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 be 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 relationship between CNRE and well established network properties (country, ASN, and BGP prefix).

By clustering clients that share high CNRE measures, we identify aggregate catchment patterns encompassing 302 popular domains. Our findings expose clients that are poorly served by their current position in this aggregate mapping scheme and show that a client's distance from the geographic center of their CNRE cluster is directly proportional to the latency they experience across providers.

1 INTRODUCTION

You and the person next to you might not be using the same Internet. With ever increasing diversity and interlinking of online services — content distribution networks (CDNs), cloud computing, CDN and cloud brokers, ad brokers, load balancing, user tracking, geoIP, and more — even the implications of loading a single web page are no longer straightforoard CITE. Often, failure to recognize the whole as distinct from the sum of its parts has inhibited progress and hampered performance in networking technology CITE. In the same way a city's skyline cannot be anticipated by the artitect of a single building, the "digital skyline" of the Internet can be neither predicted nor fully controlled by any single entity. However, skylines can always be *observed*.

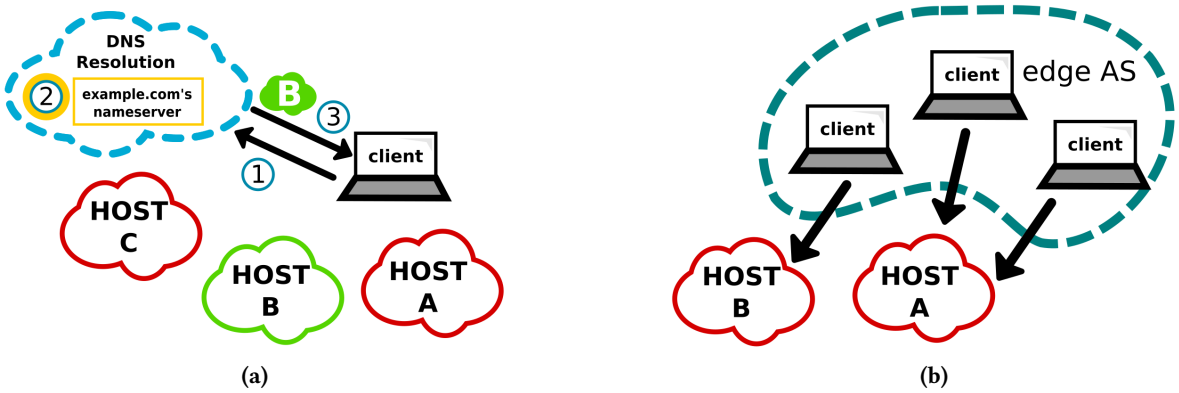
Even across a single network service, client experiences may diverge. In Figure **??**, we provide a high level illustration of how this can happen. In subfigure 1a, a client intending to connect to example.com submits a DNS query. We do not concern the minute details of the DNS resolution process, which is itself multi-tierd and possibly involving cooperation from many separate stakeholders. What is important to know is that eventually, the client's request reaches the nameserver responsible for example.com. The nameserver uses what is often internal, proprietary logic to decide which of example.com's network resources the client should be connected to. In subfigure 1b, we are reminded that this client is not the only one access example.com. However, as illustrated, the client's peers may not necessarily be directed to the same resource, despite having carried out essentially the same DNS resolution process and possibly sharing the same edge network. This potential for mismatch between clients only grows as the number of domains considered increases — which it will, often on a single web page.

In this paper, we explore the complex combination of independently operating resource allocation schemes and assess their behavior in *aggregate*. To enable our research, We introduce a new similarity measure, common network resource exposure (CNRE), which captures the extent to which a pair of clients are directed to the same network targets as each other across a broad set of domains. CNRE is, to our knowledge, the first ever method to quantify cross-provider DNS redirection patterns and their collective behavior.

We test and assess CNRE using 302 web content hosting domains for each CNRE calculation. To do this, we collect latency and DNS measurements for each domain from each of 9,024 globally distributed clients and perform over 40 million pairwise CNRE calculations between them. Our experiments validate common network research exposure as a useful quantity and explore its relationship with other cilent properties.

In order to develop the Skyline model, we performed an exhaustive set of measurements to frame client experience on a per *site* basis. In this 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 9,000 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".

This paper makes the following contributions:



(a) (b)

Figure 1: Illustration of network resource allocation. Figure 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. Figure 1b shows an example of how clients with similarly described locations may be directed to distinct network resources.

??

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

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 [1]. Further, more abstract applications may include, but are not limited to, distributed denial of service mitigation [10] and CDN node deployment [9, 13].

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) [6, 8, 10]. Our work differs significantly in scope: to our knowledge, we are the first to investigate what we refer to as *aggregate catchments*, the joint behavior of many anycast CDN catchments as well as unicast CDN targets, spread across many content distribution platforms. Conversely, this related body work either focuses on individual platforms or specific services [6, 8, 10].

Several authors have attempted to discover the topology of large CDN platforms through large scale measurement studies [2, 3, 5]. 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 [2, 3, 5]. Other work close to this space investigates the performance of a particular CDN deployment scheme [7].

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 necessary context to understand the results presented throughout this paper.

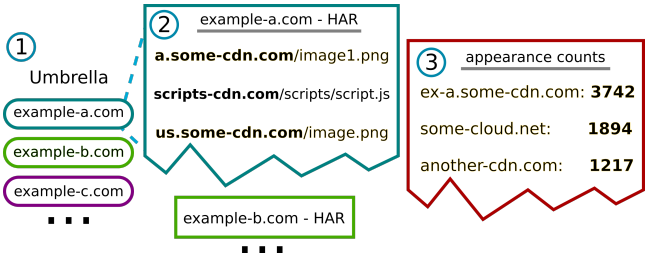


Figure 2: Diagram illustrating domain name collection: 1) Domains from the Umbrella top 1-million were loaded via Google Chrome to identify human-targeted websites. 2) For each human-targeted website's landing page, a HAR file was recorded. 3) Domains were extracted from HAR data and ranked by the number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

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 *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 [4]. Previous work has well documented the impact of individual, slow loading objects on page load time [14]. 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 the *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.

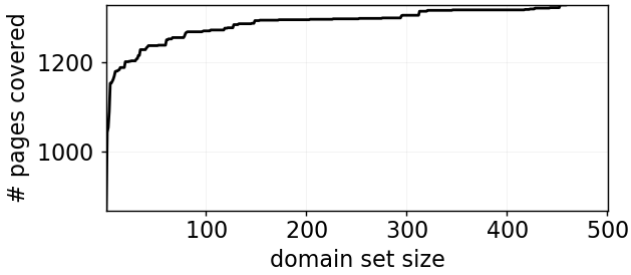


Figure 3: The number of sites containing an object hosted by a domain in our set vs the size of our set of domains.

3.2 Domain Collection

We use the top 10,000 most frequently resolved domains from Cisco's Umbrella Top 1-Million list [12] 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 format 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. 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 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 were observed across our set of HAR files. The most frequently appearing object hosting domains were given priority. Based on this prioritization, we arbitrarily used the top 304 domains from this set.

In Figues 3 and 4, we show the decreasing marginal impact of each additional domain in our set. As shown, both quantities — the number of visited pages including a URL from our

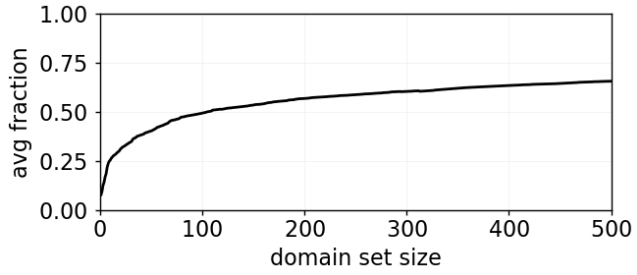


Figure 4: Mean fraction of page object links (URLs) covered per site vs the number of domains used.

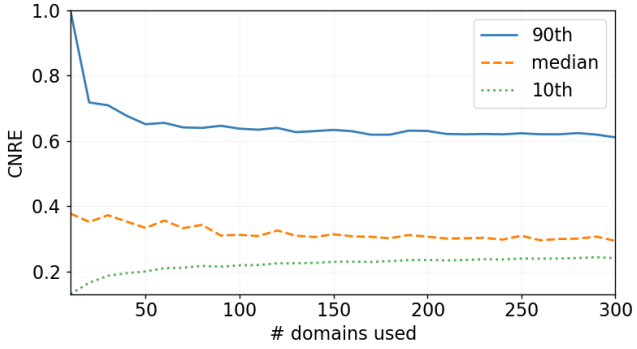


Figure 5: CDF showing the effect of the number of domains used for CNRE calculation. The 500 clients and set of domains used for each CNRE calculation were randomized.

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.

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 [1] 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.

Unavoidable flux in the availability of individual, voluntarily maintained clients lead to some clients performing 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 4 the effects of domain quantity in our measurements. Applying this contraint reduced the size of our client set to 9,024 clients.

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 between two clients, C_1 and C_2, is defined as follows:

$$\text{CNRE}(C_1, C_2) = \frac{\sum_i^D m_i(r_{1_i}^{-1} + r_{2_i}^{-1})}{\sum_i^D (r_{1_i}^{-1} + r_{2_i}^{-1})}$$

where D represents the intersection of measured domains between both clients, and m_i is 1 if 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.

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. 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.

In Figure 5, we plot the effects of the number of domains on CNRE statistics. For each data point, performed pairwise

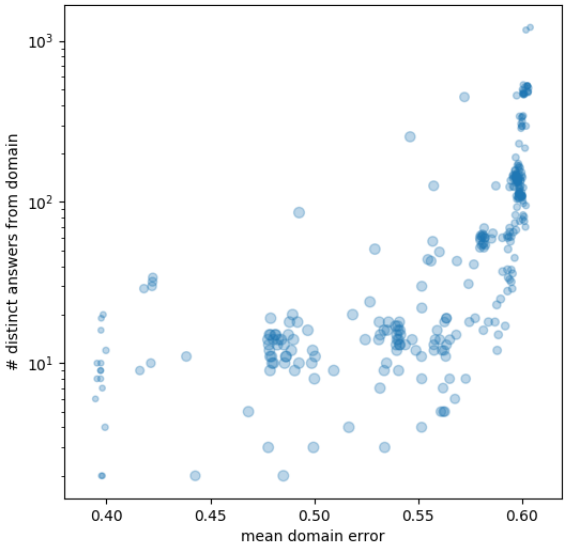


Figure 6: Mean domain error vs # of distinct answers observed from domain (one point per domain).

CNRE calculations between 500, randomly selected clients. For each individual comparison, a random set of domains were selected, matching the quantity being tested. Both upper (90^{th} percentile) and lower (10^{th}) CNRE scores stabilize and plateau significantly between by 150 domains, showing no substantial changes as the number of domains increases beyond that. This validates our use of 160 domains as a cutoff for a client's admission into our dataset.

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 measuring a single provider, which is a well explored topic. To determine whether this is occurring, 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 6, 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 Figure 6 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 resources — 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 hierarchical clustering techniques [11]. 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 4.

Establishing hierarchical 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 7 presents a dendrogram derived from pairwise CNRE distances across all clients and highlights two levels of distinct behavior regarding the distribution of CNRE distances. In the uppermost portion of the plot — where CNRE distances are beyond a threshold of 0.65 — we see that distinctions between branches and their implied client groups become well defined. There is a large cluster composed mainly of European and African probes (green cluster labelled *Europe 95%*), one representing East Europe (red cluster labelled *DE 56%*), one composed of North and South American probes (blue cluster labelled *US 59%*), a cluster composed of probes from Asia and Oceania (khaki cluster), and one made exclusively with American probes (black cluster labelled *North America 98%*). In the lower region of the tree, where CNRE distances drop below 0.65, we see that branches begin to fork unpredictably with shorter changes in CNRE distance. Some of these branches may map to specific countries, but at finer

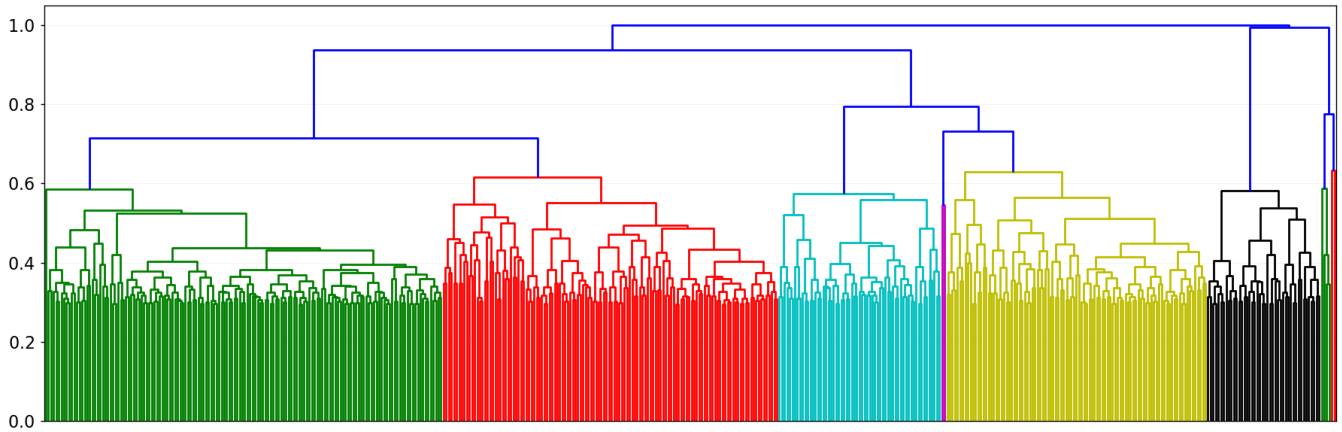


Figure 7: Dendrogram of CNRE distance across all client pairs

granularities the geographical location of probes delineate poorly the characteristics of the clusters.

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 8. 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 7, which uses CNRE distance) are likely from different ASes, while clients with CNRE > 0.73 are likely from the AS. Note, however, that 8 uses *median* values for all points shown. We analyze this further in 5.2.

Figures 8 and 9 together help provide a possible explanation for three partiions observed in Figure 7. In Figure 8, we see that in all three subplots, the aforementioned middle region of Figure 7 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 9, 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 8a.

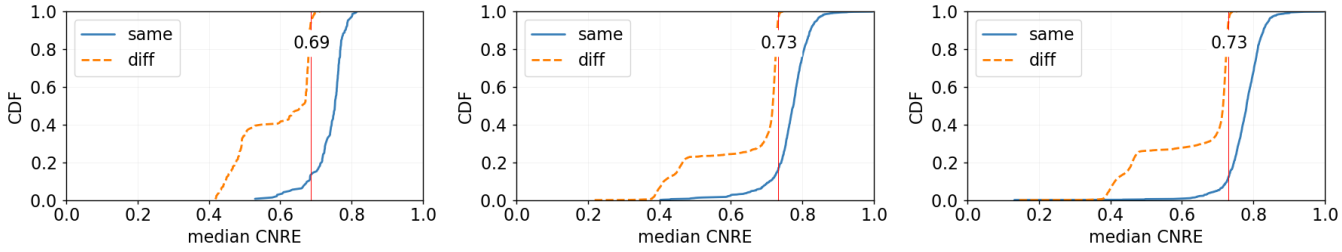
If a given country tends to have low CNREs between itself and all other countries, this implies that the country is exposed to a more exclusive set of web resources than its peers. For example, Australia, which, as shown in 8a, has a generally low CNRE with other countries, likely utilizes very locale-targeted 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 subsection as a means of validating and justifying the CNRE as a separate, currently unaddressed concept.

In Figure 10, 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. We see in Figure 10 that for country and ASN, homogeneity and completeness are never simultaneously high, rendering them unusable for determining



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

Figure 8: 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.

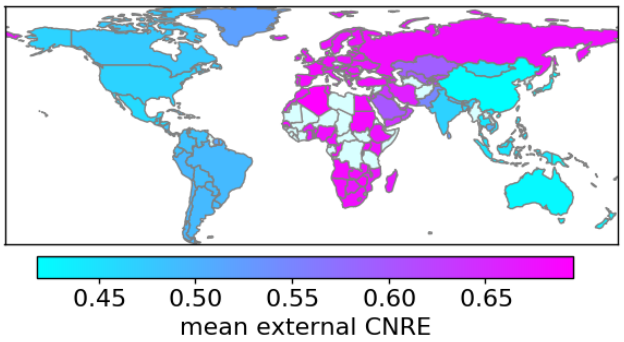


Figure 9: Choropleth with each country shaded by its median CNRE distance from all other countries.

CNRE on their own. BGP prefix, however, requires more thorough consideration. In Figure 10c

Figure 7 depicts the hierarchical clustering dendrogram based on pairwise CNRE distances. This representation highlights the similarity of clients and different possible partitioning. Each node in the tree is a cluster composed of the underneath denser clusters. A horizontal cut in the dendrogram produces a partitioning of clients for which the dissimilarity of two probes in the same partition is not greater than the y-value where the cut is done.

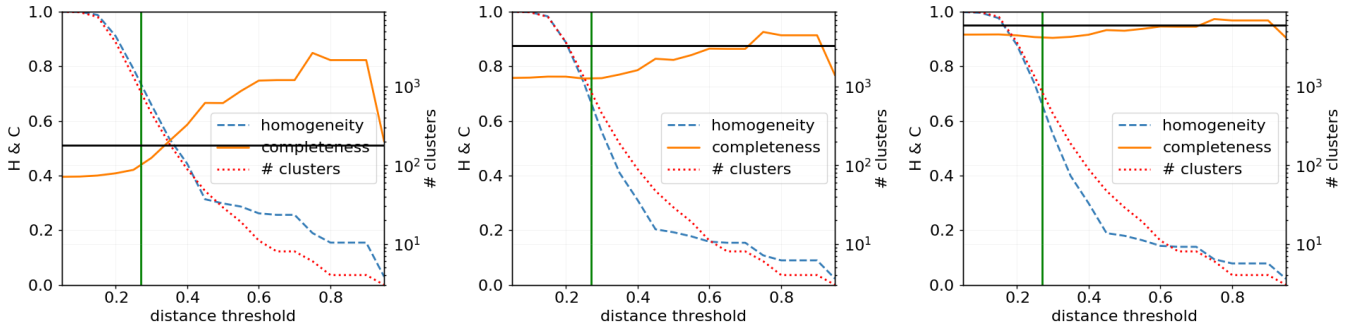
For example, the colored clusters in Figure 7 are obtained with a cut at $y = 0.65$. This partitioning produces eight clusters including three small ones composed of outliers. The five large clusters represent a very coarse partitioning of clients. 95% of probes in the green cluster are from Europe and 4% are from Africa (that is almost all African probes), the red cluster consists mainly of German, Italian, and Russian probes (79%), the blue cluster is mainly North and South American probes (resp. 80% and 18%), the khaki cluster has mostly probes from Asia and Oceania (resp. 67% and 32%), and the black cluster is mostly North American probes (98%). As each cluster is composed of smaller and denser clusters, one can again partition these clusters and form groups with clients having more network resources in common.

6 CLUSTER ANALYSIS

Now that we have built up an understanding of how CNRE behaves, we move to investigate the aggregate catchments of clients using clustering techniques discussed in the previous section. In this section, we use the aforementioned CNRE threshold of 0.73 for cluster formation. This threshold yields 870 clusters. For analysis, in which we compare clients that cohabit the same cluster, we consider only clusters for which our dataset has a representation of at least three clients; this yields 612 clusters from the original 870. The average cluster size from this reduced set is 218 members, with a standard deviation of 816 and a median size of 36. Note that cluster size variety is significantly impacted by our dataset, which has more client representation in western Europe and North America than in the rest of the world where RIPE's influence is more sparse CITE.

6.1 Geographic Spread

Here we examine each cluster's geographic spread — the closeness, in terms of geographic distance, of members of the same cluster. As clients sharing the same cluster are predominantly exposed to the same network resources, the geographic spread of a cluster's clients must related to the network performance (latency) they experience. Specifically, if a pair of clients directed to the same network resource are physically "far" apart from each other, it is likewise impossible for *both* clients to simultaneously be near said resource. In such an arrangement, the resource is either near one client and far from the other, or the resource is equidistant from both clients. In the latter case, if the clients are sufficiently



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

Figure 10: 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.

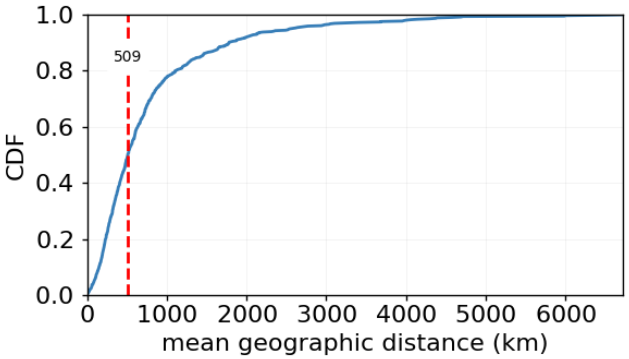


Figure 11: CDF of mean geographic distance between cluster members. The dashed vertical line marks the median.

far from each other, the resource must also far from both clients.

To calculate these geographic distances, we use coordinates for RIPE Atlas probes — our client machines in the context of this experiment — obtained from RIPE Atlas's API. RIPE acquires probe location information via manual input from volunteers who themselves maintain Atlas probes, and, where necessary, by autmated input from MaxMind CITE. Figure 11 shows the CDF of the mean geographic distance (in kilometers) between members of a cluster, for each cluster. Members of a cluster with a larger mean geographic distance are farther apart form each other, on average, than are the members of a cluster with a lower mean geographic distance. In the median case, we see an average client distance of 509 km. We observe that for 20% of clusters, members are over 1000 km on average.

Since CNRE potentially spans many, physically distinct resources, it serves as an *aggregate* measurement, and we do not attempt to pinpoint the location of any individual resource. Instead, we identify the effective "center" of each cluster and measure the effect of a member's distance from the center. Following the intuition of CDN deployment laid out in other work (CITE), we hypothesize that the geographic center of a cluster will sit physically close the location of the most of that cluster's network resources. By this logic, clients closer to their cluster's center should experience better network performance (*i.e.*, lower latency) than those farther away. To test this, we compared each client's mean latency (taken across all 299 ping responsive domains in our set) to that client's distance from its respective cluster's center. For simplicity, we use a cluster's geometric median as an estimate of its center. The results of this comparison are shown in Figure 12 as a scatter plot of mean latency versus distance from cluster center. Each point corresponds to a single client's latency and distance from its respective cluster's center. The figure also includes a best fit line, denoting the overall trend of the points.

Note the positive slope of points in Figure 12, indicative of a directly proportional relationship between latency and distance from the cluster's effective center. As a client's distance from its cluster's center increases, so does its latency. Performance for clients relatively near their respective centers — closer than 1000 km — is seemingly noisy and no trend is clearly observable. However, as the geographic distance increases beyond 1000 km, the directly proportional relationship between performance and center distance becomes more apparent.

We also point out that the slope of Figure 12's best fit line quantifies this relationship as approximately 8.2×10^7m/s,

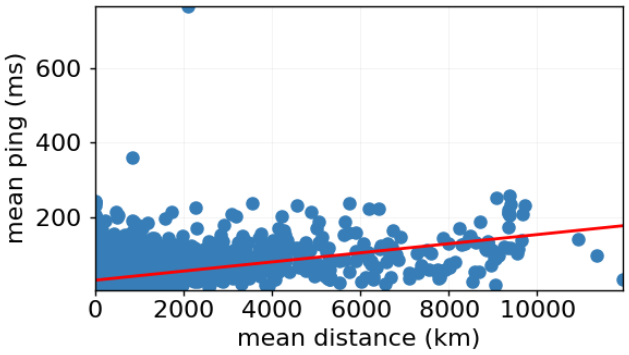
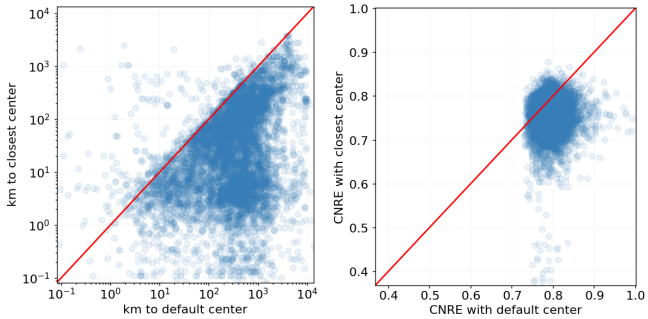


Figure 12: Scatter plot where, for each client, we compares the client's mean latency (across all responding sites) to that client's distance from its cluster's center. The line denotes a first order best fit curve for the scatter plot's points.



(a) geographic distance **(b) CNRE similarity**

Figure 13: Subfigure 13a shows a scatter plot of each client's geographic distance from its own ("default") cluster's center location versus its geographic distance to the geographically closest center of another cluster ("closest"). Subfigure 13b shows a scatter plot of each client's CNRE similarity with its own ("default") cluster's center location versus its CNRE similarity with the geographically closest center of another cluster ("closest").

which implies a general data speed of $\frac{1}{4}$th of the speed of light. This finding is similar that hypothesized by CITE. In additon, the fastest network communication mediums in use at the time of this writing move data at approximately $\frac{2}{3}$rds of the speed of light CITE. Traffic, routing complexity, and the pressence of lower speed mediums may account for the apparently lower speed in our finding.

As we have demonstrated that one's distance from their cluster's center impacts performance, clients should ideally share resources with the closest cluster center possible. Figure 12 raises an additional concern: many clients are very far away — often thousdands of kilometers — from their respective cluster centers. For perspective, we remind the reader that the circumference of the world is approximately 40,075 km; several clients reside over a fourth of that distance from their cluster's center. With such large geographic distances, however, it is likely the case that there exists some *alternative* cluster whose center is geographically nearer to the client than the client's own cluster's center. For clarity, we will refer to a client's own cluster's center as its "default" center, and the cluster center geographically closest to the client (excluding the "default" center) as the "closest center" or "alternative center". In Figure 13, we compare the properties of each client's default and closest centers.

Subfigure 13a shows a scatter plot of the geographic distance from each client (in kilometers) to its default and closest centers. The diagonal line dividing the plot indicates where the geographic distances are equal. Points beneath the line correspond to clients who are closer to their alternative centers, while clients with points above the line are closest to their default centers. Most clients are closer to their alternative centers, but there are several details to note, discussed below.

First, it is apparent that most clients are geograhpically closer to their alternative cluster centers than their default centers, in some cases by orders of magnitude. Second, we remind the reader that we employed the complete linkage method to form our hierarchical clusters. Because of the behavior of complete linkage, which determines cluster membership by pairwise distance across all members instead of individual members, it is possible that individual clients may have a higher CNRE similarity with their alternative center than with their default center. In other words, it may be the case that we have assigned some clients to the "wrong" cluster. Occurrances of this may account for some of the noise observed in default center distances below 1000 km in Figure 12. To test for mismatched clients, we plot a point for each client's CNRE similarity towards its closest center versus its default center in Subfigure 13b. The majority of CNRE values in Subfigure 13b are concentrated between 0.7 and 0.8. This suggests that geograhpically overlapping resource allocation groups may be responsible for the behavior observed in the ambiguous regions of Figures 7 and 8.

Although NUM% of clients had alternative centers geographically closer than their default centers (NUM kilometers closer in the median case), NUM% of these clients had higher CNRE similarity with their default centers (NUM% better in the median case). While we have demonstrated that high geographic distance coupled with high CNRE tends to result in higher latency, here we paradoxically observe that this is

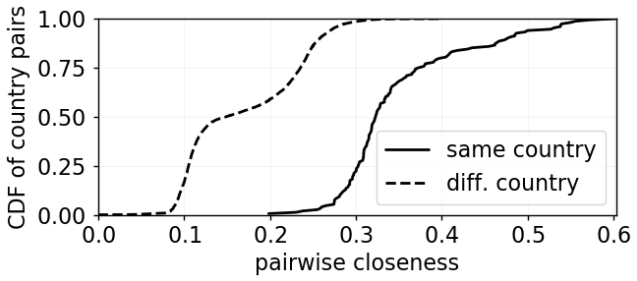


Figure 14: Domain match alignment with clusters (what format?)

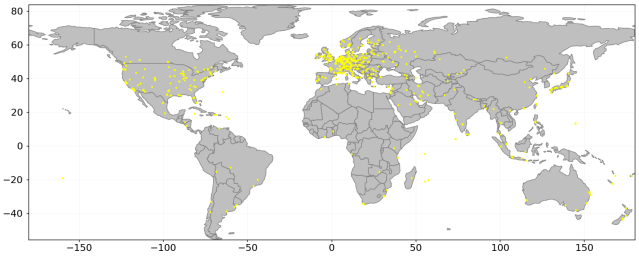


Figure 15: Map of world with point for each cluster's geographic center.

arrangement is a common occurence. We further explore the implications of this pattern in Section 7.

7 DISCUSSION

7.1 Why Web Object Domains

In Section 3.2, we described how the set of domains used in our experiment were selected. The selected domains were extracted directly from web object URLs observed across the set of web pages we checked. We note here that these domains are often abstractions of more explicit hosting schemes. For example, such domains may resolve to unique CNAMES CITE or directly resolve to third party CDN addresses CITE. In contrast to our approach, we could have converted each domain into some lower level representation (such as its CDN) and in turn performed a CNRE-like measurement study using this representation (*i.e.*, ping from each client to each CDN in our set).

While this alternative approach may provide its own insights, we chose leave each discovered domain "as is" for two reasons. First, although a given domain may use CDN hosting, it is worth noting that modern CDN selection techniques are complex and diverse. While some content providers may opt to utilize a *single* CDN for their purposes, it has also become common practice to instead depend on CDN *brokers* or *multi* CDNs to dynamically (by cost, performance, geography, *etc.*) make use of a set of CDNs. In other words, the "less abstract" representation of a given content provider is, in many cases, far from comprehensive with regard to a diverse set of clients. Second, even if a domain or content provider could adequately be reduced to a lower level description as described, the performance of a given CDN "in general" is not necessarily representative of the performance of one of its customers. The reasons for this are plentiful, ranging from customer specific policies and agreements (for example, the customer might purchase region specific support) to caching algorithms and load balancing.

REFERENCES

[1] 2016. RIPE Atlas - RIPE Network Coordination Centre. https://atlas.ripe.net/.

[2] Bernhard Ager, Wolfgang Mühlbauer, Georgios Smaragdakis, and Steve Uhlig. 2011. Web Content Cartography. In *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference (IMC '11)*. ACM, New York, NY, USA, 585–600. https://doi.org/10.1145/2068816.2068870

[3] Karyn Benson, Rafael Dowsley, and Hovav Shacham. 2011. Do You Know Where Your Cloud Files Are?. In *Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop (CCSW '11)*. ACM, New York, NY, USA, 73–82. https://doi.org/10.1145/2046660.2046677

[4] Michael Butkiewicz, Harsha V Madhyastha, and Vyas Sekar. 2011. Understanding website complexity: measurements, metrics, and implications. In *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*. ACM, 313–328.

[5] Matt Calder, Xun Fan, Zi Hu, Ethan Katz-Bassett, John Heidemann, and Ramesh Govindan. 2013. Mapping the Expansion of Google's Serving Infrastructure. In *Proceedings of the 2013 Conference on Internet Measurement Conference (IMC '13)*. ACM, 313–326. https://doi.org/10.1145/2504730.2504754

[6] Matt Calder, Ashley Flavel, Ethan Katz-Bassett, Ratul Mahajan, and Jitendra Padhye. 2015. Analyzing the Performance of an Anycast CDN. In *Proceedings of the 2015 ACM Conference on Internet Measurement Conference (IMC '15)*. ACM, 531–537. https://doi.org/10.1145/2815675.2815717

[7] F. Chen, R. Sitaraman, and M. Torres. 2015. End-User Mapping: Next Generation Request Routing for Content Delivery. In *Proceedings of ACM SIGCOMM '15*. London, UK.

[8] Marcel Flores and Stephen McQuistin. 2017. Seeing the World with RIPE Atlas. https://labs.ripe.net/Members/verizon_digital/seeing-the-world-with-ripe-atlas.

[9] Rupa Krishnan, Harsha V. Madhyastha, Sushant Jain, Sridhar Srinivasan, Arvind Krishnamurthy, Thomas Anderson, and Jie Gao. 2009. Moving Beyond End-to-End Path Information to Optimize CDN Performance. In *Internet Measurement Conference (IMC)*. Chicago, IL, 190–201. http://research.google.com/archive/imc191/imc191.pdf

[10] Giovane C.M. Moura, Ricardo de O. Schmidt, John Heidemann, Wouter B. de Vries, Moritz Muller, Lan Wei, and Cristian Hesselman. 2016. Anycast vs. DDoS: Evaluating the November 2015 Root DNS Event. In *Proceedings of the 2016 Internet Measurement Conference (IMC '16)*. ACM, New York, NY, USA, 255–270. https://doi.org/10.1145/2987443.2987446

[11] Fionn Murtagh. 1983. A survey of recent advances in hierarchical clustering algorithms. *The computer journal* 26, 4 (1983), 354–359.

[12] Quirin Scheitle, Oliver Hohlfeld, Julien Gamba, Jonas Jelten, Torsten Zimmermann, Stephen D Strowes, and Narseo Vallina-Rodriguez. 2018. A long way to the top: significance, structure, and stability of internet top lists. In *Proceedings of the Internet Measurement Conference 2018*. ACM, 478–493.

[13] Mukarram Tariq, Amgad Zeitoun, Vytautas Valancius, Nick Feamster, and Mostafa Ammar. 2008. Answering What-if Deployment and Configuration Questions with Wise. In *Proceedings of the ACM SIGCOMM 2008 Conference on Data Communication (SIGCOMM '08)*. ACM, New York, NY, USA, 99–110. https://doi.org/10.1145/1402958.1402971

[14] Xiao Sophia Wang, Aruna Balasubramanian, Arvind Krishnamurthy, and David Wetherall. 2013. Demystifying page load performance with WProf. In *Presented as part of the 10th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 13)*. 473–485.