of the infrastructure; information-hiding properties of the routing system; security and commercial sensitivities; costs of storing and processing the data; and lack of incentives to gather or share data in the first place, including cost-effective ways to use it operationally [1]. But understanding the Internet's history and present, much less its future, is impossible without realistic and representative datasets and measurement infrastructure on which to support sustained longitudinal measurements as well as new experiments.

With previous CRI (and DHS) funding we designed, implemented, deployed, and operated a secure infrastructure named Archipelago (Ark) [2, 3] that supports large-scale active measurement studies of the global Internet. We are committed to open source and have publicly released several measurement, analysis, and infrastructure tools. Since 2007 Ark has gathered the largest set of IP topology data in use by a broad set of academic researchers for a range of scientific research from physics to biology to network science, from critical infrastructure vulnerability assessments to theoretical study of complex networks.

Now that we have this community research infrastructure stably in place, we want to focus on achieving greater involvement from a broader cross-section of the CISE and other research communities, by lowering the barrier to and increasing the benefit of using the infrastructure and data products that we curate. In response to feedback from the research community, we propose four infrastructure development tasks. First, we will deploy a new hardware architecture that expands the scale and manageability of the infrastructure. Second, we will integrate into our infrastructure recent measurement and analysis advances that will enable new scientific experiments and data products. Third, we will upgrade the functionality of our measurement-on-demand web interface to the Ark infrastructure to enable richer scheduling of more complex measurements. Fourth, we will create an interface for browsing, querying, and visualizing the data gathered by the infrastructure. We will continue our AIMS annual workshop series which consistently yields feedback on what measurements, data formats, and data curation functionality would be most helpful to answer specific network and security research questions. Not only does the Ark measurement infrastructure provide a unique laboratory in which researchers can quickly design, implement, and easily coordinate the execution of experiments across a widely distributed set of dedicated monitors, but it enables data products that are more compelling than ever to a wide range of network, security, and Internet science.

Section 2 describes the infrastructure and architecture of the Ark system, including deployment status, features, and limitations, as well its relationship to other Internet mapping efforts. Section 3 reviews data products derived from the existing Ark monitoring infrastructure, and research they support. Section 4 presents our proposal for enhancing Ark's hardware and software functionality. Section 5 lists new research activities to be enabled by the enhanced Ark platform. The remaining sections describe community outreach, team qualifications, and management plan.

2 Archipelago Active Measurement Platform

Archipelago (Ark) [3] is CAIDA's active measurement infrastructure [4] running software that allows distributed nodes to operate as a coordinated secure measurement platform. From its inception in September 2007, Ark has gathered the largest global Internet topology data for use by academic researchers. Figure 1 depicts the 106 Ark monitors we deployed at an average of 15 per year (cumulative deployment is higher due to upgrades and replacements of failed hardware), with 38 having IPv6 connectivity. They are hosted by diverse organizations: 47 research/educational, 23 commercial, 10 network infrastructure (NIC/IXP), 24 residential, and 2 others. In 2012, we ported our measurement software platform to the Raspberry Pi [5], a small, inexpensive computer running Linux (700MHz ARM CPU, 512MB RAM, 8GB SD card). We have deployed 58 Raspberry Pi Ark monitors so far. (Section 4.1 describes the many advantages of this platform.)

Figure 1: As of November 2014, there are 106 Ark monitors in 40 countries (in 91 different cities).

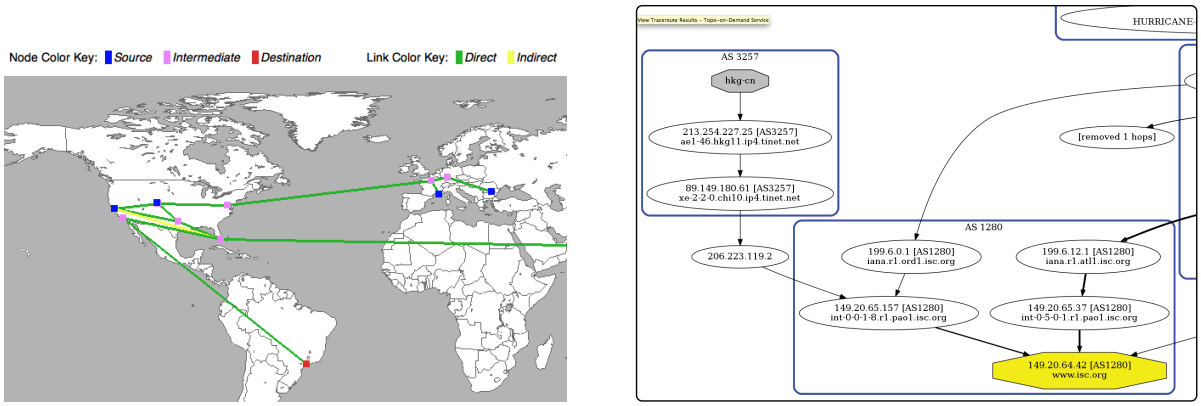
High-precision system-wide clock synchronization is an under-exploited capability in today's measurement infrastructures because it typically requires dedicated hardware (e.g., GPS, CDMA, radio clock) with its attendant costs and logistical issues. RADclock [6, 7] is a software-based alternative that provides sub-millisecond accuracy (compared to multi-millisecond accuracy with NTP). RADclock, currently running on 36 Ark monitors, enables measurements such as one-way delay that require precise comparisons of timestamps taken on separate machines. RADclock has increased the effectiveness of our MIDAR alias resolution tool [8] which needs to precisely order overlapping measurements taken by multiple monitors to the same destination (Section 3.1).

2.1 Rapid prototyping of coordinated measurements

Ark supports rapid prototyping by promoting software development at a high-level of abstraction using dynamic scripting languages and pre-built APIs and services. We use Ruby [9] for measurements and related libraries, e.g., to control *scamper* [10], a flexible active measurement tool supporting IPv4, IPv6, ping, and several traceroute variants (TCP-, UDP-, and ICMP-, and Paris [11]). Scamper is open source software actively maintained at CAIDA. To coordinate measurements on a distributed heterogeneous infrastructure, CAIDA released its open source implementation of the Marinda *tuple-space* coordination model first introduced by D. Gelernter [12]. Marinda supports decentralized measurement processes executing autonomously at each monitor and communicating as needed, e.g., to trigger measurements or analyses based on locally observed events.

2.2 Support for measurements by community researchers

The Ark infrastructure supports two means of conducting measurements. First, researchers can execute their own custom tool (using raw sockets) on each monitor using ssh-like Ark tools for remotely executing commands concurrently on multiple monitors. We coordinate such direct access to limited monitor resources to prevent interference between measurements. This method supported several research efforts that improved topology measurement and inference methods [13, 14, 8, 15, 16], refuted a recent study on traceroute data [17, 18], contributed to assessments of infrastructure vulnerability [19], and tested IPv6 functionality on World IPv6 Day [20].



(a) Visual traceroute

(b) Traceroute hops (ovals) grouped by ASes (boxes)

Figure 2: Measurement displays in Vela.

Second, researchers can remotely execute a set of measurements via Ark-provided services, such as our measurement-on-demand web interface Vela [21], that do not require accounts on Ark monitors. These services lower the barrier for researchers to take advantage of the Ark platform and allows us to implement rate limiting and scheduling to prevent overloading of Ark monitors. Vela provides a convenient way to execute on-demand ping and traceroute measurements in IPv4 and IPv6 using ICMP, UDP, or TCP from any Ark monitor. Vela has two interfaces: command-line and web-based. The command-line interface is useful for large-scale feedback-driven, or dynamic measurements under the full control of the user's own program. The web interface supports interactive ad-hoc exploratory measurements and visualization of results. For example, we geolocate traceroute paths on geographic maps (Figure 2(a)), and we display traceroute paths as graphs with hops visually grouped into ASes (Figure 2(b)).

2.3 Comparison with other measurement infrastructures

Several research infrastructures conducted active measurements in the past, but they are either no longer funded [22, 23, 24, 25, 26], or had limitations that inspired our creation of Ark [27, 28].

PlanetLab [29], a global academic network testbed for distributed computer systems research, has hosted active Internet measurement projects in the past [30, 31], but there are some limitations for Internet measurements, such as security restrictions that prevent any type of spoofing, lack of IPv6 support, academic site bias, and usage restrictions [32, 33]. (See Beverly's letter of collaboration (LOC).)

The BISmark [34] project measures residential broadband performance and home network usage by deploying routers with custom firmware in homes of regular (non-technical) users. The project's primary focus is on characterizing broadband and home-networks [34, 35], and they are interested in applying our interdomain congestion measurement capabitilies on the Bismark observatory to study Internet quality of experience for home users, as well as develop and test their own tomographic techniques to measure interdomain congestion [36]. (See Feamster's LOC.)

The RIPE (Réseaux IP Européens) NCC operates Atlas [37], an active measurement infrastructure consisting of tiny, inexpensive computers capable of ping, traceroute, DNS lookup, HTTP GET/HEAD/POST, and SSL certificate retrieval. Currently over 4000 vantage points perform periodic and user-initiated measurements to root servers or user-defined targets. The RIPE NCC provides a web-browser interface as well as a REST interface for requesting measurements that

employ one of the predefined methods. However, the limited capabilities of the Atlas hardware do not allow for the execution of user-provided measurement software.

With popular as well as scientific attention to Internet measurement growing, Ark has a unique combination of features that complement other existing Internet measurement infrastructures: diversity of vantage point deployment (Clark, Beverly, Bailey LOC); longevity that enables longitudinal data sets (over 15 years of macroscopic Internet topology data and metadata); support for not only user-defined measurement, but executing user-provided software; support for precise time synchronization; IPv6 measurement capabilities; annual workshops to serve the community; and a well-tested data sharing framework that protects privacy of Internet users as well as researchers using the data.

Other active measurement projects consist of software tools or plug-ins deployed by volunteers at the edge to measure topology [38, 39], application performance [40, 41, 42], or troubleshoot local connectivity problems [43, 44], while limiting the computation and bandwidth burden on the user. The easier deployability of software-based infrastructures generally lead to larger footprints than hardware-based infrastructures can achieve, but the drawbacks are a less-controlled measurement execution environment, and measurements often geared toward operational needs of users rather than scientific research.

Although not a measurement project itself, UCLA's Internet Research Lab provides a repository of AS-level topology data at the autonomous system (AS) level [45], derived by processing BGP data from collectors at Routeviews, RIPE NCC, PCH, and Internet2. They publish AS-level topology data aggregated to daily and monthly granularities, annotated with AS-relationships.

3 Results from Previous CRI Project (CNS-0958547, $1.5M, Mar 2010 - Feb 2014)

A previous CRI grant entitled "**Internet Laboratory for Empirical Network Science**" allowed the creation and maintenance of the Archipelago measurement infrastructure. (This project was itself a continuation of an earlier CRI project "Community-Oriented Network Measurement Infrastructure" (CNS-0551542), Sep 2006 - Sep 2011). The **intellectual merit** of this project was in the demonstrated ability for the Ark measurement infrastructure and data to serve other researchers undertaking macroscopic studies of the Internet. Our infrastructure development tasks resulted in: (1) new monitors in regions we lacked coverage; (2) novel tools for processing raw topology data; and (3) enabling active Internet measurement experimentation to a broad community. We also organized and hosted four annual workshops and published the reports in CCR. The project resulted in 20 CAIDA publications (listed at http://www.caida.org/funding/ilens) (plus many others, see below), ongoing topology-related data sets (http://www.caida.org/data), and several open source measurement and analysis software tools (http://www.caida.org/tools).

The **broader impacts** of this project were reflected by the data's effectiveness at strengthening a wide range of network modeling, simulation, analysis, and theoretical research activities, and enabling new types of research, and empirical grounding for the (then) emerging discipline of network science. This section provides details on data products provided by the Ark infrastructure and research enabled by these data products.

3.1 Data products provided by the Ark infrastructure

In this section we highlight Ark's three major data products: (1) a comprehensive longitudinal dataset of IPv4 and IPv6 topology data; (2) rich DNS data associated with observed IP addresses; and (3) strategic data set resulting from heavy curation of raw topology data to convert to router and AS-level granularities.

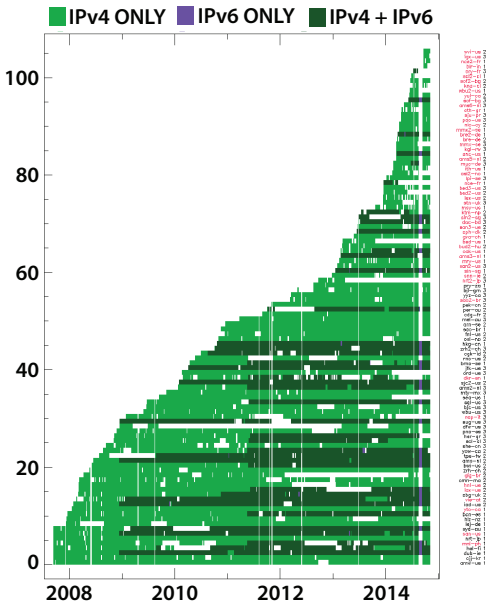


Figure 3: Darker areas indicate availability of both IPv4 and IPv6 traceroute data; lighter areas are only IPv4.

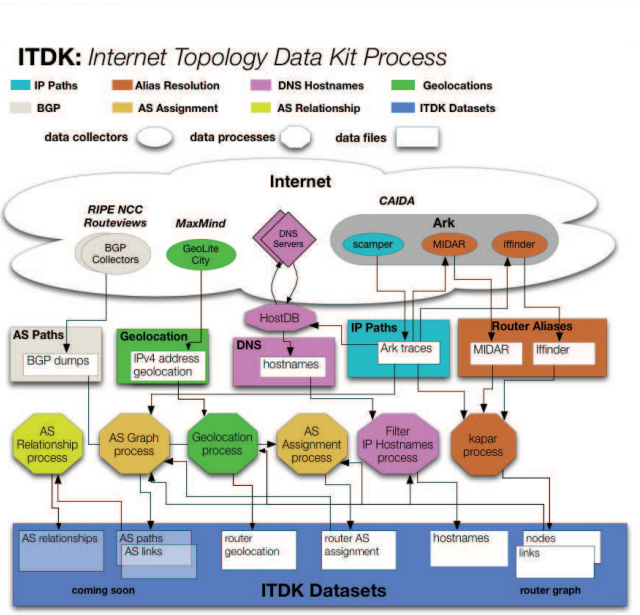


Figure 4: Internet topology data measurement, mining, and analysis process.

First, the Ark infrastructure continues to collect our most comprehensive and scientifically generative active data set – the IPv4 Routed /24 Topology Dataset [46] – by systematically measuring IP-level paths to a dynamically generated list of IP addresses covering all /24 prefixes in routed IPv4 address space. Figure 3 shows the availability of our IPv4 and IPv6 traceroute data since September 2007 (the figure also shows our monitor deployment growth). In total we have collected 32 billion IPv4 traceroutes (14 TB) and 345 million IPv6 traceroutes (158 GB).

Second, we perform DNS lookups of all IP addresses observed in our IPv4 and IPv6 topology probing. We use a customized bulk DNS lookup service capable of millions of DNS lookups per day. In addition to a simple IP-to-hostname, we store the raw DNS query/response traffic generated by the lookup service. The first dataset is useful for annotating IP topology data with information commonly encoded in router names, such as geographic location, link capacity, router type (access vs. backbone), and customer network name. The second dataset is useful for studying characteristics of DNS name servers, such as the penetration of DNSSEC and IPv6.

Third, we curate approximately two-week snapshots of these data into Internet Topology Data Kits (ITDK) [47] (Figure 4) providing inferred router-level and AS-level topologies of the global Internet. We released seven ITDKs during the course of the previous CRI project, increasing their richness over time by integrating new techniques we developed, including AS ownership inference [48] and scalable alias resolution with MIDAR [8]. *Alias resolution* is the process of identifying which interface IP addresses belong to the same routers, which is required to convert the IP-level topology discovered by traceroute to a router-level topology [49].

MIDAR (Monotonic ID-Based Alias Resolution), inspired by [50], uses multiple probing methods, multiple vantage points, and a novel sliding-window probe scheduling algorithm to increase scalability to millions of IP addresses. Because each alias resolution technique makes tradeoffs between accuracy, completeness, and scalability, we have combined the results of three techniques—MIDAR, iffinder [51], and kapar [52]—in the ITDK to produce the most comprehensive and accurate alias resolution dataset available to date.

Each data kit also contains a set of router-to-AS assignments [48] produced by (1) mapping the IP addresses of each router to the AS announcing the longest-matching prefix in publicly available BGP tables [53], and (2) inferring a single AS for the whole router based on the AS assignments of each router interface and the assignments of neighboring routers.

In addition to the ITDK, we make several processed data sets available as "soft infrastructure" to researchers: traceroute-derived AS Links (IPv4 and IPv6) [54], and BGP-derived data to support richer annotation and topology inferences [55, 56, 57]. To enable more informed selection of topology datasets for specific research needs, we have published analyses comparing different sources of topology data (BGP, WHOIS, and three sources of traceroute data—Ark, iPlane [30] and UCLA's IRL [45]) for constructing AS- and router-level graphs [58, 59].

3.2 New research opportunities enabled by current data products

Our web site lists publications known to us by non-CAIDA authors that make use of CAIDA data (summarized in Figure 5) [60], a lower bound since we cannot enforce the reporting requirement of our AUP. Researchers have requested CAIDA's topology data to support research in the areas of: modeling IPv4 and IPv6 AS-level topology and routing behavior; alias resolution, router-level, and PoP-level topology discovery (including classified work to support DARPA's Plan X project); topology inference and fault diagnosis; infrastructure failure assessments; machine-learning-based AS classification; incongruity between data plane and control plane paths; improving anycast implementations; new metrics for describing scale-free networks; peer-to-peer system scalability; improving visualization of complex systems; geolocation; modeling of delay; improved traceback for network attacks; and new protocols (extensions of IP) to support attribution and prioritization. Publications reported back to us have covered a variety of topics related to the security and stability of the Internet as critical infrastructure [61, 62, 63, 64]: growth analysis of ISPs [65]; infrastructure improvements in the developing world [66]; interdomain traffic estimation [67]; Internet mapping [68], router-level topology discovery [14, 69, 70]; tomography [71] and path prediction techniques [72]; evolution of interconnection policies and controversies [73]; risks of Internet partitioning [74]; prefix hijacking [75, 76, 77]; DDoS attack countermeasures [78, 79]; complex network robustness in the face of epidemics [80]; geometric analysis of the Internet topology [81]; complex network theory [82, 83]; future Internet architectures; CDN architectures [84]; and a geographic database ("Atlas") of the Internet at the physical layer [85, 86].

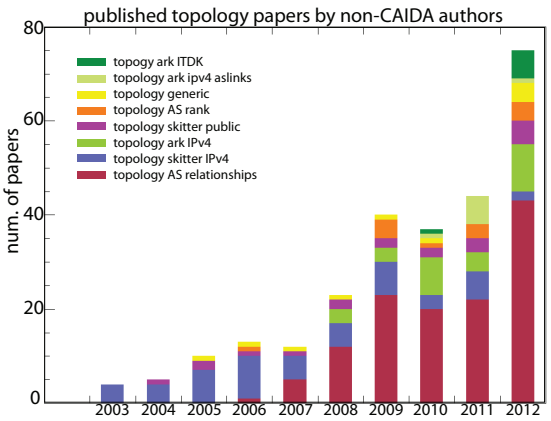


Figure 5: External (non-CAIDA) papers reported (a lower bound since reporting not enforced) to CAIDA as using our topology data.

4 Proposed Infrastructure and Data Product Enhancements

4.1 Task 1. Raspberry Pi-based infrastructure expansion

The availability of the Raspberry Pi computing platform has dramatically improved our deployment capabilities. A Raspberry Pi has minimal requirements on power, cooling, and space, and

even with required accessories, the hardware costs $70, or about one tenth the cost of our previous 1U server hardware. Shipping costs are similarly reduced, and we now have the option to hand distribute complete Ark monitor kits at conferences and other meetings, thereby further lowering distribution effort, cost, and barriers. This new platform is also more suitable for residential deployment, due to its unobtrusiveness, and distribution to underrepresented areas such as South America and Africa, where traditional shipping face customs hurdles.

We will expand our measurement infrastructure to 300 nodes, aiming for diversity in vantage points (educational, commercial, business, and residential) and a representative geographical coverage of the entire world. This larger footprint will contribute toward higher fidelity data (e.g., coverage of peering links), reduced academic and other biases (e.g., content vs. eye-ball networks), the mitigation of practical difficulties that may impede research (e.g., filtering/blocking of IP options by some networks, the 9-hop limit of the IP Record Route option), and measurement of behavior that is location-based (e.g., DNS anycasting, CDN).

We will continue developing software to reduce the impact of Ark monitor downtime on data collection. With our increasing deployment in residential locations, we can no longer rely on the availability of technically-skilled remote hands to resolve a severe failure, such as a corrupted filesystem, that renders a system remotely inaccessible. By exploiting the unique architecture of the Raspberry Pi and a feature of the Linux kernel, we have discovered a way of effectively achieving a remote serial console in software—we can create two live systems, with one always being remotely accessible. Major upgrades to the OS are also made possible with this approach.

We will continue to collaborate with the RADclock developers to deploy RADclock on the Raspberry Pi. Through this collaboration, we have already tried an early development version of the Raspberry Pi port, confirming feasibility.

4.2 Task 2: Integration of recent measurement and analysis advances

We will integrate recent measurement and analysis advances that will enable production of higher-fidelity router- and AS-level topology maps desired by the research community for not only Internet mapping but also, for example, to parameterize routing models, inform commercial peering disputes, detect IPv4 address space transfers, and validate assumptions embedded in future architecture research [87].

4.2.1 More efficient topology probing primitives

Due to the large size of the routed IPv4 address space (around 2.7 billion addresses, or 162 /8's worth, as of Nov 2014), one challenge in active-measurement based Internet-wide topology mapping is balancing probing efficiency, such as network load and measurement duration, with coverage. One reasonable tradeoff is to perform relatively low-frequency (every 2 days) sweep of the routed space at a /24-prefix granularity, as with our ongoing macroscopic topology measurements [46], which prioritizes maximal topological coverage over fine-grained temporal resolution. Other experiments may want to sample topology more frequently (for example, to detect network outages or routing instability) or with a lower probing load (for example, to exhaustively discover all network subnetting without triggering complaints).

Beverly *et al.* [88] and [89] (which used Ark) introduced three new topology-probing primitives that attempt to discover higher topological richness at a lower probing cost than brute-force approaches. We plan to further collaborate with Beverly's group (see LOC) to operationalize these techniques into Ark's ongoing probing. Two techniques are of particular interest: *Subnet-Centric Probing* and *Ingress Point Spreading*. Subnet Centric Probing carefully selects destinations in order

to maximize the chances of discovering further details about the internal structure (that is, subnets) of the target network with each additional trace. Ingress Point Spreading uses knowledge discovered about the ingress diversity of the target network in prior rounds of probing to carefully select a minimal number of vantage points that will continue to cover all known paths into the destination network in future probing. Discovery of ingress diversity is useful for characterizing the topological richness and resiliency of the constituent networks making up the Internet.

We will incorporate the above techniques into new topology measurements that complement ongoing large-scale measurements. The focus will be on high-frequency sampling of the routed address space and target networks to discover greater routing dynamics as well as additional topology details missed by our ongoing collections.

4.2.2 More accurate inferences from traceroute data

We propose to apply three experimental techniques to improve the quality of the derived data sets (e.g., ITDK, AS links) we produce from our raw traceroute data.

First, we will deploy our *prefixscan* measurement technique [10] for empirically validating that traceroute-observed addresses correspond to inbound router interfaces and not third-party addresses. Third-party addresses are traceroute measurement artifacts [90, 17, 18] that can distort inferences, such as about AS-level connectivity.

Second, we will remove IXP (Internet exchange point) addresses appearing in traceroutes due to their accidental or inappropriate announcement by IXes or their members. Links that cross an IX's address space are actually peering links between ASes connected to the IX, rather than to the IX itself. When an AS announces IX address space, a simplistic mapping of addresses to ASes will introduce false peering links to the IXes themselves, as well as hide actual peering links between pairs of ASes on either side of the IX. We developed a method to recover the true peering connectivity [91], by inferring links across IX address space as self-identified in PeeringDB [92].

Third, the most prevalent false AS link inference from traceroute data derives from IP address sharing between peering routers to establish a point-to-point link [93]. When we observe only a single router in a given AS Y before observing a router in a neighbor AS Z, and Y's observed router address is originated by AS X in BGP, we may falsely infer an AS link between X and Z. We recently developed a technique that uses traceroute graph analysis and validated AS relationships to accurately infer router ownership, and used it to infer missing AS peering links from Ark data. We will refine and integrate this system into our data curation process.

4.3 Task 3: User-friendly interface for conducting measurements

We propose to upgrade our measurement-on-demand service *Vela* to meet broader scientific needs. First, we propose supporting richer scheduling of more complex measurements, such as date/time-based execution, periodic measurements, and conditional execution based on event-based triggers (such as packet loss or a detected path change). Second, we propose providing access to capabilities already implemented in scamper that are useful for protocol, performance, and stability characterization studies. Specifically, we will integrate MDA traceroute for enumerating all load-balanced paths towards a given destination [11] and TCP behavior inference [94]. Luckie *et al.* used these capabilities on Ark to investigate the prevalence of Path MTU discovery failures [95]. We will also develop on-demand access to our existing active alias resolution capabilities—MIDAR, iffinder, and motu [8, 96, 97, 51]. At our annual AIMS workshops, we will consult with the community on additional measurements that would further their research and then provide turnkey implementations where feasible.

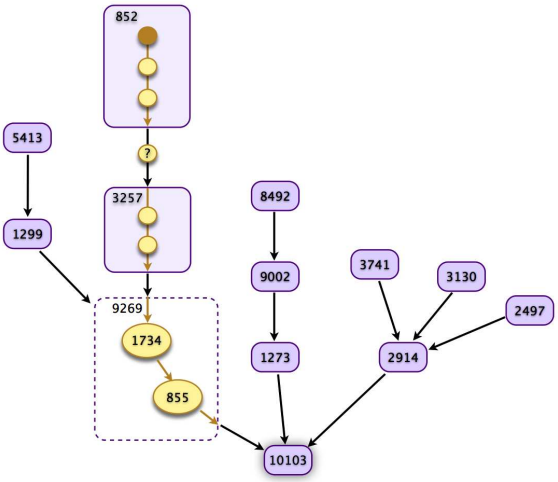


Figure 6: BGP AS paths (rectangles) toward the destination AS 10103 overlaid with a traceroute path (circles/ovals) to the same destination, revealing commonalities and differences in ASes observed by BGP and traceroute.

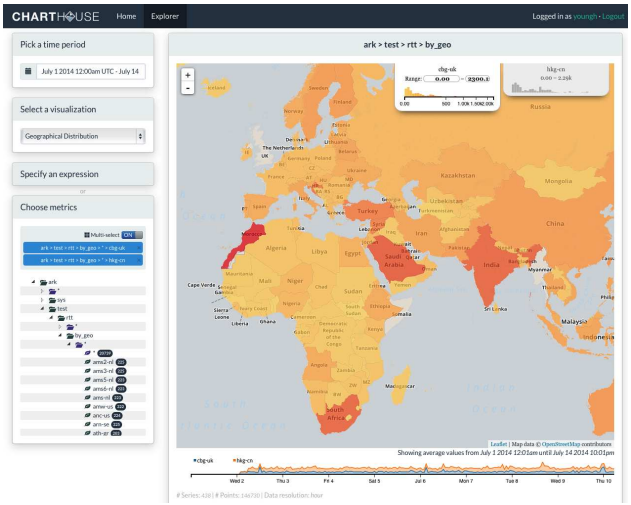


Figure 7: Viewing time series of global traceroute RTT measurements from two Ark monitors using CAIDA's Charthouse web application (in development).

We will implement a new visualization mode in Vela that highlights incongruities between AS paths derived from BGP and traceroutes. Such incongruities can arise from sibling ASes, IXP ASes, incorrect IP-to-AS mapping, third-party addresses, and other causes [98, 99, 100]. Our prototype visualization is illustrated by Figure 6 using a hypothetical example. Circles and ovals represent IP hops from traceroute, and rounded rectangles represent BGP AS hops. The first six traceroute IP hops more or less agree with BGP AS paths, with the possible exception of an unresponsive fourth hop, but they then diverge.

4.4 Task 4: Rich interface for browsing, querying, and visualizing data

Discovery of the full potential value of raw data is best served by a rich, easy-to-use interactive exploratory interface. We propose implementing web-based interfaces for browsing, querying, and visualizing our archive of multi-terabytes of data, taking inspiration from RIPEstat [101] and our own visualization efforts [102]. Users will be able to examine the data over space and time to study evolving topology and performance trends in the global Internet.

The *browsing interface* would allow researchers to understand broad properties and summary statistics of the available data over multiple time scales and aggregation levels, from simple trace counts and response rates, to calculated path-length and RTT distributions, to inferred AS links. Figure 7 shows a prototype interface for viewing the time series of global traceroute RTT measurements from two Ark monitors. This prototype is implemented with Charthouse, a web application for interactive real-time and historical time-series data exploration, currently in development at CAIDA for an NSF-funded project on Internet infrastructure outage detection [103].

The *query interface* would allow researchers to find the most relevant data for their research, such as all traceroutes through a given region and time period toward/across a particular prefix/AS. Other queries might retrieve the router address aliases for a given IP address, all routers in a given city, or all inferred links to a router identified by a given IP address.

We will take advantage of the computational and storage resources, as well as big data expertise, available at the San Diego Supercomputer Center, where CAIDA is based, to implement this

data mining functionality. We will also use open source frameworks for large-scale data processing, such as Apache Spark [104], to achieve the scalability needed for interactive performance.

5 Research Enabled by Enhanced Data and Infrastructure

The proposed expansion and extension of the infrastructure—in scale, functionality, and accessibility as well as in capabilities to navigate the resulting data—will enable the following new or expanded research opportunities of strategic national and international interest, most of them CISE-funded. Table 1 lists a sample of research interests articulated in the attached letters of collaboration, and which proposed infrastructure enhancements are required to support them.

Table 1: Research topics described in letters of collaboration (LOCs) with cross-references to proposed infrastructure enhancements (by tasks listed in Section 4) required to enable research topic.

Enabled Research	Letters of Collaboration	Proposed Enhancements
Internet Security and Stability Vulnerabilities		
· hygiene	Bailey, Beverly, Deccio	1, 2, 4
· outages	Caesar, Feamster, FCC	1, 3
· congestion	Caesar, Clark, Feamster, FCC	1, 3
· diagnostics	Feamster, Katz-B.	1, 2, 3, 4
· hijacking	Gill	1, 3, 4
· middleboxes	Beverly, Donnet	1, 3
Scientific Modeling & Mapping		
· *inferring accurate maps:*		
· · · alias resolution	Katz-B.	1, 3
· · · exchange point (IXP) addresses	Katz-B.	1, 2, 3
· · · AS relationships	Clark, Crovella, Gill, Goldberg, Katz-B.	1, 2, 3
· · · geolocation	FCC, RIPE NCC	1, 2
· · · fingerprinting	Donnet	1
· modeling of Internet routing	Goldberg, Katz-B.	1, 2
Internet Architecture & Evolution		
· longitudinal studies	Bailey, Clark, Crovella	1, 4
· IPv6	Beverly, Bailey, Donnet	1, 2, 4
· carrier-grade NAT	FCC	1, 3

5.1 Empirical analysis of Internet security and stability vulnerabilities

1. Ark's active measurement capabilities have already enabled researchers to perform **security vulnerability assessments**, including detection of IP address spoofing capability using the spoofer measurement project [19], for which CAIDA is now providing infrastructure support [105]. Researchers have asked to expand the use of Ark to assess vulnerabilities related to traffic surveillance (Goldberg and Caesar LOC), DNS resolver idiosyncrasies that could inhibit DNSSEC deployment (Deccio LOC), and network hygiene (Bailey LOC).
2. Several research groups are improving and extending methods for **detecting and quantifying the impact of wide-area Internet outages** by combining active and passive measurements [31, 106, 107, 108, 109, 110, 111]. Outage detection is inherently sensitive to the vantage points available – more vantage points yield more insight into the nature and scope of an outage. A related body of recent research focuses on **predicting, tracking, and localizing the root cause of Internet path changes** [112, 113, 114, 115, 116], generally relying on PlanetLab

measurement vantage points mostly at academic institutions. Ark's VP diversity provides a complementary, and in some cases completely different, view of Internet topology.

3. All proposed tasks will support study of **performance problems**, including **persistent interdomain congestion** due to peering disputes [117, 118, 119, 120, 121, 122]. Researchers can use Ark to identify source-destination pairs that traverse a given interdomain link, and probe these destinations to discover evidence of congestion along the path (Clark and FCC LOCs) [123, 124]. Researchers are also interested in applying **tomography techniques** [125, 126, 127, 71] to measurements aggregated from many Ark monitors toward a set of destinations can isolate the likely location of congested or failed links. (See Feamster LOC.)
   A related powerful method to support troubleshooting and diagnosis methods is Ethan Katz-Bassett's **reverse traceroute** [128] technology, which he is extending beyond the existing PlanetLab nodes. To support his CRI-funded effort (see LOC), we have integrated specific measurement primitives into scamper that reverse traceroute requires, and obtained permission from a subset of hosting sites to transmit this special class of spoofed packet. These enhancements will mitigate limitations inherent in the reverse traceroute technique, e.g., the 9-hop limit of the IP Record Route option.
4. **Detection and characterization of malicious traffic interception** (hijacking) events requires a combination of passive BGP measurements and active measurements (such as traceroutes). Alberto Dainotti (CAIDA) is collaborating with Phillipa Gill (see LOC) to develop and evaluate novel methodologies to automatically detect traffic interception events and characterize their extent, frequency, and impact. This SATC-funded project [129] requires extending the Ark infrastructure to trigger targeted active measurements when other data sources provided evidence of possible ongoing hijacking events.
5. Luckie has added functionality to scamper to extend his and other previous studies of *TCP and middlebox behavior inference* [95, 94]. Deploying this capability on Ark (Task 3) will enable tracking of TCP evolution over time, a surprisingly rarely documented activity given the revisions to TCP over the last decade, e.g., new congestion control algorithms [130] and connection establishment behaviors [131].
   Rob Beverly (see LOC) at NPS recently proposed adding transparent features to TCP applications that would detect middlebox tampering of IP and TCP headers; he used Ark to test and evaluate his software, but longer-term deployment of his software (HICCUPS) on an expanded Ark infrastructure would enable more evaluation of this powerful technique [132] that could inspire its rapid adoption and standardization.
6. The diversity of RADclock-enabled Ark vantage points in the proposed expansion will allow **health monitoring of the public Internet timing system**, a system that critically depends on stratum-1 NTP servers (the "gold standard") whose accuracy and reliability is unknown. Preliminary work using RADclock suggests that errors in accuracy are widespread, diverse, and sometimes large enough to render network measurements (among other things) meaningless. Darryl Veitch's team (U. Melbourne) is working to detect and report the nature, frequency, magnitude, and possible impacts of errors in this critical sub-system, but essential to his effort, as well as efforts to develop and validate a more accurate public timing system, are a diverse mesh of VPs with precise timing support.

5.2 Scientific modeling and mapping

1. The first three proposed enhancements will allow CAIDA and others to construct **higher fidelity IPv4 and IPv6 router-level topology maps**, including further improving on increasingly successful attempts at router IP address alias resolution [50, 133, 134, 8]. Today's

best available IPv4 router-level maps are constructed using a combination of MIDAR [8], iffinder [51], and kapar [52], but the proposed enhancements will enable researchers to experiment with additional probing techniques developed but not yet investigated at scale in the wild, e.g., [135, 97, 96].

The enhancements described in Task 2 will also allow inferences of the presence of IXPs and CDNs [136] in raw data, and support researchers who want targeted measurements to fill gaps in topology coverage [137, 138, 139] (Crovella LOC). The Ingress Point Spreading (IPS) [89] technique (Section 4.2.1) will enable researchers to estimate the prevalence of multihoming and topological resiliency to network failure.

Finally, operational use of Multiprotocol Label Switching (MPLS) can lead to false router-level links in maps derived from traceroute measurement. Researchers (Donnet LOC) have requested to integrate fingerprinting capabilities [140] to enable annotation of topology maps with MPLS and router/OS meta-data, mitigating the link hiding due to invisible MPLS tunnels [141, 142, 143], as well as informing alias resolution inferences.

2. The first three enhancements also enable **more accurate AS-level topology maps**, annotated with **more accurate AS relationship inferences**. AS-level maps use different data sources (BGP, traceroute, WHOIS, route servers) [90, 99, 100, 144, 145, 146, 147, 148, 136, 93, 149], but researchers would like to use traceroute data to augment AS-level inference capabilities, but struggle with inferential constraints related to sibling ASes [149, 150, 151], third-party addresses [18], and IXPs. We propose to mitigate or remove some of these constraints via Task 2. (Crovella and Goldberg LOC). Finally, while we can now uncover most peering relationships by querying IXP route servers [152], targeted traceroutes (Task 3) are still required to discover many important bilateral peering agreements.
3. Expanding Ark platform will help testing and extending research on **automating the inference of router geolocation** using geographically meaningful strings in DNS hostnames [153] or constraint-based geolocation based on latency and/or inferred distance [154, 155, 156, 157, 158, 159]. This capability would directly support inference of PoP-level maps, of interest to those studying Internet infrastructure resiliency. CAIDA is collaborating with RIPE NCC (see LOC) to leverage each other's efforts in using active measurements to geolocate router resources.
4. Tasks 1 and 3 will enable investigation of open issues with **IPv4 and IPv6 alias resolution techniques**. Ark has deployed the most effective known Internet-scale IPv4 alias resolution technique, MIDAR [8], and was used to develop and test the most effective known IPv6 alias resolution technique (Speedtrap) [16]. But both techniques have open issues because many routers are unresponsive to specific probes, and researchers will be able to use Ark to further advance the accuracy and efficiency of Internet-scale alias resolution.

5.3 Internet architecture and evolution

1. Using **longitudinal measurements**, many researchers are trying to develop a more comprehensive understanding of how the routing system and interconnection patterns of autonomous systems change over a decade or more, to inform new protocol design, understand the economic relationships among Internet stakeholders, and enable fact-based public policy. (See Crovella LOC.) Ark (and its predecessor Skitter) is the longest running global Internet measurement infrastructure serving the research community, providing comprehensive topology measurements for over 15 years.
2. Our investigation of more efficient and intelligent measurement primitives is critical for active measurement experiments in the vastly larger IPv6 address space. Ark's IPv6 capabili-

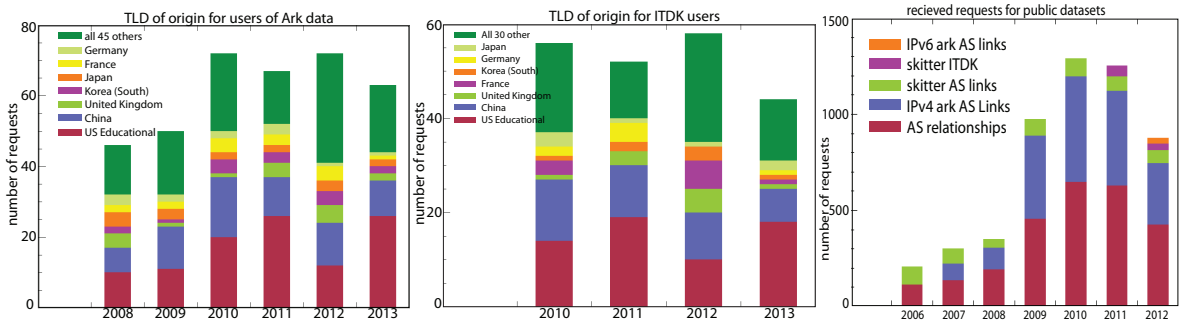
ties will enable the research community to improve the state of **quantitative modeling of the IPv6 transition** by allowing the collection of rigorous empirical data on IPv6 deployment, the relative performance of IPv4 and IPv6 paths to the same destination, and the prevalence and performance impact of the leading alternative to IPv6, i.e., Carrier Grade NAT (see FCC LOC).

3. Ark provides another opportunity to search for evidence of **grey market transfers of IPv4 address blocks**. Initial BGP-based detection methods are suboptimal due to noise in BGP data [160], but reverse DNS mappings and variations in RTT measurements can help reduce false positives in a set of BGP-inferred candidate transfers, as well as potentially detect transfers not revealed by BGP data.
4. The historical data sets and facility for targeted measurements on Ark provide means to **evaluate hypotheses about future Internet architectures**, such as whether named-based forwarding architectures [161] are likely to align well with how topology and naming tend to evolve.

Finally, Ark topology data is a gold mine for student projects (see LOCs): quantifying asymmetry of paths (from the full mesh in and out of Ark nodes); determining whether a sampled topology is representative of a larger network, comparing the effectiveness of algorithms on different topology samples, comparing communications to biological networks [162].

6 Community Outreach and Service

Figure 8 shows the count and geographic distribution (by TLD) of users of all Ark-related data and the Internet Topology Data Kits for the last several years. Our Data Administrator generally responds to data requests within 48 hours, and regularly responds to questions sent to data-info@caida.org. CAIDA maintains mailing lists for researchers who have requested our data as well as a public list for general announcements regarding CAIDA data, and supports a public web forum on DatCat. The forum provides users with a channel to post messages to initiate or respond to topical discussions. The threaded forum structure facilitates and archives historical discussion among data providers and consumers which can then be searched internally or via search engines.



(a) Ark-related data requests (b) ITDK data requests per year (c) Public data requests per year

Figure 8: Distribution of data requests for all Ark-related data, ITDK data set, and public data sets.

Per our usage agreements for each protected dataset, we conduct periodic (at least annual) surveys of our data users to request a summary of research results. We also solicit feedback on the usability of specific datasets (e.g., ITDK), any difficulties users had with the data, and what new datasets researchers would like to analyze. Resources allowing, CAIDA makes custom datasets available to researchers with special requests such as higher resolution timestamps for our traces.

We propose to continue our Active Internet Measurement Systems (AIMS) workshop series, by now a community tradition [28, 163, 164, 165, 166] and important channel for assessing the needs of researchers. We will invite a broad cross-section of CISE and other researchers to these workshops, where we will introduce new capabilities of the infrastructure, review experiences with recent enhancements, and obtain feedback on what capabilities, data formats, and curation functionality would be most helpful to answer specific research questions. We can then customize measurements, data curation, and the query interface to support study of those questions. Our workshops always include a written survey where we solicit additional feedback on presented capabilities and plans.

References

[1] C. Hall, R. Clayton, R. Anderson, and E. Ouzounis, *Inter-X: Resilience of the Internet Interconnection Ecosystem*. European Network and Information Security Agency (ENISA), April 2011. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/inter-x/interx/inter-x.

[2] K. Claffy, Y. Hyun, K. Keys, M. Fomenkov, and D. Krioukov, "Internet Mapping: from Art to Science," in *IEEE DHS Cybersecurity Applications and Technologies Conference for Homeland Security (CATCH)*, March 2009.

[3] Center for Applied Internet Data Analysis, "Archipelago Measurement Infrastructure." http://www.caida.org/projects/ark.

[4] Center for Applied Internet Data Analysis, "Macroscopic Topology Measurements." Research Project. http://www.caida.org/projects/macroscopic/.

[5] http://www.raspberrypi.org/.

[6] D. Veitch, J. Ridoux, and S. B. Korada, "Robust Synchronization of Absolute and Difference Clocks over Networks," *IEEE/ACM Transactions on Networking*, vol. 17, April 2009.

[7] J. Ridoux and D. Veitch, "Principles of Robust Timing Over the Internet," *Communications of the ACM*, vol. 53, May 2010.

[8] K. Keys, Y. Hyun, M. Luckie, and k. claffy, "Internet-Scale IPv4 Alias Resolution with MIDAR," *IEEE/ACM Transactions on Networking*, vol. 21, Apr 2013.

[9] "Ruby Language." http://www.ruby-lang.org/.

[10] M. Luckie, "Scamper: a scalable and extensible packet prober for active measurement of the Internet," in *ACM SIGCOMM Internet Measurement Conference (IMC)*, 2010.

[11] B. Augustin, T. Friedman, and R. Teixeira, "Measuring load-balanced paths in the Internet," in *ACM SIGCOMM Internet measurement Conference (IMC)*, Oct. 2007.

[12] D. Gelernter, "Generative communication in Linda," *ACM Transactions on Programming Languages and Systems*, vol. 7, 1985.

[13] M. Luckie, Y. Hyun, and B. Huffaker, "Traceroute probe method and forward IP path inference," in *ACM SIGCOMM Internet measurement Conference (IMC)*, Oct 2008.

[14] P. Mérindol, B. Donnet, J.-J. Pansiot, M. Luckie, and Y. Huyn, "MERLIN: MEasure the Router Level of the INternet," in *Euro-nf Conference on Next Generation Internet (NGI)*, June 2011.

[15] R. Beverly, W. Brinkmeyer, M. Luckie, and J. Rohrer, "IPv6 Alias Resolution via Induced Fragmentation," in *Passive and Active Network Measurement Conference (PAM)*, Mar 2013.

[16] M. Luckie, R. Beverly, W. Brinkmeyer, and k. claffy, "Speedtrap: Internet-scale ipv6 alias resolution," in *ACM SIGCOMM Internet measurement Conference (IMC)*, Oct 2013.

[17] P. Marchetta, W. de Donato, and A. Pescapé, "Detecting third-party addresses in traceroute traces with IP timestamp option," in *PAM*, pp. 21–30, Apr. 2013.

[18] M. Luckie and k. claffy, "A Second Look at Detecting Third-Party Addresses in Traceroute Traces with the IP Timestamp Option," in *Passive and Active Network Measurement Workshop (PAM)*, vol. 8362, pp. 46–55, Mar 2014.

[19] R. Beverly, A. Berger, Y. Hyun, and k. claffy, "Understanding the efficacy of deployed Internet source address validation filtering," in *ACM SIGCOMM Internet measurement conference (IMC)*, 2009.

[20] kc claffy, "CAIDA participation in IPv6 day," June 2011. http://blog.caida.org/best_available_data/2011/06/05/caida-participation-in-ipv6-day/.

[21] "Vela: On-Demand Topology Measurement Service." http://www.caida.org/projects/ark/vela/.

[22] S. Kalidindi and M. J. Zekauskas, "Surveyor: An infrastructure for Internet performance measurements," in *INET'99*, June 1999.
[23] "Active Measurement Project." `http://amp.nlanr.net/`.
[24] V. Paxson, A. Adams, and M. Mathis, "Experiences with NIMI," in *Passive and Active Measurement*, Apr. 2000.
[25] K. Claffy, T. Monk, and D. McRobb, "Internet Tomography," *Nature, Web Matters*, January 1999. `http://www.nature.com/nature/webmatters/tomog/tomog.html`.
[26] D. G. Andersen, H. Balakrishnan, M. F. Kaashoek, and R. Morris, "Resilient overlay networks," in *ACM Symposium on Operating Systems Principles*, 2001.
[27] k. claffy, M. Crovella, T. Friedman, C. Shannon, and N. Spring, "Community-Oriented Network Measurement Infrastructure (CONMI) Workshop Report," *ACM SIGCOMM Computer Communication Review (CCR)*, vol. 36, Apr 2006.
[28] k. claffy, M. Fomenkov, E. Katz-Bassett, R. Beverly, B. Cox, and M. Luckie, "The Workshop on Active Internet Measurements (AIMS) Report," *ACM SIGCOMM Computer Communication Review (CCR)*, vol. 39, Oct 2009.
[29] L. Peterson, T. Anderson, D. Culler, and T. Roscoe, "A blueprint for introducing disruptive technology into the Internet," in *Hotnets*, 2002.
[30] H. Madhyastha, T. Isdal, M. Piatek, C. Dixon, T. Anderson, A. Krishnamurthy, and A. Venkataramani, "iPlane: an information plane for distributed services," in *Symposium on Operating Systems Design and Implementation (OSDI)*, 2006.
[31] E. Katz-Bassett, H. V. Madhyastha, J. P. John, A. Krishnamurthy, and T. Anderson, "Studying black holes in the Internet with Hubble," in *USENIX Symposium on Networked Systems Design & Implementation (NSDI)*, 2008.
[32] "PlanetLab Acceptable Use Policy," 2013. `http://planet-lab.org/aup`.
[33] L. Peterson, "Understanding and Resolving Conflicts on PlanetLab," 2008. `http://www.cs.princeton.edu/~llp/policy.pdf`.
[34] Srikanth Sundaresan and Sam Burnett and Nick Feamster and Walter de Donato, "BISmark: A Testbed for Deploying Measurements and Applications in Broadband Access Networks," 2014.
[35] S. Sundaresan, N. Feamster, R. Teixeira, and N. Magharei, "Measuring and mitigating web performance bottlenecks in broadband access networks," in *ACM SIGCOMM Internet Measurement Conference*, October 2013.
[36] S. Roy and N. Feamster, "Characterizing correlated latency anomalies in broadband access networks," in *Proceedings of the 2013 ACM SIGCOMM Conference*, 2013.
[37] RIPE Labs, Robert Kisteleki, "RIPE Atlas," 2011. `http://atlas.ripe.net`.
[38] Y. Shavitt and E. Shir, "DIMES: Let the Internet measure itself," *ACM SIGCOMM Computer Communication Review (CCR)*, vol. 35, October 2005.
[39] K. Chen, D. R. Choffnes, R. Potharaju, Y. Chen, F. E. Bustamante, D. Pei, and Y. Zhao, "Where the Sidewalk Ends: Extending the Internet AS Graph Using Traceroutes from P2P Users," in *CoNEXT*, 2009.
[40] D. R. Choffnes and F. E. Bustamante, "Taming the torrent: a practical approach to reducing cross-isp traffic in peer-to-peer systems," *ACM SIGCOMM Computer Communication Review (CCR)*, vol. 38, no. 4, 2008.
[41] 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," *USENIX Symposium on Networked Systems Design & Implementation (NSDI)*, 2013.
[42] D. R. Choffnes, F. E. Bustamante, and Z. Ge, "Crowdsourcing service-level network event monitoring," in *ACM SIGCOMM*, 2010.

[43] M. Dhawan, J. Samuel, R. Teixeira, C. Kreibich, M. Allman, and V. Paxson, "The Fathom Firefox Extension: A Browser-based Network Measurement Platform," in *ACM SIGCOMM Internet Measurement Conference (IMC)*, 2012.

[44] C. Kreibich, N. Weaver, B. Nechaev, and V. Paxson, "Netalyzr: illuminating the edge network," in *ACM SIGCOMM Internet Measurement Conference (IMC)*, 2010.

[45] R. Oliveira, "UCLA's IRL Internet Topology Collection," July 2009. http://irl.cs.ucla.edu/topology/.

[46] Center for Applied Internet Data Analysis (CAIDA), "The IPv4 Routed /24 Topology Dataset." http://www.caida.org/data/active/ipv4_routed_24_topology_dataset.xml.

[47] CAIDA's Macroscopic Internet Topology Data Kit (ITDK). http://www.caida.org/data/active/internet-topology-data-kit/.

[48] B. Huffaker, A. Dhamdhere, M. Fomenkov, and k. claffy, "Toward topology dualism: Improving the accuracy of AS annotations for routers," in *Passive and Active Network Measurement Conference (PAM)*, Apr. 2010.

[49] K. Keys, "Internet-Scale IP Alias Resolution Techniques," *ACM SIGCOMM Computer Communication Review (CCR)*, vol. 40, pp. 50–55, Jan 2010.

[50] A. Bender, R. Sherwood, and N. Spring, "Fixing Ally's Growing Pains with Velocity Modeling," in *ACM SIGCOMM Internet measurement Conference (IMC)*, 2009. http://www.cs.umd.edu/ bender/radargun/.

[51] K. Keys, "iffinder ipv4 alias resolution tool," 2001. http://www.caida.org/tools/measurement/iffinder/.

[52] K. Keys, "kapar Alias Resolution Tool," 2012. http://www.caida.org/tools/measurement/kapar/.

[53] "University of Oregon Route Views Project." http://www.routeviews.org/.

[54] Center for Applied Internet Data Analysis (CAIDA), "AS links." http://www.caida.org/data/active/ipv4_routed_topology_aslinks_dataset.xml.

[55] Center for Applied Internet Data Analysis (CAIDA), "Prefix to AS mappings." http://www.caida.org/data/routing/routeviews-prefix2as.xml.

[56] Center for Applied Internet Data Analysis (CAIDA), "AS Taxonomy." http://www.caida.org/data/active/as_taxonomy/.

[57] Center for Applied Internet Data Analysis (CAIDA), "AS Relationships BGP-inferred." http://www.caida.org/data/active/as-relationships/index.xml.

[58] P. Mahadevan, D. Krioukov, M. Fomenkov, B. Huffaker, X. Dimitropoulos, and kc claffy, "Lessons from three views of the internet topology: Technical report," tech. rep., UC, San Diego, 2005. http://www.caida.org/publications/papers/2005/tr-2005-02/.

[59] B. Huffaker, M. Fomenkov, and k. claffy, "Internet Topology Data Comparison," tech. rep., Center for Applied Internet Data Analysis (CAIDA), May 2012.

[60] Center for Applied Internet Data Analysis (CAIDA), "Papers Published (by non-CAIDA Authors Using CAIDA Datasets." http://www.caida.org/data/publications/.

[61] G. Yan, S. Eidenbenz, S. Thulasidasan, P. Datta, and V. Ramaswamy, "Criticality analysis of Internet infrastructure," *Computer Networks*, vol. 54, May 2010.

[62] W. Deng, M. Karaliopoulos, W. Mühlbauer, P. Zhu, X. Lu, and B. Plattner, "k-Fault tolerance of the Internet AS graph," *Computer Networks*, vol. 55, no. 10, 2011.

[63] A. Haeberlen, I. Avramopoulos, J. Rexford, and P. Druschel, "NetReview: Detecting when interdomain routing goes wrong," in *USENIX Symposium on Networked Systems Design & Implementation (NSDI)*, Apr 2009.

[64] Min Suk Kang and Virgil Gilgor, "Routing Bottlenecks in the Internet - Causes, Exploits, and Countermeasures," tech. rep., Carnegie Mellon University, 2014. http://repository.cmu.edu/cylab/133/.

[65] Andrew D. Ferguson and Jordan Place and Rodrigo Fonseca, "Growth Analysis of a Large ISP," in *ACM SIGCOMM Internet measurement Conference (IMC)*, Oct 2013.

[66] M. Chowdhury, R. Agarwal, V. Sekar, and I. Stoica, "A longitudinal and cross-dataset study of internet latency and path stability," Tech. Rep. UCB/EECS-2014-172, EECS Department, UC, Berkeley, Oct 2014.

[67] Mario A. Sanchez and Fabian E. Bustamante and Balachander Krishnamurthy and Walter Willinger and Georgios Smaragdakis and Jeffrey Erman, "Inter-Domain Traffic Estimation for the Outsider," in *ACM SIGCOMM Internet measurement Conference (IMC)*, Nov 2014.

[68] Bruce Maggs, "Mapping the Whole Internet," tech. rep., Duke University, 2014. http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2\&doc=GetTRDoc.pdf\&AD=ADA603795.

[69] P. Marchetta, P. Mérindol, B. Donnet, A. Pescapè, and J.-J. Pansiot, "Topology Discovery at the Router Level: A New Hybrid Tool Targeting ISP Networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 9, 2011.

[70] Marchetta, Pietro and Mérindol, Pascal and Donnet, Benoit and Pescapé, Antonio and Pansiot, Jean-Jacques, "Quantifying and mitigating IGMP filtering in topology discovery," in *IEEE Global Communications Conference (GLOBECOM)*, 2012.

[71] Liang Ma and Ting He and Ananthram Swami and Don Towsley and Kin K. Leung and and Jessica Lowe, "Node Failure Localization via Network Tomography," in *ACM SIGCOMM Internet measurement Conference (IMC)*, Nov 2014.

[72] J. Juen, A. Das, A. Johnson, N. Borisov, and M. Caesar, "Defending Tor from Network Adversaries: A Case Study of Network Path Prediction," *ArXiv e-prints*, Oct. 2014.

[73] David Reed and Donny Warbritton and Douglas Sicker, "Current Trends and Controversies in Internet Peering and Transit: Implications for the Future Evolution of the Internet," in *Telecommunications Policy Research Conference (TPRC)*, 2014.

[74] M. Wachs, C. Grothoff, and R. Thurimella, "Partitioning the Internet," in *International Conference on Risk and Security of Internet and Systems (CRiSIS)*, pp. 1–8, 2012.

[75] Y. Liu, B. Dai, P. Zhu, and J. Su, "Whom to Convince? It Really Matters in BGP Prefix Hijacking Attack and Defense," in *Future Information Technology* (J. J. Park, L. Yang, and C. Lee, eds.), vol. 184 of *Communications in Computer and Information Science*, 2011.

[76] Y. Liu, B. Zhang, W. Fei, and J. Su, "Evaluation of Prefix Hijacking Impact Based on Hinge-Transmit Property of BGP Routing System.," *Journal of Next Generation Information Technology (JNIT)*, vol. 1, no. 3, 2010.

[77] W. Deng, P. Zhu, N. Xiong, Y. Xiao, and X. Hu, "How resilient are individual ASes against AS-level link failures?," in *Workshop on Security in Computers, Networking and Communications (SCNC)*, 2011.

[78] V. Kambhampati, C. Papadopoulos, and D. Massey, "Epiphany: A location hiding architecture for protecting critical services from DDoS attacks.," in *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2012.

[79] M. D. D. Moreira, R. P. Laufer, N. C. Fernandes, and O. C. M. B. Duarte, "A Stateless Traceback Technique for Identifying the Origin of Attacks from a Single Packet," in *IEEE International Conference on Communications (ICC)*, 2011.

[80] M. Youssef, R. Kooij, and C. Scoglio, "Viral conductance: Quantifying the robustness of networks with respect to spread of epidemics," *Journal of Computational Science*, vol. 2, 2011.

[81] J. Parker and A. Boedihardjo, "Evidence of spatial embedding in the IPv4 router-level Internet network," *ArXiv e-prints*, Oct. 2014.
[82] M. Boguñá, F. Papadopoulos, and D. V. Krioukov, "Sustaining the Internet with Hyperbolic Mapping," *Nature Communications*, vol. 1.
[83] F. Papadopoulos, C. Psomas, and D. V. Krioukov, "Replaying the Geometric Growth of Complex Networks and Application to the AS Internet," *ACM SIGMETRICS Performance Evaluation Review*, vol. 40, no. 3, 2012.
[84] M. Yu, W. Jiang, H. Li, and I. Stoica, "Tradeoffs in CDN designs for throughput oriented traffic," in *ACM CoNEXT*, 2012.
[85] R. Durairajan, S. Ghosh, X. Tang, P. Barford, and B. Eriksson, "Internet Atlas: A Geographic Database of the Internet," in *ACM HotPlanet Workshop*, August 2013.
[86] R. Durairajan, J. Sommers, and P. Barford, "Layer 1-Informed Internet Topology Measurement," in *ACM SIGCOMM Internet measurement Conference (IMC)*, November 2014.
[87] National Science Foundation, "NSF Future Internet Architecture Projects," 2013. `http://www.nets-fia.net/`.
[88] R. Beverly, A. Berger, and G. G. Xie, "Primitives for Active Internet Topology Mapping: Toward High-Frequency Characterization," in *ACM SIGCOMM Internet measurement Conference (IMC)*, Nov. 2010.
[89] G. Baltra, R. Beverly, and G. G. Xie, "Ingress Point Spreading: A New Primitive for Adaptive Active Network Mapping," in *Passive and Active Network Measurement Conference (PAM)*, Mar. 2014.
[90] Y. Hyun, A. Broido, and kc claffy, "On Third-party Addresses in Traceroute Paths," in *Passive and Active Network Measurement Workshop (PAM)*, PAM, Apr 2003.
[91] B. Huffaker, M. Fomenkov, M. Luckie, and kc claffy, "Visualizing IPv4 and IPv6 Internet Topology at a Macroscopic Scale," 2013. `http://www.caida.org/research/topology/as_core_network/`.
[92] "PeeringDB Peering Database." `http://www.peeringdb.com`.
[93] Y. Zhang, R. Oliveira, H. Zhang, and L. Zhang, "Quantifying the Pitfalls of Traceroute in AS Connectivity Inference," in *Passive and Active Measurement Conference*, 2010.
[94] A. Medina, M. Allman, and S. Floyd, "Measuring the Evolution of Transport Protocols in the Internet"," *ACM SIGCOMM Computer Communication Review*, vol. 35, Apr. 2005.
[95] M. Luckie and B. Stasiewicz, "Measuring path MTU discovery behaviour," in *ACM SIGCOMM Internet Measurement Conference (IMC)*, 2010.
[96] CAIDA, "motu IPv4 address dealiasing tool." `http://www.caida.org/tools/measurement/motu/`.
[97] J. Sherry, E. Katz-Bassett, M. Pimenova, H. V. Madhyastha, T. Anderson, and A. Krishnamurthy, "Resolving IP aliases with prespecified timestamps," in *ACM SIGCOMM Internet Measurement Conference (IMC)*, 2010.
[98] Y. Hyun, A. Broido, and kc claffy, "Traceroute and BGP AS path incongruities," tech. rep., Center for Applied Internet Data Analysis, 2003. `http://www.caida.org/outreach/papers/2003/ASP/`.
[99] Z. M. Mao, J. Rexford, J. Wang, and R. Katz, "Towards an accurate AS-level traceroute tool," in *ACM SIGCOMM*, Sept. 2003.
[100] Z. Mao, D. Johnson, J. Rexford, J. Wang, and R. Katz, "Scalable and Accurate Identification of AS-level Forwarding Paths," in *IEEE INFOCOM*, March 2004.
[101] R. NCC, "RIPE Statistics," 2013. `https://stat.ripe.net/`.
[102] A. King, A. Dainotti, B. Huffaker, and k. claffy, "A Coordinated View of the Temporal Evolution of Large-scale Internet Events," *Computing*, Jan 2013.

[103] "NSF CNS-1228994: Detection and analysis of large-scale Internet infrastructure outages (IODA)." http://www.caida.org/funding/ioda/.
[104] "Apache Spark." https://spark.apache.org.
[105] M. Luckie, R. Beverly, K. Keys, and kc claffy, "Spoofer Project," 2014. http://spoofer.caida.org.
[106] A. Schulman and N. Spring, "Pingin' in the rain," in *ACM SIGCOMM Internet Measurement Conference (IMC)*, 2011.
[107] A. Dainotti, C. Squarcella, E. Aben, K. Claffy, M. Chiesa, M. Russo, and A. Pescap?, "Analysis of Country-wide Internet Outages Caused by Censorship," in *Internet Measurement Conference (IMC)*, (Berlin, Germany), pp. 1–18, ACM, Nov 2011.
[108] A. Dainotti, R. Amman, E. Aben, and K. Claffy, "Extracting benefit from harm: using malware pollution to analyze the impact of political and geophysical events on the Internet," *SIGCOMM Comput. Commun. Rev.*, vol. 42, January 2013.
[109] L. Quan, J. Heidemann, and Y. Pradkin, "Towards Active Measurements of Edge Network Outages," in *Passive and Active Measurement*, 2013.
[110] L. Quan, J. Heidemann, and Y. Pradkin, "Trinocular: Understanding Internet Reliability Through Adaptive Probing," in *ACM SIGCOMM*, August 2013.
[111] X. Fan and J. Heidemann, "Selecting representative IP addresses for internet topology studies," in *ACM SIGCOMM Internet measurement Conference (IMC)*, 2010.
[112] I. Cunha, R. Teixeira, N. Feamster, and C. Diot, "Measurement methods for fast and accurate blackhole identification with binary tomography," in *ACM SIGCOMM Internet Measurement Conference (IMC)*, 2009.
[113] I. Cunha, R. Teixeira, and C. Diot, "Measuring and Characterizing End-to-End Route Dynamics in the Presence of Load Balancing," in *Passive and Active Measurement Conference*, April 2011.
[114] I. Cunha, R. Teixeira, D. Veitch, and C. Diot, "Predicting and tracking Internet path changes," in *ACM SIGCOMM*, 2011.
[115] U. Javed, I. Cunha, D. R. Choffnes, E. Katz-Bassett, T. Anderson, and A. Krishnamurthy, "PoiRoot: Investigating the root cause of interdomain path changes," in *ACM SIGCOMM*, August 2013.
[116] E. Katz-Bassett, C. Scott, D. R. Choffnes, I. Cunha, V. Valancius, N. Feamster, H. V. Madhyastha, T. E. Anderson, and A. Krishnamurthy, "LIFEGUARD: practical repair of persistent route failures," in *ACM SIGCOMM*, 2012.
[117] EURESCOM, "Cdn interconnection," 2010. http://www.ist-daidalos.org/Public/Projects/P1900-series/P1955/default.asp.
[118] Cogent Communications, "Public consultation on the open internet and net neutrality in europe: Contribution by cogent communications," 2010. http://ec.europa.eu/information_society/policy/ecomm/doc/library/public_consult/net_neutrality/comments/01operators_isps/cogent_communications.pdf.
[119] Free, "Response by Free to Public Consultation on the Open Internet and Net Neutrality in Europe," 2010. http://ec.europa.eu/information_society/policy/ecomm/doc/library/public_consult/net_neutrality/comments/01operators_isps/free_iliad.pdf.
[120] K. Bode, "'free ride' google working with telcos on congestion: France telecom states talks underway about prioritized access," 2011. http://www.dslreports.com/shownews/Free-Ride-Google-Working-With-Telcos-on-Congestion-114645.
[121] Backdoor Santa, "Some Truth About Comcast - WikiLeaks Style," 2010. http://www.merit.edu/mail.archives/nanog/msg15911.html.

[122] W. Norton, "The emerging 21st century access power peering," *Communications And Strategies*, vol. 84, pp. 55–73, 2011.
[123] Matthew Luckie and Amogh Dhamdhere and David Clark and Bradley Huffaker and kc claffy, "Challenges in Inferring Internet Interdomain Congestion," in *ACM SIGCOMM Internet measurement Conference (IMC)*, 2014.
[124] D. Clark, S. Bauer, k. claffy, A. Dhamdhere, B. Huffaker, W. Lehr, and M. Luckie, "Measurement and Analysis of Internet Interconnection and Congestion," in *Telecommunications Policy Research Conference (TPRC)*, Sep 2014.
[125] N. Duffield, "Network tomography of binary network performance characteristics," *IEEE Transactions on Information Theory*, vol. 52, p. 2006, 2006.
[126] A. Dhamdhere, R. Teixeira, C. Dovrolis, and C. Diot, "NetDiagnoser: Troubleshooting Network Unreachabilities Using End-to-end Probes and Routing Data," in *ACM CoNEXT*, 2007.
[127] S. Zarifzadeh, M. G K, and C. Dovrolis, "Range tomography," in *Proceedings of the 12th ACM SIGMETRICS/PERFORMANCE joint international conference on Measurement and Modeling of Computer Systems*, SIGMETRICS '12, (New York, NY, USA), pp. 389–390, ACM, 2012.
[128] E. Katz-Bassett, H. V. Madhyastha, V. K. Adhikari, C. Scott, J. Sherry, P. Van Wesep, T. Anderson, and A. Krishnamurthy, "Reverse traceroute," in *USENIX Symposium on Networked Systems Design & Implementation (NSDI)*, 2010.
[129] Alberto Dainotti and Phillipa Gill, "NSF CNS-1423659. HIJACKS: Detecting and Characterizing Internet Traffic Interception based on BGP Hijacking," 2014. `http://www.caida.org/funding/hijacks/`.
[130] I. R. Sangtae Ha and L. Xu, "CUBIC: A new TCP-friendly high-speed TCP variant," *ACM SIGOPS Operating System Review*, vol. 32, pp. 64–74, June 2008.
[131] N. Dukkipati, T. Refice, Y. Cheng, J. Chu, T. Herbert, A. Agarwal, A. Jain, and N. Sutin, "An argument for increasing TCP's initial congestion window," *CCR*, vol. 40, July 2010.
[132] R. Craven, R. Beverly, and M. Allman, "Detecting packet header manipulations with HICCUPS," in *Proceedings of the 2014 ACM SIGCOMM Conference*, 2013.
[133] S. Garcia-Jimenez, E. Magana, M. Izal, and D. Morato, "Validity of Router Responses for IP Aliases Resolution," in *Passive and Active Measurement Conference*, 2012.
[134] L. Spinelli, M. Crovella, and B. Eriksson, "Aliascluster: A lightweight approach to interface disambiguation," in *INFOCOM*, 2013.
[135] R. Sherwood, A. Bender, and N. Spring, "Discarte: A disjunctive Internet cartographer," in *ACM SIGCOMM*, 2008.
[136] B. Augustin, B. Krishnamurthy, and W. Willinger, "IXPs: mapped?," in *Proceedings of the 9th ACM SIGCOMM conference on Internet measurement conference*, IMC '09, pp. 336–349, 2009.
[137] B. Eriksson, P. Barford, J. Sommers, and R. Nowak, "Inferring Unseen Components of the Internet Core," *IEEE Journal on Selected Areas in Communications (JSAC)*, vol. 29, no. 9, 2011.
[138] T. Bourgeau and T. Friedman, "Efficient IP-Level Network Topology Capture," *Passive and Active Measurement*, 2013.
[139] B. Eriksson, G. Dasarathy, P. Barford, and R. Nowak, "Efficient network tomography for Internet topology discovery," *IEEE/ACM Transactions on Networking*, vol. 20, June 2012.
[140] Y. Vanaubel, J.-J. Pansiot, P. Merindol, and B. Donnet, "Network Fingerprinting: TTL-based Router Signatures," in *ACM SIGCOMM Internet measurement Conference (IMC)*, Oct 2013.
[141] J. Sommers, B. Eriksson, and P. Barford, "On the prevalence and characteristics of MPLS deployments in the open Internet," in *ACM SIGCOMM Internet measurement Conference (IMC)*, Nov. 2011.
[142] B. Donnet, M. Luckie, P. Mérindol, and J.-J. Pansiot, "Revealing MPLS Tunnels Obscured from Traceroute," *ACM SIGCOMM Computer Communications Review*, April 2012.

[143] A. Dhamdhere, "False IP links due to MPLS opaque tunnels," 2013. email amogh@caida.org for copy.
[144] P. Mahadevan, D. Krioukov, M. Fomenkov, B. Huffaker, X. Dimitropoulos, kc claffy, and A. Vahdat, "The Internet AS-Level Topology: Three Data Sources and One Definitive Metric," *ACM SIGCOMM Computer Communications Review*, vol. 36, no. 1, 2006.
[145] R. Bush, O. Maennel, M. Roughan, and S. Uhlig, "Internet optometry: assessing the broken glasses in Internet reachability," in *ACM SIGCOMM Internet Measurement Conference (IMC)*, 2009.
[146] G. Gürsun, N. Ruchansky, E. Terzi, and M. Crovella, "Inferring visibility: who's (not) talking to whom?," in *ACM SIGCOMM*, 2012.
[147] R. Oliveira, D. Pei, W. Willinger, B. Zhang, and L. Zhang, "The (In)completeness of the observed Internet AS-level structure," *IEEE/ACM Transactions on Networking*, vol. 18, 2010.
[148] Y. Zhang, Z. Zhang, Z. M. Mao, Y. C. Hu, and B. M. Maggs, "On the Impact of Route Monitor Selection," in *ACM SIGCOMM Internet Measurement Conference*, 2007.
[149] M. Luckie, B. Huffaker, A. Dhamdhere, V. Giotsas, and k. claffy, "AS Relationships, Customer Cones, and Validation," in *ACM SIGCOMM Internet Measurement Conference (IMC)*, Oct 2013.
[150] B. Huffaker, K. Keys, M. Fomenkov, and K. Claffy, "AS-to-Organization Dataset." `http://www.caida.org/research/topology/as2org`.
[151] Y. Zhang, R. Oliveira, Y. Wang, S. Su, B. Zhang, J. Bi, H. Zhang, and L. Zhang, "A Framework to Quantify the Pitfalls of Using Traceroute in AS-Level Topology Measurement," *IEEE Journal on Selected Areas in Communications special issue on Internet topology*, October 2011.
[152] V. Giotsas, S. Zhou, M. Luckie, and k claffy, "Inferring multilateral peering," in *CoNEXT*, Dec. 2013.
[153] J. Chabarek and P. Barford, "What's in a Name? Decoding Router Interface Names," in *ACM HotPlanet Workshop*, August 2013.
[154] Y. Shavitt and N. Zilberman, "Improving IP Geolocation by Crawling the Internet PoP Level Graph," in *Networking*, 2013.
[155] Y. Shavitt and N. Zilberman, "A Structural Approach for PoP Geolocation," *Proceedings of the 2010 IEEE INFOCOM Conference*, 2010.
[156] A. H. Rasti, N. Magharei, R. Rejaie, and W. Willinger, "Eyeball ASes: from geography to connectivity," in *ACM SIGCOMM Internet Measurement Conference (IMC)*, 2010.
[157] Z. Hu and J. Heidemann, "Towards Geolocation of Millions of IP Addresses," in *ACM SIGCOMM Internet Measurement Conference (IMC)*, 2012.
[158] Y. Wang, D. Burgener, M. Flores, A. Kuzmanovic, and C. Huang, "Towards street-level client-independent IP geolocation," in *USENIX Symposium on Networked Systems Design & Implementation (NSDI)*, 2011.
[159] B. Huffaker, M. Fomenkov, and kc claffy, "Geocompare: a comparison of public and commercial geolocation databases," tech. rep., Center for Applied Internet Data Analysis, 2011. `http://www.caida.org/publications/papers/2011/geocompare-tr/`.
[160] I. Livadariu, A. Elmokashfi, A. Dhamdhere, and kc claffy, "A first look at IPv4 transfer markets," in *CoNEXT*, 2013.
[161] "Named Data Networking Architecture Research Project," 2010. `http://named-data.net/techreport/TR001ndn-proj.pdf`.
[162] C. Partridge, "Forty data communications research questions," *SIGCOMM Comput. Commun. Rev.*, vol. 41, Oct. 2011.
[163] kc claffy, E. Aben, J. Augé, R. Beverly, F. Bustamante, B. Donnet, T. Friedman, M. Fomenkov, P. Haga, M. Luckie, and Y. Shavitt, "The 2nd Workshop on Active Internet Measurements

(AIMS-2) Report," *ACM SIGCOMM Computer Communication Review (CCR)*, vol. 40, Oct. 2010.
[164] kc claffy, "The 3rd Workshop on Active Internet Measurements (AIMS-3) Report," *ACM SIGCOMM Computer Communication Review (CCR)*, vol. 41, July 2011.
[165] kc claffy, "The 4th Workshop on Active Internet Measurements (AIMS-4) Report," *ACM SIGCOMM Computer Communication Review (CCR)*, vol. 42, Jul 2012.
[166] kc claffy, "The 5th Workshop on Active Internet Measurements (AIMS-5) Report," *ACM SIGCOMM Computer Communication Review (CCR)*, vol. 43, Jul 2013.