Skylines: Demystifying Network Resource Islands with Virtual Landmarks

ABSTRACT

"Do you see what I see?" The vastness of today's Internet creates an intuitive but often overlooked phenomenon: not everyone is exposed to the same web resources. Even across the set of objects embedded in a single web page, a pair of clients with apparently similar network properties may assigned to barely overlapping sets of network resources to pull from. While the properties of individual content distribution networks (CDNs) and the like are well explored, there has been, until now, a lack of insight regarding the *aggregate* behavior of these many large networks co-existing.

In this paper, we perform the first, deep analysis of cross-provider resource allocation patterns and the resulting aggregate mapping of over 10,000 RIPE Atlas clients around the world. To facilitate our research, we introduce common network resource exposure (CNRE) - a measure of the degree to which a pair of clients are exposed to the same network destinations as each other across a large set of domains. We explore the implications of high and low CNRE scores, and assess the applicability of well established network properties (country, ASN, BGP prefix, and /24) in estimating CNRE. Our findings expose clients that are poorly served by their current position in this aggregate mapping scheme and highlight the existence of "outlier" CDNs, who allocate their resources in a way that goes against broader Internet trends.

1 INTRODUCTION

"What's in a name?" — in the context of networking, quite a lot! IP addresses and prefixes indicate to routers where particular interfaces or subnets reside in the greater Internet [**?**]. Domain names offer a simple, human-readable overlay for the complicated, often multiplexed addressing scheme underneath [**?**]. Autonomous system (AS) numbers often help to distingish one network from another [**?**]. Names and labels such as these, whatever form they take, allow us to organize immense network spaces with manageable and descriptive abstractions.

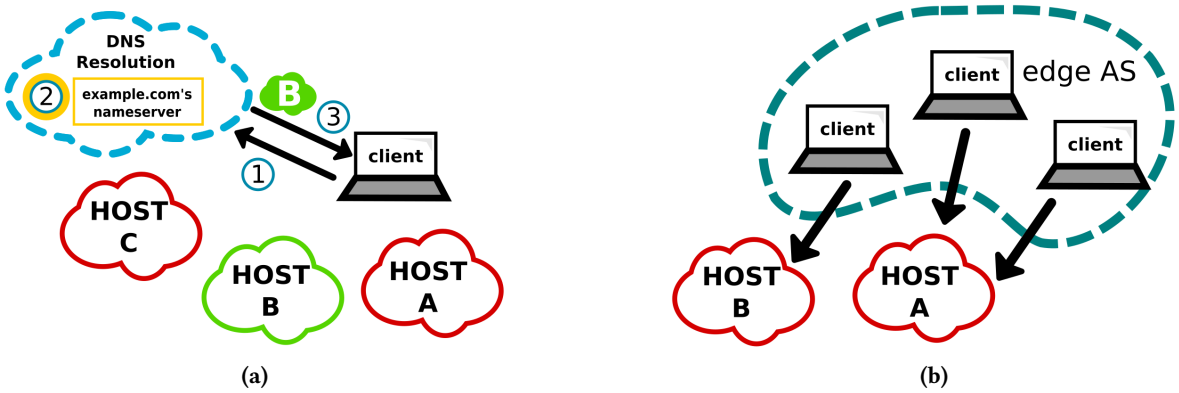
Unfortunately, a single name is often not enough. One machine can be described in terms of all of the examples listed above, and more. This is because it is important that names carry information relavant to the specific way in which they will be used. Routers are unable to direct traffic with domain names, just as humans cannot be expected to remember the plethora IP addresses they access every day. While it is intuitive that no labeling system is applicable across all possible dimensions, in practice, this fact is often taken for granted or neglected entirely.

In this project, we challenge the careless application of conventional client labeling schemes in Internet measurement experiments, particulary those subject to the effects of DNS redirection and CDN PoP (point of presence) catchment formation. we uncover and quantify the degree of misalignment between experimentally determined aggregate catchments and labels often assumed to indicate "similarity" between clients — country, AS number, announced BGP prefix, and /24 subnet — and use this to design the Skyline model, a grouping system which describes clients' relative distances from each other in terms of their *common network resource exposure* (CNRE). Describing clients in such terms highlights what should be a chief concern in large scale Internet measurement platforms and network optimization efforts: the sets of clients actually being directed the same resources.

In order to develop the Skyline model, we performed an exhaustive set of measurements to frame client experience on a per *site* basis. In our completed, preliminary work, we capture a snapshot of both DNS resolutions and latency measurements toward the 304 domains that appeared most frequently in the top 2441 most popular webpages. Our measurements span over 10,000 unique clients spread across 185 countries and 3637 autonomous systems. we performed over 52 million pairwise comparisons with the results of these measurements to arrive at the foundation of what we have coined the "Skyline model".

With this project, we make the following contributions, including those we expect to stem from proposed work, which we have designated with (*p*)

- we perform a large exploration of client network performance on a per webpage level. Our raw results are publically available on the RIPE Atlas platform.
- (*p*) we quantify the degree of misalignment between conventional grouping schemes and aggregate catchments.
- (*p*) we introduce the Skyline model, a client grouping scheme that reflects the extent of CNRE.
- (*p*) Using the Skyline model, we identify and analyze network resource islands — sets of clients with very high degrees CNRE.



(a) (b)

Figure 1: Illustration of network resource resource allocation. Subfigure 1a shows DNS resolution at a high level: 1) The client deploys a DNS query for example.com. 2) This query ultimately reaches nameserver responsible for example.com and decides which of example.com's network resources should serve the client. 3) The nameserver's resource selection is returned to the client. Subfigure 1b shows an example of how clients with similarly described locations may be directed to distinct network resources.

2 PROBLEM SPACE AND RELATED WORK

This projects aims to gain an understanding of which clients are directed to the same set of resources across many distinct domains. Its most direct and immediate use case is influencing probe selection in large scale Internet measurements. For researchers, likely unaware of the relatively hidden allocation schemes of the wide array of CDN platforms and other large content distributors, it is difficult to determine, a priori, the degree of similarity between clients. Knowledge of whether there is a high probability that a pair of clients are being directed to altogether different resources may be significant to their experiment design. This approach to experiment design is in line with RIPE Atlas, one of the largest client based measurement platforms, which maintains an exhaustive set of tags on all of their clients in order to help researchers and network operators filter and refine the set selected for their experiment [**?**]. Further, more abstract applications may include, but are not limited to, distributed denial of service mitigation [**?**] and CDN node deployment [**? ?**].

The most similar body of related work involves anycast CDN catchment analysis, which aims to investigate the set of clients routed towards particular CDN points of presence (PoPs) [**? ? ?**]. Our work differs significantly in scope: to our knowledge, we are the first investigate what we refer to as *aggregate catchments*, the joint behavior of many anycast CDN catchments and unicast CDN targets, spread across many content distribution platforms. Conversely, this related body work either focuses on individual platforms or specific services [**? ? ?**].

Several authors have attempted to discover the topology of large CDN platforms through large scale measurement studies [**? ? ?**]. While their findings are potentially of use in this project, their goals and contributions run parallel to what we aim to accomplish. They seek to identify the properties and locations of CDN resources; conversely, we seek to identify the target pools (sets of clients) of overlapping CDN resource catchments [**? ? ?**]. Other work close to this space investigates the performance of a particular CDN deployment scheme [**?**].

3 EXPERIMENT & DATA COLLECTION

The main preliminary steps performed to enable our work are twofold: 1) domain name collection and 2) per-provider performance measurement. The remainder of this section details these steps and the reasoning behind them while providing context with which to view results presented throughout this paper.

3.1 Definitions

As our aim in this paper is to explore the cross-provider behavior of Internet resource-to-client mapping schemes, it is necessary to first establish what qualifies as "cross-provider" and what sort of cross-provider behavior is of relevance. For example, the reader may have observed that, if a pair of providers are not used in *together* for a given online experience, there is no reason not to keep their analyses separate. For the purposes of this paper, we choose to focus on the providers of webpage objects, which are known to often span a multitude of providers CITE. Previous work has well documented the impact of individual, slow loading objects on

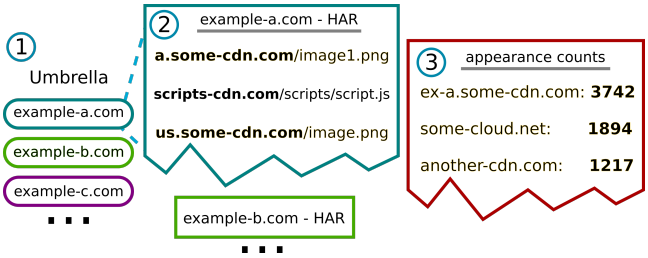


Figure 2: Diagram illustrating domain name collection: 1) Domains from the Umbrella top 1-million were loaded via Google Chrome to identify human-targeted websites. 2) For each human-targeted website's landing page, a HAR file was recorded. 3) Domains were extracted from HAR data and ranked by the number of times observed.

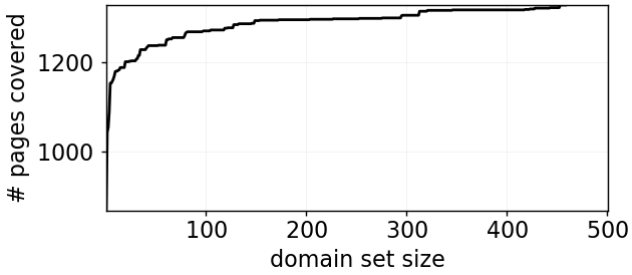


Figure 3: The number of sites containing an object hosted by a domain in our set vs the size of our set of domains.

page load time CITE. To this end, we target domains which we empirically found to co-inhabit large numbers of webpages as web object hosts. Throughout this paper, we equate "domain" to "host" or "provider", recognizing, however, that it is often the case that a single provider will use several domain aliases.

Likewise, we also note here that our use of the term "[web] resource" is deliberately ambiguous: the explicit implementation method used by each provider — ranging from a single subnet per geographic point-of-presence to a number of software-partitioned subnets per machine — is opaque and beyond the scope of this paper. Our chief concern is that an identifiable distinction is made between the set of targets (IP addresses) provided in DNS answers: the sheer fact that they are not labeled as *same* target indicates that there is likely some difference, performance or otherwise, between them. For simplicity, we treat each /24 IPv4 subnet (generally, the most fine-grained BGP prefix route announcement allowed, by convention) as a potentially distinct resource, noting that it may be the case that larger providers operate with smaller (more coarse grained) prefixes.

3.2 Domain Collection

We use the top 10,000 most frequently resolved domains from Cisco's Umbrella Top 1-Million list CITE as a starting point. However, as this list is obtained from the perspective of DNS resolution, the relationship *between* these domains is unclear. Further, as there is no complete URL information from such a perspective, there is no indication which domains are used for downloading web content, as opposed to providing some other service or interface. To address this, we attempt to load pages from this list and ultimately use domains providing web objects discovered on each successfully loaded page. This process is detailed below and illustrated in Figure 2.

First we attempt to load each web page from the Umbrella list using Google Chrome. If a page loaded, its source was checked for any indication that the page was not intended for human use (for example, automated server response pages for non-200 HTTP status messages). This filter reduced the size of our domain set from 10,000 pages to 2,441 pages. For each of these pages, a HAR file (in HTTP Archive foromat file) was saved to capture the full set of web objects loaded with the page. By using HAR files instead of just the page source, we avoid missing any dynamically loaded objects that may not appear in the original source. Even after using this approach, the space of possible domains remains larger than we can address in the scope of this experiment. The HAR file provides the full HTTP path of each web object retrieved. Domains used in this experiment come from this dataset.

Due to security related rate limits, our our experiment was limited to 15-20 domain measurements per client per day, thus further restricting the number of domains to be used in our experiment. Since the entire set obtained was large, we *ranked* object hosting domains by how frequently they wre observed across our set of HAR files. The most frequently appearing object hosting domains were given priority. Ultimately, 304 domains were used for the work described in this paper.

In Figues 3 and 4, we show the decreasing marginal impact of each additional domain our set. As shown, both quantities — the number of visited pages including a URL from our domain set and the fraction of URLs on each page addressed by our set — exhibit logarithmic-like growth patterns, beginning to plateau well before 100 domains are reached. We assert that this demonstrates the aggregate behavior of the 304 domains obtained above should sufficiently cover the domain diversity of a "typical" popular web page.

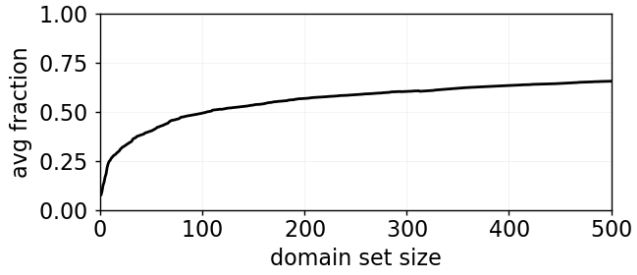


Figure 4: Mean fraction of page object links (URLs) covered per site vs the number of domains used.

3.3 Per-Provider Performance Measurement

Any attempt to identify the general groups that Internet clients are mapped to requires a dataset with a uniquely broad scope: not only breadth — a diverse set of clients — but also depth — many clients from each, yet to be uncovered, group or cluster. In addition, we are required to minimize the temporal spread of the measurements, as network resource allocation is known to change over time. We utilize the RIPE Atlas platform CITE for our measurements. RIPE Atlas offers a large number of globally distributed clients, capable of performing lightweight network measurements, such as pings, on behalf of configurable requests received by the Atlas API. We deployed ping measurements to the previously described 304 domains from 10,274 of RIPE's clients. Each client performed DNS resolution for pings via their local DNS resolver, ensuring that they each targeted the web resource they would ordinarily be directed to.

Unavoiable flux in the availability of individual, voluntarily maintained clients lead to some clients to performinging only a subset of the given measurements, thus missing some of the domains of interest. To be sure that this does not dramatically affect our findings, we arbitrarily enforce minimal amount of domain coverage — 160 domains, just more than half of our set — for use of a given client's data. We show in Section REF the effects of domain quantity in our measurements.

4 COMMON NETWORK RESOURCE EXPOSURE

This paper seeks to explore aggregate network resource catchments — the set of users exposed to the same set of web resources as each other across a given set of domains. We introduce a new similarity measure, which we have coined common network resource exposure (CNRE), to quantify the extent to which two clients are exposed to the same network resources. Inspired by the Jaccard index CITE, CNRE is defined as follows:

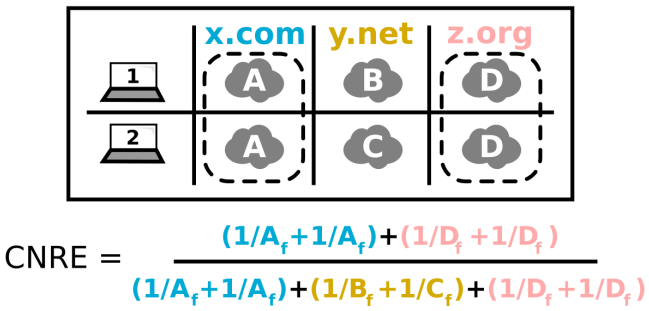


Figure 5: diagram illustrating CRNE

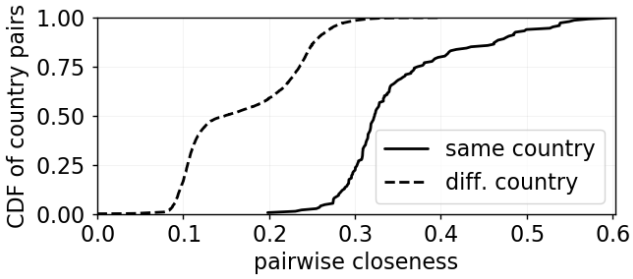


Figure 6: "High" closeness (90th percentile?) vs # domains measured

$$\text{CNRE} = \frac{\sum_i^D m_i(r_{1_i}^{-1} + r_{2_i}^{-1})}{\sum_i^D (r_{1_i}^{-1} + r_{2_i}^{-1})}$$

where D represents the intersection of measured domains between two clients, C_1 and C_2, and m_i is 1 the C_1 and C_2's i^{th} domain answers match (otherwise zero). The values r_{1_i} and r_{2_i} represent the fraction of all measurements (across the entire dataset) that matched C_1's and C_2's DNS answer for that domain, respectively. For example, if C_1's answer for domain i appeared 900 times across the 9024 times it was tested in our dataset (once by client), $r_{1_i} = 900/9024$, or 0.09973 (*i.e.* roughly 10% of the answers). In other words, r_{n_i} captures the *rarity* of the DNS answer received by client C_n for domain i. An example of CNRE calculation is shown in Figure 5.

In our calculation of CNRE, we use the inverse of r_{n_i} to add increased weight to the impact of a mismatch on rare answers. CNRE is therefore designed to be higher between clients with more matching rare answers. However, as it is ultimately a measure of similarity between clients, CNRE values range from 0 through 1, with 1 being the most similar. To ease discussion in the remainder of this paper, here we also define *distance* as 1−CNRE unless otherwise noted.

TODO: get 90th percentile plot and write about it

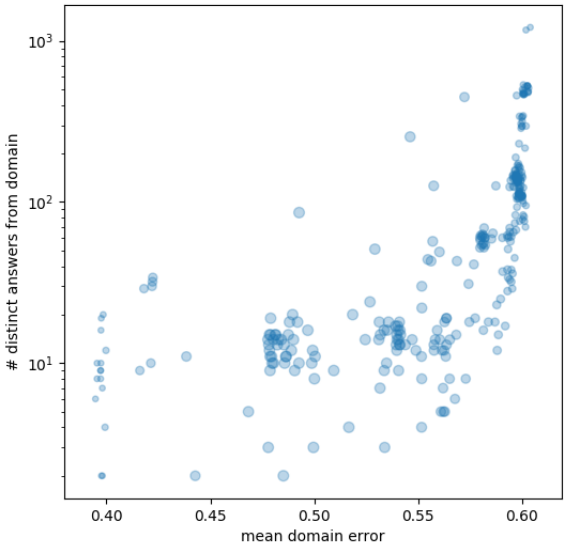


Figure 7: Mean domain error vs # of distinct answers observed from domain (one point per domain).

We pause here to address potential bias given toward individual domains. As CNRE calculation gives increased weight to rare answers, there is the possibility that the allocation patterns of large providers (who often have more answer variety related to the scale of their networks) may dominate the results. This would be detrimental to the main purpose of CNRE — a supposedly aggregate measure — as it would ultimately revert to essentially measureing a single provider, which is a well explored topic. To determine whether this is occuring, we calculate the *domain error*, for a single domain, as follows: Given a pair of clients, first, find their CNRE normally. Next, let us set d to be 1 if the DNS answer for the domain of interest matches between the pair of clients, and otherwise 0. Finally, the domain error is the absolute value of d−CNRE. In Figure 7, we plot this, with each point representing the mean domain error for a given domain across the entire set of client combinations.

With domain error, we simply capture how different the CNRE would have been had that domain been the only one used in CNRE's calculation. A *low* mean domain error — close to zero — implies that the domain is dominating over the CNRE. A *high* mean domain error — close to one — implies that the domain has little impact on CNRE's value. A mean domain error close to the middle — 0.5 — is ideal, as it implies that the domain is neither dominant nor irrelevant. We see in 7 that domains with many answers (and hence increased rarity per answer) actually have the highest error. Further, the range of domain error across all domains spans roughly from 0.4 to 0.6, indicative of the absence of substantial bias towards any given domain in our approach.

5 FINDING HIGH CNRE CLUSTERS

Finding aggregate catchments — pools of clients essentially directed toward the same web resoures — necessarily involves finding sets of clients with high CNRE measures between each other. Because CNRE is a measure of similarity, this problem naturally lends itself to heirarchical clustering techniques. We employ the complete linkage method to ensure cluster formation reflects commonalities across all cluster members as opposed to potentially edge-specific properties. Note that in all *clustering* calculations, we opt to use the CNRE *distance* (1−CNRE) as defined in Section **??**.

Establishing heirchical clusters requires that we have some definition of what constitutes a *high* or *low* CNRE measure and at what threshold it is appropriate to consider clients sufficiently similar such that they appear in the same cluster. In this section, we explore the implications of various CNRE values, as well as CNRE's relationship with other, well-established client grouping systems: country, ASN, BGP prefix, and /24 prefix subnet.

5.1 Group Formation Patterns

Figure 8 presents a dendrogram derived from pairwise CNRE distances across all clients and highlights three levels of distinct behavior regarding the distribution of CNRE distances. First, in the uppermost portion of the plot — where CNRE distances are beyond a threshold of 0.63 — we see that distinctions between branches and their implied client groups become well defined. Second, in the middle region of the tree, between CNRE distances of 0.25 and 0.63, we see that branches begin to fork unpredictably with shorter changes in CNRE distance. Finally, in the lowest region of the plot, where CNRE distances drop below 0.25, we see the amount of branching increase once again, rapidly increasing the granularity of each branch as CNRE decreases further.

We compare established client group labeling schemes — country, ASN, and BGP prefix — to CNRE similarity between clients with matching (*e.g.*, same country) and differing (*e.g.*, different country) labels. Our findings are shown in Figure 9. The 95th percentile CNRE between groups with differing labels is marked on each plot by a vertical red line; at this point, differing and matching labels become distinguishable. For example, in Figure **??**, a pair of clients with CNRE < 0.73 (see 0.27 in Figure 8, which uses CNRE distance) are likely from different ASes, while clients with CNRE > 0.73 are likely from the AS. Note, however, that 9 uses *median* values for all points shown. We analyze this further in 5.2.

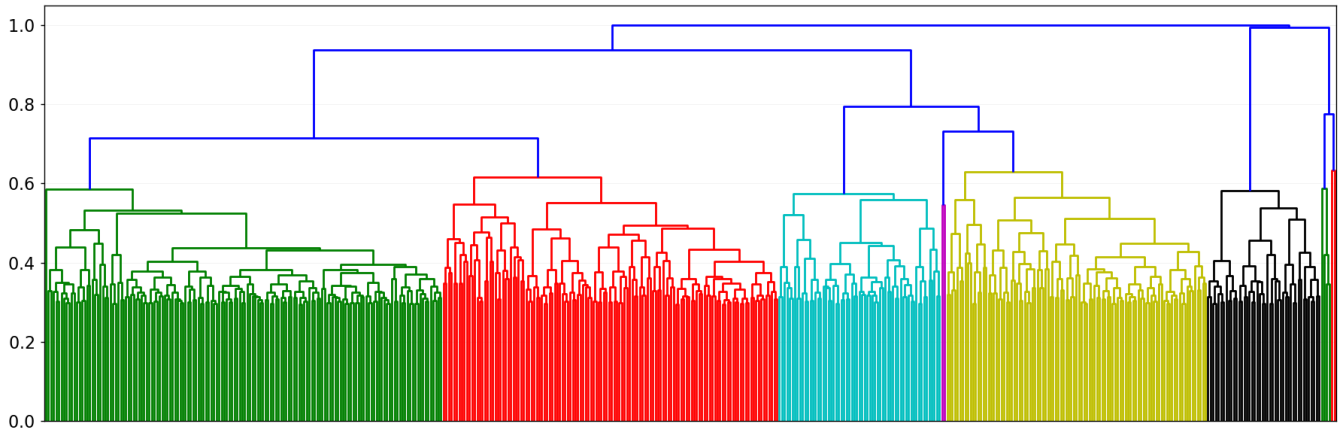
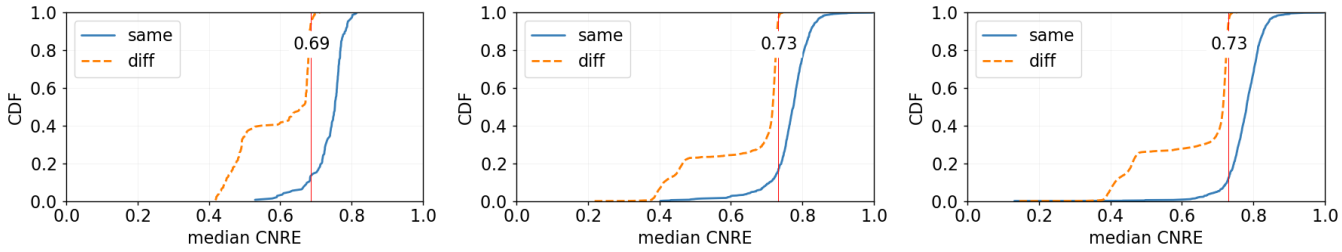


Figure 8: Dendrogram of CNRE distance across all client pairs



(a) country **(b) ASN** **(c) BGP prefix**

Figure 9: CDFs of CNREs across client sets with matching (same) and non-matching (diff) labels. "Same" shows the CDF for the median CNRE distance across all client pairs matching a given label. "Diff" shows the CDF for the median CNRE distance from each label group toward all other labels. The red, vertical line in each subfigure marks the 95th percentile CNRE for for differing labels.

Figures 9 and 10 together help provide a possible explanation for three partiions observed in Figure 8. In Figure 9, we see that in all three subplots, the aforementioned middle region of Figure 8 appears again, this time as a plateau in both the "Diff" and "Same" curves. In this region, "Diff" and "Same" overlap significantly, rendering them indistinguishable. This transient zone is given further context in Figure 10, where we shade each country's median CNRE towards other countries (*i.e.*, outbound comparisons) — the same data used to plot the "Diff" CDF in Figure 9a.

If a given country tends to have low CNREs between itself and all other countries, this implies that the country is exposed to a more exclusive set of web resources than its peers. For example, Australia, which, as shown in 9a, has a generally low CNRE with other countries, likely utilizes very locale-targeted infrastructure given its relative distance from more more broadly used network resources. Likewise, China, which is well documented as having its Internet infrastructure deliberately disjoint from much of the world (CITE great firewall, etc), also has a low CNRE with most other countries. Conversely, we see most that countries within Europe and Africa tend toward having higher CNREs with most other countries, implying that the majority of web resources exposed in those regions are neither exclusive nor fine grained.

5.2 Label Alignment

Now that we have established some concept of what constitutes a "high" or "low" CNRE measure, we further consider CNRE in comparison to country, ASN, and BGP prefix — three labeling schemes commonly used group Internet clients. Specifically, we wish to determine if the information captured by CNRE (the extent to which clients are exposed to the same web resources) is reasonably captured by any pre-existing system. If this were the case, one might argue that the premise of treating CNRE as a separate system would be redundant and arbitrarily complex. Therefore, we treat this

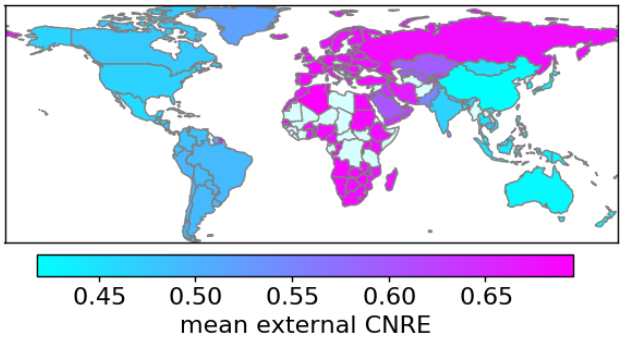


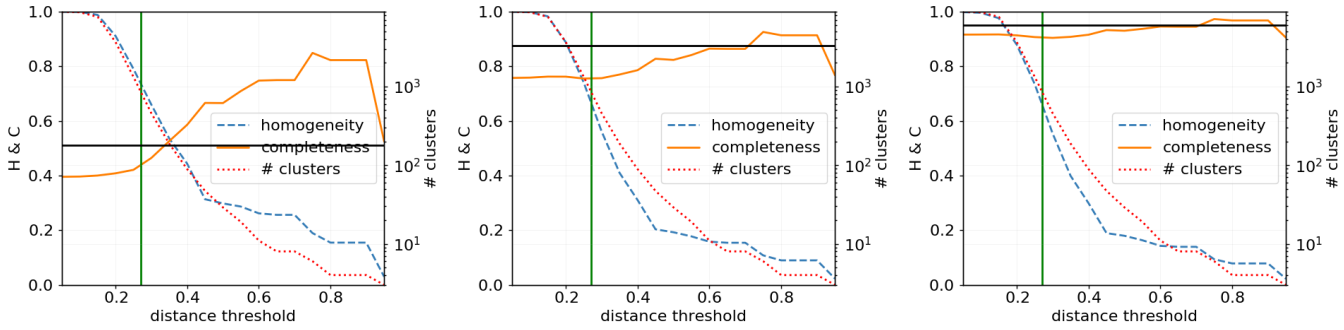
Figure 10: Choropleth with each country shaded by its median CNRE distance from all other countries.

subsection as a means of validating and justifying the CNRE as a separate, currently unaddressed concept.

In Figure 11, we plot the completeness, homogeneity, and number of clustesr for the aforementioned labeling schemes as we cluster clients in our dataset, varying the CNRE distance threshold used for cluster formation. In addition, we also mark, with a vertical line, the CNRE distance at which labels become distinct (see Figure 5.1), and we mark the number of labels (*i.e.*, the number countries, ASes, or BGP prefixes) present with a horizontal line (using the righthand y-axis).

If homogeneity and completeness, which together indicate how well cluster membership aligns with a given labeling scheme, is not high, the CNRE-related implications of a given label become ambiguous.

6 CLUSTER ANALYSIS



(a) country (b) ASN (c) BGP prefix

Figure 11: Completeness, homogeneity, and number of clusters versus clustering distance threshold. The vertical line marks 0.27, the CNRE distance at which clients with differing labels become distinguishable, and the horizontal line denotes (using the right-side y-axis) the number of different real labels (for example, the number of countries) preesent in our data set for the given labeling scheme.

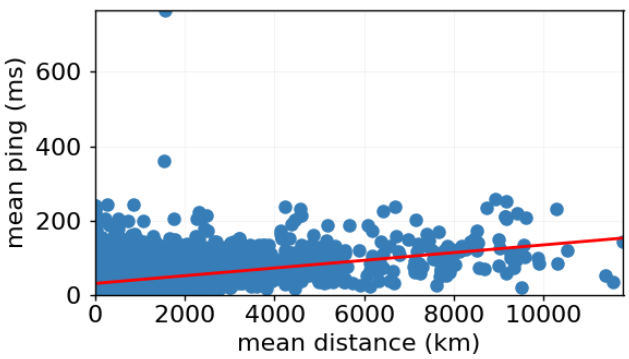


Figure 12: CDF of # of outliers per cluster for geo distance, etc

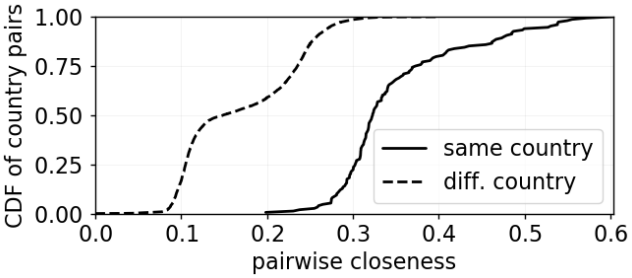


Figure 13: Domain match alignment with clusters (what format?)

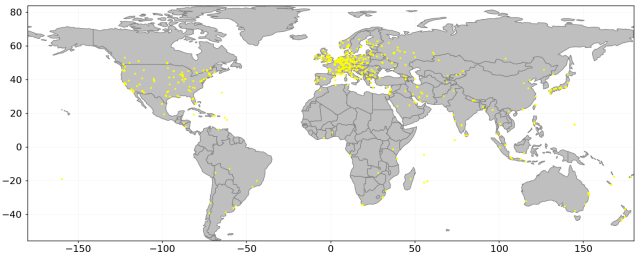


Figure 14: Map of world with point for each cluster's geographic center.