A First Look at Deployment Strategies of Services Provisioned using Anycast

Gustavo Luvizotto Cesar*, Remi Hendriks*, Martin Angelov*,
Mattijs Jonker*, Roland van Rijswijk-Deij*, Johannes Zirngibl†, Ralph Holz*‡
* *University of Twente*, Enschede, The Netherlands
{g.luvizottocesar, remi.hendriks}@utwente.nl
† *Max Planck Institute For Informatics*, Saarbrücken, Germany
‡ *University of Münster*, Münster, Germany

***Abstract*—IP anycast is a fundamental Internet technology where a prefix is made available in multiple locations to bring services closer to users and, most importantly, improve service resilience. Despite the growth in anycast—with censuses reporting 1×10^3 ASes and 14×10^3 /24-prefixes in 2026— little is known about how operators provision services using anycast. We address this gap by characterizing the deployment strategies used by anycast operators, based on the locations behind anycast prefixes and the topologies visible in routing data. We design a pipeline that measures 120 ports on TCP and UDP, and evaluates the use of QUIC and 32 different application-layer protocols to identify services replicated using anycast.**

We show large differences in deployment strategies: 77% of anycast Autonomous Systems (ASes) announce prefixes with a few IP addresses hosting services, whereas 7% fully utilize their prefixes, with five ASes alone accounting for more than 88% of anycast IP addresses hosting services. We find 18% of ASes make use of the same Bring-Your-Own-Autonomous-System (BYOAS) infrastructure hosting provider, highlighting hidden dependencies not visible without topological analysis. Regional anycast is widespread, with 35% of operators replicating prefixes within a single continent, including 23 ASes with regional prefixes in multiple regions. While most anycast prefixes are used for web services (including deployments with significant QUIC adoption), they are largely originated by a few Content Delivery Network (CDN) ASes. Conversely, we find most ASes use anycast to replicate DNS using a few prefixes, highlighting distinct strategies between CDNs and DNS operators.

***Index Terms*—Anycast, Anycast Deployment, Internet Services, DNS, CDN, QUIC, Resilience**

I. Introduction

Anycast is the practice of making a service address available in multiple, discrete, autonomous locations [1], which we refer to as Points of Presence (PoPs) throughout this paper. The first RFC describing anycast (RFC 1546 [2]) was published in 1993 and explains how anycast simplifies finding an appropriate server. As service examples, they list DNS, FTP, and 'Archie' (one of the first Internet search engines). More than three decades later, anycast is widely deployed for critical Internet infrastructure, such as the DNS [3], and by Content Delivery Networks (CDNs) to provide web services [4], [5]. Reasons for providing a service using anycast include increased service resilience through automatic failover (where traffic is redirected to a different PoP if one fails), service replication closer to users to reduce latencies, and load distribution amongst PoPs.

Given the importance of anycast, previous studies have characterized the services hosted on anycast prefixes [4], [5]. However, these works are more than ten years old and cover only 1.7×10^3 prefixes. As of 2026, anycast deployments have grown significantly, with recent daily censuses [6] detecting 14×10^3 anycast /24-prefixes and 12×10^3 IPv6 /48-prefixes.

In this work, we provide an up-to-date view of how anycast is used globally by looking at the services replicated with anycast and investigating the deployment strategies used by operators to provision such services. We achieve this by investigating the number and location of PoPs behind anycast prefixes and their topologies visible in routing data. Additionally, we construct a pipeline to perform service-aware scanning from multiple Vantage Points (VPs), combining TCP, UDP, and QUIC scans using ZMap [7], LZR [8] and ZGrab2 [9].

Our contributions are as follows:

(i) For the 1×10^3 ASes detected by *LACeS* to replicate services using anycast (*i.e.*, anycast ASes), we find 77% host services on less than 10% of their announced IP addresses, and 7% utilize more than 90% of their prefixes. Thus, five ASes alone account for more than 88% of anycast IP addresses hosting services. This concentration has implications for the resilience and diversity of anycast infrastructure.

(ii) We show that Bring-Your-Own-Autonomous-System (BYOAS) has become a significant deployment pattern. 18% of anycast ASes replicate their services using a single BYOAS provider. Half of these ASes use that provider exclusively. This reveals hidden dependencies where independent ASes rely on the same provider and infrastructure.

(iii) We demonstrate that anycast is often deployed regionally (*i.e.*, within a single continent), with 35% of ASes have at least one regional prefix, some of which having distinct regional prefixes in multiple continents. This shows that anycast is not just used to replicate services globally but also to provide redundancy for regional services.

(iv) We find web services dominate anycast at prefix granularity, with a significant (42%) presence of QUIC, signaling

G. Luvizotto Cesar and R. Hendriks are shared first author.

978-3-903176-83-6

operators are adopting modern transport protocols. At AS level, however, DNS is the most common service (61%), particularly amongst operators hosting services on only one or a few IP addresses. This contrast highlights distinct deployment strategies between large CDNs and DNS-focused operators.

II. Background and Related Work

When a user connects to an anycast address, BGP directs the request to a single PoP, typically one that is topologically close to the user [1], from which the service replies. A common misconception is that announcing an address at multiple locations, in itself, is classified as anycast. Many CDNs announce their prefixes at multiple network edges (in different geographic regions), where they route traffic internally to a single PoP hosting the service. Critically, as defined in RFC 4786 [1], anycast is the replication of a service address where several PoPs make the service available.

In this work, we use anycast prefixes from *LACeS*, a daily anycast census covering both IPv4 and IPv6. We use prefixes classified as anycast with high confidence using their latency-based detection method. This method also provides a lower bound of the number of PoPs behind anycast prefixes and their locations using iGreedy [10]. *LACeS* covers both large global anycast networks, such as most DNS root server deployments [11], and small-scale regional anycast networks (*e.g.*, confined within a continent or a country), like those deployed by some country code Top-Level Domain (ccTLD) operators. Finally, *LACeS* covers rare cases of "partial" anycast (*i.e.*, prefixes that contain a mix of replicated and non-replicated IP addresses). For example, they discuss a tier-1 that replicates a DNS resolver on a single IP address, whereas all other IP addresses are internally routed to a single location.

In 2015, Cicalese *et al.* characterized services running on 1 696 IPv4 anycast /24-prefixes announced by 346 distinct ASes [4]. They achieved this using Nmap port scans targeting a single IP address for 897 /24-prefixes within the top 100 ASes, identifying 449 open ports associated with common services. Their results show that DNS is the most common service, found in over 60% of ASes, and most ASes have an open TCP port with HTTP/HTTPS present in over 20%. In this work, we scan all IP addresses within anycast prefixes using ZMap [7], LZR [8], Zgrab2 [9], and QUIC-specific probing [12] to discover ports and detect services. While our port selection is narrower, focusing on well-known ports and protocols, we prioritize accurate service identification across all addresses.

Sattler *et al.* [13] investigated so-called highly responsive prefixes (HRPs) where more than 231 IP addresses within a single /24-prefixes are responsive to TCP scans. They showed that many prefixes originated by CDNs are HRPs and provided guidelines on how to manage such prefixes in measurement studies. Due to the strong CDN bias in anycast (more than 59% [6]), we separately assess HRPs in our results.

In 2021, Sommese *et al.* investigated the adoption of anycast within DNS infrastructure [3], showing an increase in anycast usage for authoritative nameservers. Our work provides an overview of DNS in anycast prefixes, covering authoritative nameservers (including root-servers) and the software used, as well as domain names on anycast from the perspective of generic Top-Level Domains (gTLDs).

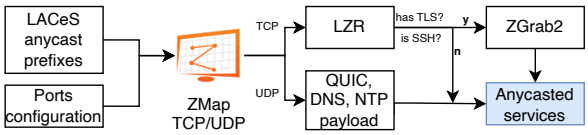

Fig. 1: Measurement pipeline overview.

III. Methodology

In this section, we describe the methodology we use to characterize services hosted on anycast prefixes.

While other service discovery data sets exist, *e.g.*, Censys Universal Internet Data Set (CUIDS) [14], we opt to use our own scanning infrastructure. Due to the distributed nature of anycast, we investigate differences in service deployments amongst PoPs by probing from two VPs on different continents. Although CUIDS is scanned from multiple VPs [14], the data set does not provide information from *which* VP the results are from. Furthermore, prior work indicates that network operators block CUIDS scans more frequently than those originating from academic networks [15]. We make all results collected using our scanning pipeline publicly available for reproducibility and future research [16]. We provide a brief comparison between our measurements and a snapshot of CUIDS from February 3, 2026, in Section V-B.

Our measurement pipeline scans both TCP and UDP ports. For TCP, we detect open ports with ZMap [7], then we proceed with service detection using LZR [8] and ZGrab2 [9]. On UDP ports, we use ZMap's UDP probes and a QUIC probe [12] to force QUIC version negotiation. The TCP and UDP measurements are performed from two VPs, one in the Netherlands and one in Australia. The ZMap and LZR measurements are from February 18th, and the follow-up ZGrab2 measurement is from February 20th, 2026. Fig. 1 provides an overview of our pipeline.

As input, we retrieve anycast prefixes from *LACeS* [6]. Whilst other anycast censuses exist, we chose *LACeS* because it provides an open-source data set that is extensively validated using ground truth. On the TCP scans, we configure our scanning pipeline to use the 100 `nmap`'s most common ports [17], and we complement them with 18 additional ports associated with services that LZR supports. On UDP, we scan the ports 53 (DNS, included in the `nmap`'s common ports), 123 (Network Time Protocol (NTP)), 853 (DNS over QUIC (DoQ)), and 443 (HTTP over QUIC). Port 443 is an exception where we also scan on the TCP protocol.

We instrument LZR to follow the handshake order strategy proposed by Izhikevich *et al.* [8]. Izhikevich *et al.* found that the most efficient initial step is to *wait* for servers to send an initial packet, as certain protocols transmit a banner that can be fingerprinted upon connection (*e.g.*, SSH, FTP, SMTP). If no response is received from the server that can

already be fingerprinted after the handshake, a protocol packet is sent. For ports associated with one of LZR's 32 supported protocols, we structured our handshake sequence to begin with a *wait* step, followed by the port's protocol-specific handshake, and subsequently a fallback sequence consisting of TLS, HTTP, DNS, and Point-to-Point Tunneling Protocol (PPTP) (as the sequence in [8]). This approach prioritizes detecting of expected services while robustly capturing anomalous applications running on standard ports. For ports where LZR lacks specific service support, we directly applied the empirically derived handshake order proposed by Izhikevich *et al.* (Table 2 in [8]). The authors demonstrated that this sequence of five handshakes successfully identifies over 99% of unexpected services, allowing us to optimize our scanning efficiency without sacrificing detection coverage.

We parse the DNS, NTP, and QUIC responses using Python libraries for DNS [18], NTP [19], and QUIC [20], and fingerprint the successfully parsed responses.

LZR can fingerprint services that run with TLS. However, LZR cannot detect whether the scanned host runs, for example, HTTP over TLS (HTTPS). Hence, to detect services running over TLS, we follow up with a ZGrab2 [9] measurement on February 20th targeting the IP addresses and ports where LZR detects TLS. We target the following port/application layer protocols: 443/8443/HTTPS, 465/SMTPS, 990/FTPS, 993/IMAPS, 995/POP3S, and 5671/AMQPS. All other ports we scan as HTTPS, given its prevalence on the Internet.

To verify our findings, we re-ran the pipeline on March 3rd, 2026, adding a third VP in Germany. This allowed us to rule out measurement anomalies (*e.g.*, blocked scans) that may have affected our initial campaign of February 18th [21]. We then compare the Dutch VP against the Australian one, and the German VP against the Australian one, and discuss the results in Section V-D.

LZR does not provide the SSH host keys needed to determine whether we are connecting to the same physical machine across different PoPs. To determine whether our VP reaches the same physical machine, we conducted an additional ZGrab2 scan on March 5th, 2026, to retrieve and compare SSH host keys (see Section V-B).

We detect highly responsive anycast prefixes in our data set according to Sattler *et al.* [13], *i.e.*, /24-prefixes with more than 231 IP addresses responsive to TCP-SYN from ZMap measurements. We aggregated across all the ports we scan, *i.e.*, all distinct IP addresses that respond to ZMap scans on all ports. Throughout our analysis, we refer to *active IPs* as the IP addresses we detect at least one service based on LZR's and ZGrab2's outputs. We also use the term *IP utilization*, which is the ratio of *active IPs* over the total number of responsive IPs in a prefix.

Limitations – Our pipeline focuses on IPv4 addresses, despite the growth in IPv6. On one hand, scanning all IPv6 addresses in anycast prefixes is infeasible. On the other hand, the current IPv6 hitlist data sets are biased towards specific services based on their creation methodology, *e.g.*, derived from domain names extracted from different sources [22], [23] or from known-service ports such as 80, 443 and 53 [24]. Hence, our analysis would highly biased towards Web and DNS services.

Since *LACeS* detects anycast using ICMP and transport-layer measurements, it may lead to false inferences regarding service-layer replication. For instance, operators with a private backbone may configure their PoPs (at the edges of their networks) to respond to pings, whereas service-layer traffic is tunneled to a single location from which the service is provided. We accept this potential overestimation of service-layer replication because there are no service-layer-aware anycast censuses.

LZR has a limit of 32 different common protocols. Hence, we lack coverage for other protocols. However, Izhikevich *et al.* [8] showed that across all ports they scanned, nearly "65% of unexpected, but identifiable, services speak HTTP and 30% speak TLS". Hence, our results are a lower bound, but we cover a high number of services hosted on anycast prefixes. Our scans characterize the use of anycast networks, however establish ownership of all hosted services is not trivial, and we can do so, for instance, in our email analysis in Section V-B.

While additional VPs could improve the results, we limit our study to two VPs, complemented by a third for validation. Scanning services from many VPs can impose a burden on network operators. Hence, our analysis of regional services is limited by the use of only a few VPs. Moreover, two VPs on different continents have high chances to hit different anycast endpoints, thereby covering a large set of anycast sites for our service characterization.

IV. Anycast Deployment Strategies

This section investigates the various deployment strategies used by anycast operators to deploy their services. We use a single *LACeS* snapshot, collected on February 18th, 2026, for this analysis. On this day, 14 346 IPv4 /24-prefixes and 13 007 IPv6 /48-prefixes were detected as anycast with confidence.

A. Anycast Topology

To evaluate the upstream ASes for anycast prefixes, we use upstream data from *bgp.tools* which contains 7 442 routed prefixes (4 685 IPv4 and 2 757 IPv6 prefixes) that cover the *LACeS* /24-and /48-prefixes. We use *bgp.tools* as they rely on many BGP sessions (3×10^3 [25]) to maximize visibility for used upstreams. Furthermore, unlike AS relationship data sets, the shared data set reports upstreams for each prefix separately. For example, the University of Maryland (AS 10886) has different upstreams for its anycast prefix 199.7.91.0/24 (D-root), and its on-premise university ranges, where the AS relationship data would include upstreams for both prefixes.

For anycast prefixes, we find tier-1 transit networks to be the most common upstreams (see Table V in Appendix C). We also find 37% of IPv4 and 29% of IPv6 routed prefixes with only a single upstream. This is surprising, as one would expect anycast ASes to have a large variety of upstreams due to their distributed nature.

Fig. 2 plots the most frequent upstreams for single-upstream anycast ASes alongside the total customer anycast

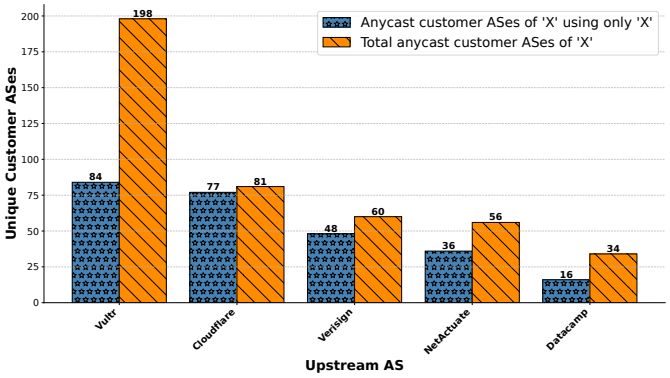

Fig. 2: Most common upstreams for single-upstream anycast ASes.

ASes for that upstream. These links mostly include customer-provider relationships for BYOAS customers, where operators announce their own ASN and prefix using a provider's infrastructure (with the provider ASN being their only upstream).

We find 198 ASes use Vultr as upstream to make use of anycast. Furthermore, 84 out of these entirely use Vultr (as a single provider). Next, we have 77 ASes that replicate their services solely using Cloudflare and 36 that deploy entirely using NetActuate.

We also observe Verisign with 60 customer ASes, which are same-organization links for their Multi-Origin AS (MOAS) anycast infrastructure. RFC 6382 describes using multiple ASNs for a single anycast prefix (one per PoP) via MOASes [26]. This practice allows anycast operators, *e.g.*, to have a unique identifier for each PoP in routing data, to assist with traffic engineering, or to deploy an anycast service across multiple organizations.

Previous work by Sediqi et al. [27] looked at long-lived MOASes, and found they were rarely used for anycast. We find similar results, as only 204 IPv4 and 111 IPv6 anycast prefixes have multiple AS origins. Of these, 65% consist of 2 origin ASes, 14% have between 2 and 8 origins, and 35% range from 8 to 15. Lastly, we find that most belong to Verisign (authoritative for many TLDs and author of RFC 6382). We suspect the relatively low adoption of MOASes for anycast is caused by the operational complexity of maintaining and deploying multiple ASes.

Key takeaways: A substantial fraction of anycast prefixes use a single upstream provider (37% for IPv4 and 29% for IPv6), many of which rely on provider-based BYOAS models. BYOAS providers such as Vultr, Cloudflare, and NetActuate are often used by ASes to deploy anycast infrastructure.

B. Geographic Placement Strategies

Alongside detection, *LACeS* also enumerates and geolocates anycast prefixes using iGreedy [10]. However, iGreedy's performance depends on the distribution of VPs used and has known limitations like struggling to differentiate between PoPs in close geographical proximity. To mitigate these limitations, we only look whether an anycast AS has presence within subregions (as defined by the United Nations [28]) that span large

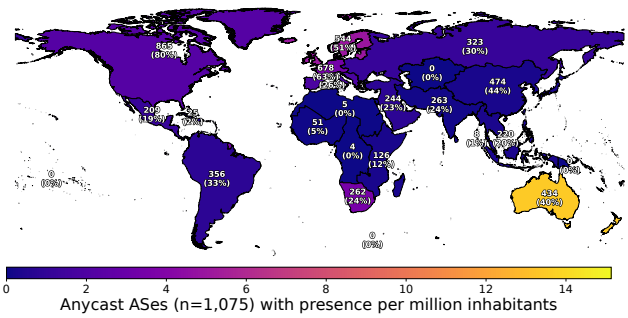

Fig. 3: Heatmap of the number of anycast ASes with presence in each subregion, normalized by millions of inhabitants.

TABLE I: Regional deployment scope of ASes (n=1 075) with IPv4 anycast /24-prefixes (n=14 346) observed by *LACeS*.

Deployment Scope	ASes	/24-Prefixes
Global (multi-continent)	794 (74%)	13 135 (92%)
Single continent	381 (35%)	1 211 (8%)
Single country	245 (23%)	769 (5%)
Single-continent deployments by region (ASes=381*, /24s*=1 211*)*		
North America	196 (51%)	724 (60%)
Europe	119 (31%)	223 (18%)
Asia	51 (13%)	128 (11%)
Oceania	46 (12%)	122 (10%)
South America	10 (3%)	12 (1%)
Africa	2 (1%)	2 (0%)

geographic areas where operator presence is more reliably detected in *LACeS*.

1) Global PoP placement: Fig. 3 shows the number of anycast ASes with presence in each subregion. We find most operators have presence in North America (80%), Western Europe (63%), and Northern Europe (51%). Other subregions, such as Central America, Africa (except Southern Africa), Central Asia, and the Pacific Islands, have a sparse presence.

To assess whether anycast deployment is equitable, we normalize presence by population count (using UN estimates [29]). We find the Australia and New Zealand subregion to be the most represented by far. We attribute this to the sparse population of this subregion, combined with its large digital economy.

South American and Eastern Asia have a considerable number of ASes with presence (33% and 44% respectively) but are underserved when considering their large population.

These results show deployment differences where operators are likely to have presence in some subregions but appear lacking in others. We leave a more detailed analysis of anycast in underserved regions to future work

2) Regional Anycast: LACeS provides geolocation data for 1 075 ASes deploying IPv4 anycast, some of which are "regional", which we define as anycasted within a single continent or country. Table I provides a breakdown of the geographic deployment scope of anycast ASes and prefixes.

We find 74% of ASes have at least one prefix with global presence (*i.e.*, spanning multiple continents), and 35% have a prefix within a continent. For these ASes announcing prefixes within a single continent, we find 51% have prefixes confined

TABLE II: Largest ASes by number of active IPs, alongside the number of /24s and active IP & HRP ratios.

Org (ASN)	Active IPs	/24s	Active IP ratio	HRP Ratio
Cloudflare (13335)	658×10^3	2 866	0.896	0.989
Google (396982)	492×10^3	4 298	0.447	0.973
Fastly (54113)	209×10^3	827	0.989	0.990
AWS (16509)	133×10^3	1 603	0.325	0.260
Cloudflare (209242)	60×10^3	270	0.862	0.967
Fly.io (40509)	22×10^3	223	0.387	1.000
GoDaddy (398787)	16×10^3	64	1.000	1.000
AceVille (139341)	13×10^3	118	0.430	0.805
Vercara (12008)	12×10^3	98	0.459	0.449
Nazwa.pl (15967)	11×10^3	195	0.224	0.959

to North America, 31% confined to Europe, 13% confined to Asia, 12% confined to Oceania, and less than 5% confined to South America and Africa. This shows many ASes deploy regional anycast and highlights the bias of operators to deploy in North America and Europe whereas few deploy inside of South America and Africa.

Notably, 23 ASes (mostly CDNs) announce regional anycast prefixes within multiple continents (see Table VI in Appendix D). For example, AWS (AS 16509) has distinct regional deployments in five continents.

Previous work on regional IP anycast [30] identifies that CDN operators deploy regional anycast to ensure clients route to geographically nearby PoPs, reducing latency and improving performance whilst benefiting from the resilience anycast offers. We also observe ccTLD operators that confine anycast nameservers to their respective region (*e.g.*, *.nz* has multiple anycast nameservers confined to New Zealand [31]).

Key takeaways: When normalized by population, deployment is unequal with the Australia and New Zealand subregion overrepresented while, *e.g.*, subregions in Africa, South America, and Eastern Asia are underserved. Whilst most ASes (74%) deploy anycast globally, we find regional anycast is widespread with 35% of ASes having at least one anycast prefix confined to a single continent.

C. IP utilization

Unlike previous work, that only measured a single IP address per prefix [4], we scan prefixes in their entirety allowing us to assess the IP utilization of anycast. In total, our scanning reveals 1.77×10^6 addresses with active services within *LACeS* prefixes. These prefixes cover 1 223 distinct ASes of which 1 075 announce IPv4, 579 announce IPv6 anycast, and 431 announce both IPv4 and IPv6 anycast. However, as stated by Hendriks et al. *LACeS* has limited coverage for IPv6 due to hitlist limitations [6], and we suspect the actual number of ASes announcing IPv6 anycast to be higher.

Table II shows the largest ASes by number of anycasted IPv4 addresses with active services found using our pipeline alongside the number of /24-prefixes they originate.

We also include the IP utilization and HRP ratios. The former is the ratio of active IPs, *i.e.* with detected active services, the latter is the ratio of HRP /24-prefixes [13]. In total, 9.7×10^3 /24s (68%) are classified as HRP for which

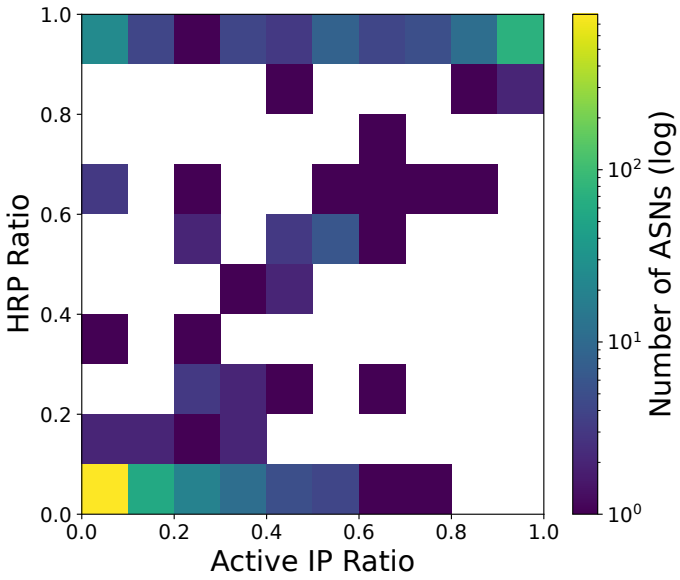

Fig. 4: Heatmap of HRP ratio against active IP ratio for anycast ASes (IPv4 only).

we find an average IP utilization of 42% compared to 12% for non-HRP prefixes. Thus, while for HRPs a majority of IP addresses result in a successful TCP handshake, a valid service can only be identified for 42% of addresses.

Hendriks *et al.* showed a clear dominance of so-called hypergiants where the top five ASes announce roughly two-thirds of all anycast /24-prefixes [6]. We find this is even more centralized as 88% of active IPs are originated by these top five ASes, due to their high IP utilization.

For Cloudflare, Fastly, and GoDaddy, we find high IP utilization and HRP ratios, with Cloudflare originating 37% of active anycast IP addresses. Despite an IP utilization of 45%, Google has the second-most active IP addresses (28%) as they originate the most /24-prefixes. This suggests Google can provision the same number of services using fewer prefixes.

For IPv6, we find Cloudflare (AS 209242) to originate 49% of /48s (see Table IV in Appendix B. We do not know the active IP ratio for IPv6 prefixes, due to the large number of addresses in /48-prefixes, which makes scanning impossible.

These results show that most active anycast IPs are hosted by a few ASes that originate the majority of prefixes, which are also classified as HRP with high IP utilization. For this reason, we will separately consider HRP prefixes in parts of our presented results.

Fig. 4 shows the correlation between HRP and active IP ratios for IPv4 anycast ASes. We find the majority of ASes have a low active IP and HRP ratio (bottom left), as we discuss later in §V, these are mostly ASes deploying DNS. Next, we find a considerable number of ASes with high HRP and active IP ratio (top right), these are hypergiant ASes like Cloudflare, Fastly, and GoDaddy, as seen in Table II.

Interestingly, we observe 31 ASes that deploy HRP with few active IPs (top left), mostly CDN operators based on manual inspection. In the bottom-right corner, we find FastHosts (AS 15418) and InternetNamesForBusiness (AS 14116), both

TABLE III: Transport protocols (filtered post-HRP classification). Columns show *active IPs*, /24-prefix with *active IPs*, and ASes with at least one prefix with detected service.

	Services (IP)	Services (/24)	Services (ASes)
HRP	1.6×10^6	9.4×10^3	177
TCP	895.2×10^3 (55%)	9.2×10^3 (98%)	153 (86%)
UDP	65.4×10^3 (4%)	591 (6%)	65 (37%)
QUIC	1.1×10^6 (66%)	4.9×10^3 (53%)	89 (51%)
Non-HRP	141.9×10^3	3.8×10^3	823
TCP	113×10^3 (80%)	2.4×10^3 (63%)	535 (65%)
UDP	30.9×10^3 (22%)	2.4×10^3 (64%)	646 (78%)
QUIC	3.5×10^3 (2%)	651 (17%)	93 (11%)

with high IP utilization and no HRP. They use anycast DNS infrastructure as domain registrars (not classified as HRP, which is based on open TCP ports). In the center, we find 13 ASes that deploy a near-even split of HRP and non-HRP prefixes. The largest of which are Vercara (AS 12008), a subsidiary of DigiCert, and Alibaba (AS 24429), both offering a large variety of services including DNS and DDoS protection.

Key takeaways: The top five ASes control 88% of anycast IPv4 addresses hosting services due to high IP utilization rates. Conversely, most ASes have few active anycast IP addresses.

V. Service Discovery

In this section, we provide a comprehensive overview of services on anycast, focusing on the most relevant and interesting ones. We show the correlation of services and network operators, and how services are replicated. Finally, we analyze the differences in accessing a service from different VPs. We detect and group the responsiveness of anycast prefixes in our data set according to Sattler *et al.* [13]. The results we present are based on the merged measurements of February 18th and 20th (pipeline) from one VP in the Netherlands. We mention when additional data from other campaigns is used.

A. Transport Layer

We see that for 96% of all /24 anycast prefixes, at least one IP address hosts at least one service. Overall, HRPs and non-HRPs exhibit different protocol preferences. Table III shows a breakdown of IP addresses, prefixes, and ASes that have a service running for each transport-layer protocol. We group by responsiveness (HRP and non-HRP), and we show the *active IPs*, the /24-prefixes with at least one *active IP*, and the ASes with at least one /24-prefix where we detect a service.

Similar to prior work [13], we find a low prevalence of UDP services compared to TCP on HRPs. In contrast, UDP services such as DNS and NTP present in anycast prefixes are comparable to TCP on non-HRPs. We further investigate DNS and NTP in Section V-B. We observe a longer tail of ASes in the non-HRPs group that host UDP services, compared to the HRPs group. The scenario changes when we look at the HRP group, where CloudFlare accounts for 49% of the prefixes supporting UDP services, suggesting centralization.

Our measurements show a significant deployment of QUIC. For instance, 42% of anycast prefixes host QUIC on at least one IP address. Among HRPs, TCP and QUIC dominate deployments and appear at comparable numbers. While we detect TCP services on 55% of IP addresses, QUIC appears even more frequently (66%). At the prefix level, TCP is nearly on all HRP (98%), whereas QUIC is present in 53%. This indicates that QUIC prefixes are more dense, *i.e.*, with more active IP addresses than TCP prefixes. However, a smaller number of ASes have at least one prefix with a QUIC service compared to ASes on TCP services. Hence, QUIC distribution is skewed on fewer ASes (51% vs 86% on TCP for HRPs), with CloudFlare, Google, Amazon, and Fastly being the most common providers. We show later in Section V-B that these are largely used for Web.

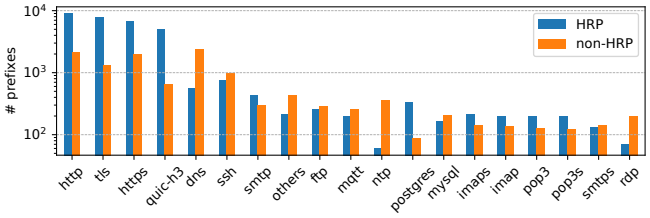

Fig. 5: Services identified on anycast prefixes.

Servers negotiate different QUIC versions with clients. Among anycast prefixes supporting QUIC on port 443, 98% accept version 1, roughly 40% accept a draft QUIC version, and only 6% accept version 2. QUIC deployment on port 853 is limited: 97% (32) of anycast prefixes negotiate version 1. Version 2 is recent (May 2023) and was introduced to mitigate protocol ossification and exercise version negotiation. Version downgrade from 2 to 1 poses no known security risk [32].

Key takeaways: Nearly all (96%) anycast prefixes host at least one service. QUIC has substantial adoption with comparable numbers to TCP at IP address level, though QUIC is concentrated in a handful of large providers (CloudFlare, Google, Amazon, and Fastly).

B. Application Layer

We depict the services we find in Fig. 5. Among common established deployments on anycast prefixes such as web services (HTTP/HTTPS) and DNS, we find SSH, mail services (*e.g.*, SMTP), and databases (*e.g.*, MySQL and PostgreSQL). We classify TLS-based services by their specific application protocol (*e.g.*, HTTPS) when ZGrab succeeds with an application-layer handshake. Otherwise, we categorize them broadly as "tls". We categorize services found in fewer than 100 prefixes as "other" since these are a small fraction of anycast services. For instance, Modbus, Siemens S7 (industrial control), VNC (remote desktop), RTSP (streaming), and Telnet are publicly visible on the Internet, which is surprising.

We analyze the detected open ports and their underlying protocols to evaluate how strictly anycast networks adhere to IANA port assignments [33]. Across all measured ports, 84% of identified services run the expected protocol. Excluding the highly prevalent TLS and HTTP services increases adherence to 94%. As in prior work [8], we observe that port 80 responds

to HTTP in 93% of cases. Services on anycast prefixes are likely commercial and user-facing, leading to the high port-protocol adherence we observe.

Web – We find that the majority of anycast is used to replicate web servers (running HTTP/HTTP(s) or HTTP/3 with QUIC). In total, 86% of /24s prefixes, and 56% (553) of ASes have a web service hosted, while 42% prefixes and 16% (165) of ASes have HTTP/3 services. We find that web services are also hosted on ports 8080 and 8443 (22%) and on other non-standard ports (15%), in addition to the common ports (80 and 443). While prior work [13] observed a high prevalence of web services on HRP, this trend also extends to anycast deployments. Web content can benefit from replication using anycast [34], [35]. For instance, CloudFlare functions as a reverse proxy, caching content across various geographic locations to ensure proximity to the user [36].

DNS – We observe that DNS is largely deployed via anycast on 22% (2.9×10^3) of prefixes, covering 61% (658) ASes, with most DNS servers on non-HRPs (80%). The top DNS providers include Amazon (15% of /24-prefixes), Identity Digital (7%), CloudFlare (3%), NetActuate (3%), and Vercara (3%), which are big DNS providers. We find DNS over QUIC (UDP/853) deployments in small numbers (1 338 IPs), where 95% of the IP addresses originate from NextDNS (AS34939). By querying `CHAOS TXT` records from multiple VPs, we find 25 ASes (including root server and ccTLD operators) run different DNS software across PoPs sharing the same anycast address (detailed in Appendix E).

To investigate the dependency of DNS on anycast, we look at registered domain names under well over 1000 legacy and new gTLDs using *OpenINTEL* data [23]. The data set is from February 18th, 2026, with 204.1×10^6 domains. We label domain names as using anycast based on whether all the domain's authoritative name server A records match anycast prefixes in our data set, unicast if none match, or a mix of both. We find that 72% of domains rely on at least one anycast authoritative name server, while 4% rely on a mix of anycast and unicast authoritative name servers. Mix deployments can result in higher DNS name resolution latency [37]. Sommese *et al.* studied anycast adoption in authoritative DNS in 2021. We see that anycast adoption grew (57% in 2021) and mix deployments decreased (5% in 2021). Our data set includes 43% more /24 anycast prefixes than in 2021, which may contribute to the observed growth. In the Sommese *et al.* study, they aggregate ccTLDs in their analysis, but these are closed data and difficult to obtain. We argue that gTLDs provide a generic yet comprehensive view of global trends in DNS, given their size in terms of domain names. We look at the effect of adding open ccTLDs (*e.g.*, `.ch` and `.se`, 3.7×10^6 domain names) and we find marginal changes (<1%).

We observe that 28% of domain names in our gTLD data set rely on Host Europe, 22% on CloudFlare, 8% on Google, 5% on Vercara, and 3% on IONOS. Thus, many gTLD domains rely on a few anycast DNS providers.

SSH – Surprisingly, we see SSH servers in anycast prefixes: 13% (1.7×10^3) of prefixes across 20% (215) ASes. SSH is typically used for remote management or as a proxy to a remote machine, where service replication across anycast nodes is counterintuitive. To determine whether our VPs reaches the same physical machine, we conducted an additional ZGrab2 scan on March 5th, 2026, collecting SSH host keys. However, if system administrators reuse the same host key when creating a new anycast node, different machines may end up with identical keys. We find 70 IP addresses where the VP see a different key, suggesting different machines. Furthermore, this practice suggests that clients may connect to different SSH servers, based on their location (the nearest node), as we suspect SSH is not replicated. Operationally, SSH should use unicast addresses of the machine on which it is configured. However, if misconfigured, SSH may be unintentionally exposed to anycast address due to the OpenSSH daemon, which listens on all local addresses by default [38].

Mail – We detect IMAP(s) or POP3(s) on 376 (3%) anycast prefixes and SMTP(s) on 746 (6%). Mail infrastructure is consolidated, with just five providers–Nazwa.pl, Amazon, Google, OVH, and Fly.io–accounting for 70% of the identified mail services. Since POP3 and IMAP are used to store and retrieve email, we cannot determine whether the deployments are fully replicated backend mail or they function as edge proxies [39] distributed across multiple locations. We find 2 346 anycast IP addresses hosting SMTPS on port 465, which is used for secure mail communication between clients and mail servers (submission) [40]. We inspect the TLS certificates of these servers to understand what type of email servers they are. We observe a long tail distribution, where 46% IPs have certificates with *smtp.gmail.com* as subject name, under Google's infrastructure (AS15169), where the certificates are issued by Google Trust Services WR4 [41], and valid for 90 days, suggesting *Gmail* instances. Following, 6% have certificates with *netart.com* as subject name, under Nazwa.pl (AS15967), where the certificate is issued by *netartSSL*.

Other notable services – We observe a few instances of NTP servers. 3% of prefixes (420) are spread across 13% of ASes (144), with the majority being deployed in non-HRP (360 cases). In total, we find 1 951 IP addresses hosting NTP. While NTP can be deployed using anycast, operational challenges exist [42], including time inconsistencies caused by routing changes, the inability for clients to distinguish between servers sharing the same anycast address, and the need for multiple independent server addresses despite anycast deployment.

Surprisingly, we also detect database services such as MySQL, PostgreSQL, Redis, MsSQL, MongoDB, and OracleDB on anycast prefixes. We find in 5% (726) of the prefixes and 5% (54) of the ASes. 86% of the anycast prefixes are from Nazwa.pl, Amazon, Google, OVH, or Fly.io. Deploying databases over anycast is generally discouraged, as these services rely on long-lived connections that are susceptible to disruption from anycast routing changes [1]. We suspect that these servers are in a single location where the anycast data set measurements reach their different endpoints. Furthermore,

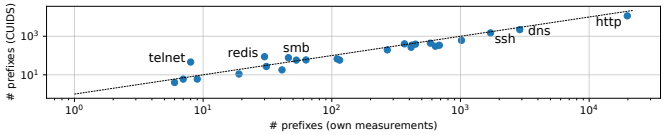

Fig. 6: Comparison of services identified by our own measurements and CUIDS on anycast prefixes.

we suspect that the exposure of databases to the Internet stems from broad interface binding configurations. For instance, binding MySQL to `0.0.0.0` [43] or using the ⋆ wildcard in PostgreSQL [44] causes the daemon to listen on all available local addresses. However, these are not default configurations, and online tutorials incorrectly recommend them, allowing their users to remotely access the database [45].

CUIDS comparison – We compare CUIDS with our measurements by selecting the same ports and services included in our analysis. We find more services on anycast prefixes compared to CUIDS, and show a comparison of the overlapping services we find with our measurements and with CUIDS in Fig. 6. There are three notable exceptions where CUIDS reports substantially more prefixes: telnet (46 vs. 8), redis (87 vs. 30), and SMB (77 vs. 46). Excluding these three outliers, we observe 47% more prefixes per service on average. For example, for HTTP(S), our measurements identify 73% more prefixes (19.8×10^3 vs. 11.4×10^3). We find 46% more prefixes than CUIDS hosting QUIC. Scan blocking may be one contributor [15]. Unfortunately, without an exact understanding of CUIDS' measurement campaigns, it is not possible for us to investigate further potential reasons.

Key takeaways: Anycast prefixes prominently replicate web services. The DNS infrastructure reveals growing reliance on anycast: 72% of gTLD domains rely on at least one anycast authoritative name server, 15% increase since 2021. At the same time, consolidation is evident, as Host Europe, Cloudflare, and Google together operate 58% of gTLD domains that run exclusively on anycast infrastructure. We find SSH and databases on anycast, potentially due to misconfigurations.

C. Services, Operators and Resilience

We investigate the leading operators hosting services on anycast prefixes. As shown in Fig. 7, CloudFlare, Google, and Fastly dominate the web services detected on anycast, since they operate large CDN and edge computing platforms that heavily rely on anycast to replicate content across their global infrastructure. Alongside Identity Digital, Amazon hosts the largest share of DNS services. As a major domain registry and registrar, Identity Digital relies on anycast to provide authoritative DNS for the top-level domains it manages.

We find that 1.5×10^3 prefixes exclusively host DNS, outnumbering other single-service deployments (52%). Anycast prefixes can be utilized such that one IP address associated with a service is covered by one advertised prefix (single service on the prefix) or alternatively multiple services are covered by the same prefix [1]. Operationally, hosting multiple services in the same anycast prefix offers advantages in

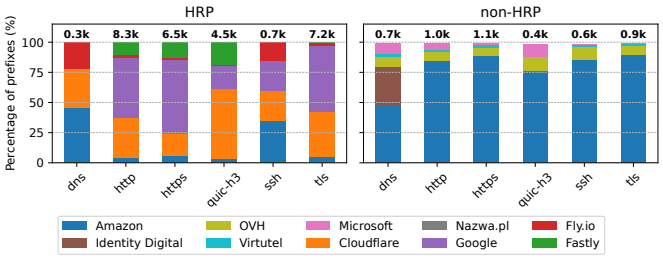

Fig. 7: Top 10 ASes based on unique prefixes with services and the top services.

resource utilization and scalability, whereas hosting a single service is used for a small number of critical infrastructure services [1]. Single-service prefixes' isolation strategy helps for DDoS mitigation, as it enables operators to drop malicious traffic at the network edge, for instance, via BGP blackholing [46], without causing latency effects on unrelated services, as clients would be routed to another less optimal PoP.

Fig. 8 correlates our identified services with the number of anycast prefix PoPs from *LACeS*. Our result suggests a trimodal deployment distribution characteristic for anycast, a sign of different operational strategies. The three clusters correspond to services replicated on $<$15, between 15 and 50, and $\geq$50 PoPs. Fastly leads the first cluster, followed by Afilias and Nazwa.pl, with a long tail of 921 other ASes. The second cluster is also lead by Fastly, followed by Fly.io and Vercara, with other 147 ASes. The third cluster is concentrated around Google, CloudFlare and Amazon, followed by other 90 ASes.

Interestingly, we find the vast majority of services with a PoP count of more than 50 (third cluster) originate from few operators (CloudFlare, Google, and Amazon AWS). When excluding these operators, we find the vast majority of deployments have fewer than 50 PoPs detected in the *LACeS* data set. Such pattern is not applicable to the first and second clusters when we exclude the top three ASes of the given cluster. This suggests that deployments with $\geq$50 PoPs are best understood as a contribution of a few operators and the services they replicate whereas deployments with fewer PoPs have a large operator diversity.

We observe that web services on anycast are predominantly hosted on hypergiant infrastructure (third cluster), where anycast HRPs are prevalent. For DNS, deployments are concentrated on non-HRP prefixes (1.5×10^3, 65%) and replicated across different numbers of PoPs. Email on the contrary is mainly seen on infrastructures with $\leq$50 PoPs.

We analyze services in 1 211 prefixes anycasted within a single continent based on *LACeS* to evaluate the regional deployment patterns. North America hosts the most DNS overall (21%), followed by Europe (10%). However, web services lead the anycast deployment across the continents. QUIC is present in high numbers in North America (19%), but surprisingly not much in Europe (1%) or Asia (2%). Overall, these results suggest that regional anycast deployments are primarily used to support web services, and that Europe lags behind in local modern web service provision (*e.g.*, QUIC).

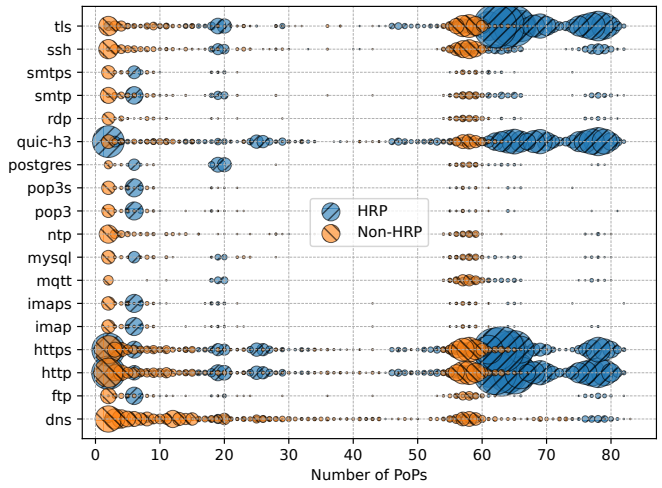

Fig. 8: Distribution of number of PoPs for each service.

DNS infrastructure is in smaller numbers across the regions. However, initiatives to regionalize DNS have been taken. For example, *DNS4EU* replicates DNS resolvers within Europe [47]. With ongoing discussions on data sovereignty [48], we may see more operators deploy regional anycast within their jurisdiction.

Key takeaway: Anycast hosting is dominated by Google, Cloudflare, and Fastly for web services, and by Amazon and Identity Digital for DNS. Web services concentrated on large-scale hypergiant infrastructure (>50 PoPs), DNS spread across different scales and email on small and medium infrastructure (≤50 PoPs). DNS show small presence across regions, however sovereignty-driven initiatives like *DNS4EU* may push more operators toward future regionalized anycast.

D. Distributed Port Scanning

To understand how service visibility varies by location, we compare the services detected on anycast prefixes from our Dutch and Australian VPs using a snapshot of February 18th, 2026. We find that 4% (560) of the prefixes classified as HRPs from Australia are entirely unresponsive to TCP or UDP probes from the Netherlands. Within this unresponsive subset, we detect services on only 44 distinct prefixes (<1% of all anycast prefixes), the majority of which are DNS (37%, 24 prefixes). Furthermore, roughly 30% (4×10^3) of the prefixes classified as anycast HRPs from Australia do respond to TCP and UDP probes from the Netherlands, yet fail to meet the HRP criteria from the Dutch VP. We observe that 80% of such prefixes have 151 or fewer TCP-responsive IP addresses, indicating that the entire prefix is not blocked, but rather that a portion of the IP addresses are not served to the Dutch VP.

To quantify overall measurement consistency, we calculate the Jaccard similarity index–the intersection of prefixes of a given detected service over their union–across the different VPs. We observe an average similarity of 0.8, indicating that services are mostly deployed on the same prefixes regardless of the observer's location. We suspect that discrepancies in service visibility can be attributable to unpredictable, transient network issues, as found in prior work [15]. For instance, Wan *et al.* observed that hosts are transiently inaccessible when the host was inaccessible from one VP but accessible (completed application-layer handshake) from a different VP, which is similar to what we observe with the 44 prefixes we see a service in Australia but not in the Netherlands.

We validate our findings with a follow-up measurement on March 3rd, 2026, by adding a third VP in Germany. Results are consistent with the February 18th measurement, in which the German VP and the Australian VP show a Jaccard index of 0.9, with HTTP mostly affected. However, we still observe a high dominance of web services on anycast, and hence, this measurement artifact does not change our overall conclusions.

Key takeaway: Service visibility is consistent across our VPs. However, location-dependent gaps do exist: 4% of HRPs visible from Australia are unresponsive from the Netherlands, and another 30% respond but fall below the HRP threshold due to partial IP-level reachability rather than full prefix blocking.

VI. Summary and Conclusions

This paper provides a comprehensive characterization of anycast, analyzing both the deployment strategies operators use and the services they replicate. We use a service-aware scanning pipeline to measure replicated services from multiple VPs using ZMap, LZR, and ZGrab2.

Despite 1×10^3 ASes deploying anycast, we find that only five ASes account for over 88% of anycast IP addresses hosting services, as most operators announce prefixes with only a few active addresses. Furthermore, five operators (including Cloudflare) account for 61% of anycast DNS deployments and 72% of domain names under gTLDs rely on authoritative name servers deployed on anycast infrastructure. We identify that BYOAS is commonly used, with 18% of ASes using a single BYOAS provider, and 77 ASes deploy anycast prefixes solely with Cloudflare. Hence, disruptions or attacks targeting Cloudflare's anycast network [49], [50] could extend beyond its direct customers, such as 22% of domain names under gTLD, to potentially affect Cloudflare's 77 downstream anycast ASes. This consolidation creates significant dependencies on a few operators, potentially lowering the ecosystem's resilience.

Web services are the most common services hosted on anycast prefixes, with a few ASes deploying QUIC, indicating that these hypergiants are adopting modern technologies to improve web content delivery.

Our results show regional anycast is widespread, with 35% of ASes providing replicated services within a continent. Hence, anycast is not just used for global redundancy, but also for localized content.

Acknowledgment

We thank both our shepherd, Stephen Strowes, and the reviewers for their valuable feedback that improved our paper.

This work was supported by INTERSCT (NWO grant NWA.1160.18.301), CATRIN (NWA.1215.18.003), Catalyst (funding provided by the New Zealand Ministry of Business Innovation and Employment and administered by the

Royal Society Te Apārangi) and the European Commission's GÉANT GN5-2 Project.

We thank Ben Cartwright-Cox for providing data from bgp.tools, Raffaele Sommese for his assistance with DNS data from *OpenINTEL* and, Grant Williams and Liz Izhikevich to point to a public functional branch of LZR. We acknowledge the support of Censys for providing access to their data. This research was enabled by *OpenINTEL*, a joint project of the University of Twente, SURF, SIDN, and NLnet Labs. Any views and opinions expressed in this work are those of the authors and do not necessarily reflect those of the Dutch research funding agency NWO, which cannot be held responsible for them.

REFERENCES

[1] K. E. Lindqvist and J. Abley, "Operation of Anycast Services," Internet Engineering Task Force, RFC 4786, 2006. [Online]. Available: https://www.rfc-editor.org/info/rfc4786

[2] T. Mendez, W. Milliken, and D. C. Partridge, "Host Anycasting Service," Internet Engineering Task Force, RFC 1546, 1993. [Online]. Available: https://www.rfc-editor.org/info/rfc1546

[3] R. Sommese, G. Akiwate, M. Jonker, G. C. Moura, M. Davids, R. v. Rijswijk-Deij, G. M. Voelker, S. Savage, A. Sperotto *et al.*, "Characterization of anycast adoption in the dns authoritative infrastructure," in *TMA*. ACM, 2021.

[4] D. Cicalese, J. Augé, D. Joumblatt, T. Friedman, and D. Rossi, "Characterizing ipv4 anycast adoption and deployment," in *Proc. CoNEXT*. New York, NY, USA: ACM, 2015. [Online]. Available: https://doi.org/10.1145/2716281.2836101

[5] D. Giordano, D. Cicalese, A. Finamore, M. Mellia, M. Munafò, D. Z. Joumblatt, and D. Rossi, "A First Characterization of Anycast Traffic from Passive Traces," *TMA*, 2016.

[6] R. Hendriks, M. Luckie, M. Jonker, R. Sommese, and R. van Rijswijk-Deij, "Laces: An open, fast, responsible and efficient longitudinal anycast census system," in *Proc. IMC*. ACM, 2025. [Online]. Available: https://doi.org/10.1145/3730567.3764484

[7] Z. Durumeric, E. Wustrow, and J. A. Halderman, "ZMap: Fast internet-wide scanning and its security applications," in *USENIX Security*, 2013. [Online]. Available: https://www.usenix.org/conference/usenixsecurity13/technical-sessions/paper/durumeric

[8] L. Izhikevich, R. Teixeira, and Z. Durumeric, "LZR: Identifying unexpected internet services," in *USENIX Security*, 2021. [Online]. Available: https://www.usenix.org/conference/usenixsecurity21/presentation/izhikevich

[9] Z. Durumeric, D. Adrian, A. Mirian, M. Bailey, and J. A. Halderman, "A search engine backed by internet-wide scanning," in *Proc. SIGSAC CCS*. ACM, 2015. [Online]. Available: https://doi.org/10.1145/2810103.2813703

[10] D. Cicalese, D. Joumblatt, D. Rossi, M.-O. Buob, J. Augé, and T. Friedman, "A fistful of pings: Accurate and lightweight anycast enumeration and geolocation," in *IEEE Conference on Computer Communications (INFOCOM)*, 2015.

[11] "Root Server Technical Operations Association — root-servers.org," https://root-servers.org/, [Accessed 2026-02-06].

[12] J. Zirngibl, P. Buschmann, P. Sattler, B. Jaeger, J. Aulbach, and G. Carle, "It's over 9000: Analyzing early quic deployments with the standardization on the horizon," in *Proc. IMC*. ACM, 2021.

[13] P. Sattler, J. Zirngibl, M. Jonker, O. Gasser, G. Carle, and R. Holz, "Packed to the brim: Investigating the impact of highly responsive prefixes on internet-wide measurement campaigns," *Proc. Netw.*, no. CoNEXT3, 2023. [Online]. Available: https://doi.org/10.1145/3629146

[14] Z. Durumeric, H. Clark, J. Cody, E. Cubit, M. Ellison, L. Izhikevich, and A. Mirian, "Censys: A map of internet hosts and services," *Proc. SIGCOMM Conference*, 2025. [Online]. Available: https://doi.org/10.1145/3718958.3754344

[15] G. Wan, L. Izhikevich, D. Adrian, K. Yoshioka, R. Holz, C. Rossow, and Z. Durumeric, "On the origin of scanning: The impact of location on internet-wide scans," in *Proc. IMC*. ACM, 2020. [Online]. Available: https://doi.org/10.1145/3419394.3424214

[16] G. Luvizotto Cesar, R. Hendriks, M. Angelov, M. Jonker, R. van Rijswijk-Deij, J. Zirngibl, and R. Holz, "Data set of the paper: A First Look at Deployment Strategies of Services Provisioned using Anycast," 2026. [Online]. Available: https://doi.org/10.5281/zenodo.20374518

[17] G. F. Lyon, *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*. Insecure, 2009.

[18] Bob Halley, "dnspython," https://pypi.org/project/dnspython/, 2025, [Accessed 2026-03-14].

[19] Charles-Francois Natali, "ntplib," https://pypi.org/project/ntplib/, 2021, [Accessed 2026-03-14].

[20] J. Zirngibl, F. Gebauer, P. Sattler, M. Sosnowski, and G. Carle, "QUIC Hunter: Finding QUIC Deployments and Identifying Server Libraries Across the Internet," in *PAM Conference*, 2024.

[21] P. Sermpezis, L. Prehn, S. Kostoglou, M. Flores, A. Vakali, and E. Aben, "Bias in internet measurement platforms," in *TMA*, 2023.

[22] O. Gasser, Q. Scheitle, S. Gebhard, and G. Carle, "Scanning the ipv6 internet: Towards a comprehensive hitlist," in *TMA*, 2016.

[23] R. van Rijswijk-Deij, M. Jonker, A. Sperotto, and A. Pras, "A high-performance, scalable infrastructure for large-scale active dns measurements," *IEEE JSAC*, vol. 34, no. 6, 2016.

[24] J. Zirngibl, L. Steger, P. Sattler, O. Gasser, and G. Carle, "Rusty clusters? dusting an ipv6 research foundation," in *IMC*. ACM, 2022.

[25] bgp.tools, "Data sources bgp.tools," https://bgp.tools/features, 2026, [Accessed 2026-02-06].

[26] D. R. McPherson, R. Donnelly, and F. Scalzo, "Unique Origin Autonomous System Numbers (ASNs) per Node for Globally Anycasted Services," Internet Engineering Task Force, RFC 6382, 2011. [Online]. Available: https://www.rfc-editor.org/info/rfc6382

[27] K. Z. Sediqi, A. Feldmann, and O. Gasser, "Live long and prosper: Analyzing long-lived moas prefixes in bgp," in *TMA*, 2023.

[28] United Nations, Statistics Division, "Un m49 standard — geographic regions and subregions," https://unstats.un.org/unsd/methodology/m49/, 2023, [Accessed 2026-02-06].

[29] United Nations, Department of Economic and Social Affairs, Population Division, "World Population Prospects 2024," https://population.un.org/wpp/, 2024, [Accessed 2026-03-17].

[30] M. Zhou, X. Zhang, S. Hao, X. Yang, J. Zheng, G. Chen, and W. Dou, "Regional ip anycast: Deployments, performance, and potentials," in *Proceedings of the ACM SIGCOMM 2023 Conference*, ser. ACM SIGCOMM '23. New York, NY, USA: Association for Computing Machinery, 2023, p. 917–931. [Online]. Available: https://doi.org/10.1145/3603269.3604846

[31] InternetNZ, "DNS infrastructure," https://internetnz.nz/access-and-security-online/infrastructure-services/dns/, accessed: 2026-05-13.

[32] M. Duke, "QUIC Version 2," Internet Engineering Task Force, RFC 9369, 2023. [Online]. Available: https://www.rfc-editor.org/info/rfc9369

[33] Internet Assigned Numbers Authority, "Service name and transport protocol port number registry," https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml, 2026, [Accessed: 2026-03-07].

[34] Cloudflare, "Cloudflare Cache," https://developers.cloudflare.com/cache/, 2026, [Accessed 2026-03-14].

[35] G. C. Moura, R. d. O. Schmidt, J. Heidemann, W. B. de Vries, M. Muller, L. Wei, and C. Hesselman, "Anycast vs. ddos: Evaluating the november 2015 root dns event," in *Proc. IMC*. ACM, 2016. [Online]. Available: https://doi.org/10.1145/2987443.2987446

[36] Cloudflare, "How Cloudflare DNS works," https://developers.cloudflare.com/fundamentals/concepts/how-cloudflare-works/, 2026, [Accessed 2026-03-14].

[37] M. Müller, G. C. M. Moura, R. de O. Schmidt, and J. Heidemann, "Recursives in the wild: engineering authoritative dns servers," in *Proc. IMC*. ACM, 2017. [Online]. Available: https://doi.org/10.1145/3131365.3131366

[38] "Sshd_config(5) - OpenBSD manual pages," https://man.openbsd.org/sshd_config.

[39] Y. Khalidi, "How Microsoft builds its fast and reliable global network," 2017.

[40] K. Moore and C. Newman, "Cleartext Considered Obsolete: Use of Transport Layer Security (TLS) for Email Submission and Access," Internet Engineering Task Force, RFC 8314, 2018. [Online]. Available: https://www.rfc-editor.org/info/rfc8314

[41] Google, "Google Trust Services | Repository," https://pki.goog/repository/, [Accessed 2026-03-14].

[42] D. Reilly, H. Stenn, and D. Sibold, "Network Time Protocol Best Current Practices," Internet Engineering Task Force, RFC 8633, 2019. [Online]. Available: https://www.rfc-editor.org/info/rfc8633
[43] Oracle, "MySQL :: MySQL Router 9.6 :: 4.3.3 Configuration File Options," https://dev.mysql.com/doc/mysql-router/9.6/en/mysql-router-conf-options.html#option_mysqlrouter_bind_address, [Accessed 2026-03-14].
[44] The PostgreSQL Global Development Group, "19.3. Connections and Authentication," https://www.postgresql.org/docs/18/runtime-config-connection.html, 2026, [Accessed 2026-03-14].
[45] DigitalOcean, "How To Allow Remote Access to MySQL - SnapShooter Tutorials," https://snapshooter.com/learn/mysql/allow-mysql-remote-access, [Accessed 2026-03-14].
[46] T. King, C. Dietzel, J. Snijders, G. Döring, and G. Hankins, "BLACKHOLE Community," Internet Engineering Task Force, RFC 7999, 2016. [Online]. Available: https://www.rfc-editor.org/info/rfc7999
[47] DNS4EU, "Dns4eu for public," https://joindns4.eu/for-public, 2025, [Accessed 2026-03-24].
[48] Jurgen Gaeremyn, "European critical dependencies – Pseudo Random Noise," https://jurgen.gaeremyn.be/2025/03/08/european-critical-dependencies/, 2025, [Accessed on 2026-03-26].
[49] Cloudflare, "Cloudflare outage on November 18, 2025," https://blog.cloudflare.com/18-november-2025-outage/, 2025, [Accessed 2026-03-14].
[50] ——, "Details of the Cloudflare outage on July 2, 2019," https://blog.cloudflare.com/details-of-the-cloudflare-outage-on-july-2-2019/, 2019, [Accessed 2026-03-14].
[51] K. Claffy, Y. Hyun, K. Keys, M. Fomenkov, and D. Krioukov, "Internet mapping: From art to science," in *2009 Cybersecurity Applications & Technology Conference for Homeland Security*, 2009.

Appendix A
Ethics

We follow best practices for measurements [7], and we have obtained ethical approval from our institution. No sensitive information is collected. We use a limited number of VPs to reduce the impact of our scanning activity. We received one complaint from our Computer Emergency Response Team (CERT) due to high scanning traffic. We limited the scanning rate by distributing the pipeline over a 24-hour period and used a blocklist from prior measurements.

Appendix B
IPv6 Anycast

TABLE IV: Top 5 ASes by number of anycast IPv6 /48-prefixes (n=13 007).

Org (ASN)	/48-Prefixes
Cloudflare Spectrum (209242)	6 421 (49%)
Cato Networks (214040)	1 795 (13%)
Fastly (54113)	760 (6%)
Cloudflare (13335)	620 (5%)
Incapsula (19551)	587 (5%)

Table IV shows the top 5 ASes that deploy IPv6 anycast. Unlike IPv4, we do not know the number of active IPs for IPv6 due to the large number of addresses within /48-prefixes. However, based on the number of /48s covered by *LACeS*, we find that Cloudflare is, by far, the largest operator of IPv6 anycast. We note that *LACeS* has limited IPv6 visibility, as their hitlists do not cover the full IPv6 address space.

Appendix C
Anycast upstreams

TABLE V: Top 5 upstreams visible for routed anycast prefixes.

Name (ASN)	Total Prefixes	IPv4 Prefixes	IPv6 Prefixes
Arelion (1299)	2 977 (40%)	1 751 (37%)	1 226 (45%)
Cogent (174)	2 577 (35%)	1 557 (33%)	1 020 (37%)
NTT (2914)	2 153 (28%)	1 171 (25%)	982 (36%)
Lumen (3356)	2 049 (28%)	1 485 (32%)	564 (21%)
Telxius (12956)	1 557 (21%)	1 076 (23%)	481 (17%)

Table V shows the most frequent upstream ASes for 7 442 routed prefixes covering the /24, and /48 anycast prefixes of *LACeS*. Unsurprisingly, these are all tier-1 networks (except Cogent for IPv6). Comparing IPv4 and IPv6, we find they provide roughly equal connectivity.

Appendix D
Multi-Regional Providers

TABLE VI: Top ASes by number of regional anycast prefixes.

Org (ASN)	Regions (# of /24s)
AWS (16509)	AS (11), NA (7), EU (1), OC (1), SA (1)
BunnyCDN (200325)	NA (2), AS (1), OC (1), SA (1)
Akamai (33905)	AS (10), NA (10), OC (10), EU (1)
Fortanix (23013)	AS (1), EU (1), NA (1)
GCORE (199524)	EU (2), NA (2), AS (1)
Vultr (20473)	NA (3), AS (1), OC (1)
Fortinet (40934)	NA (5), AS (2), EU (2)
Bytedance (396986)	EU (3), AS (2), NA (1)
Cato networks (13150)	NA (5), EU (3), AS (1)
Level 3 (3356)	NA (8), EU (1)
Fastly (54113)	NA (180), EU (1)

Table VI lists all ASes for which *LACeS* detects regional (*i.e.*, confined within a single continent) anycast prefixes in multiple continents. We note that the iGreedy [10] geolocation method used by *LACeS* struggles with detecting regional anycast and may miss certain prefixes.

Appendix E
DNS Software

We request `TXT CHAOS` records for commonly used records such as `id.server` and `version.bind` to investigate the DNS software running on anycast prefixes. For example, *ns.es.hk2.bind* strongly indicates that this particular DNS server in Hong Kong uses BIND. We perform this measurement using Ark [51] that lets us request these records from 350+ different VPs.

In total, 658 ASes run an anycasted DNS service and 190 ASes (29%) reveal the software used in the requested TXT records. As observed by Cicalese et al. [4], we find BIND is the most commonly used DNS software, seen in 92 ASes, followed by PowerDNS with 86 ASes.

Interestingly, we find 25 ASes that deploy multiple DNS software using the same anycast IP address, where, depending on the PoP reached, a different DNS software is observed. Examples include: K- and B-root, AS112, AWS, Google, Verizon, CIRA (.ca), and RIR (LACNIC, RIPE, APNIC) DNS infrastructure such as rDNS.