February 2025
Geoff Huston

# DNS Nameservers: Service Platforms and Resilience

Last year, in December, I looked at the behaviour of DNS recursive resolvers from the perspective of optimising performance and resilience of name resolution (https://www.potaroo.net/ispcol/2024-12/nameservers.html). When given a choice of nameservers to use to query for a particular name within a domain will the resolver try to make an "optimal" choice? Will it gravitate towards using the nameserver that is the fastest to answer its queries? Or will it show no such efforts to optimise name resolution performance? The study looked at the behaviour of DNS recursive resolvers and used a large-scale measurement exercise to conclude that these days you just can't rely on the recursive resolver's server selection algorithm to make an optimal selection. Now if a zone is being served by a set of unicast authoritative nameservers this is a significant concern. Why go to all the trouble and expense to set up secondary nameservers across the entire Internet if recursive resolvers will just pick any server to query?

If name resolution performance and resilience is an important consideration, then the DNS service operator needs to look to an anycast nameserver solution, preferably with a highly diverse collection of points of presence within the anycast constellation. The study also suggested that the optimal approach for a domain when considering both performance and operational resilience is for the domain to be served by at least two distinct dual-stack diverse (and dense) anycast nameservers, but once you are using two such anycast platforms the additional benefits of adding more anycast service platforms to the mix is marginal.

Given these considerations, how do we provision DNS nameservers today? Are we still using dispersed unicast nameservers? Or are nameservers provisioned using multiple anycast platforms? Let's look at a two quite different collections of domain names and see how they are served.

## Nameservers for Top Level Domains

The Root Zone of the DNS contains a total of 1,445 delegations. These delegation records list the names of 6,012 nameservers, which implies that each delegated domain in the root zone is served by an average of 4.2 nameservers.

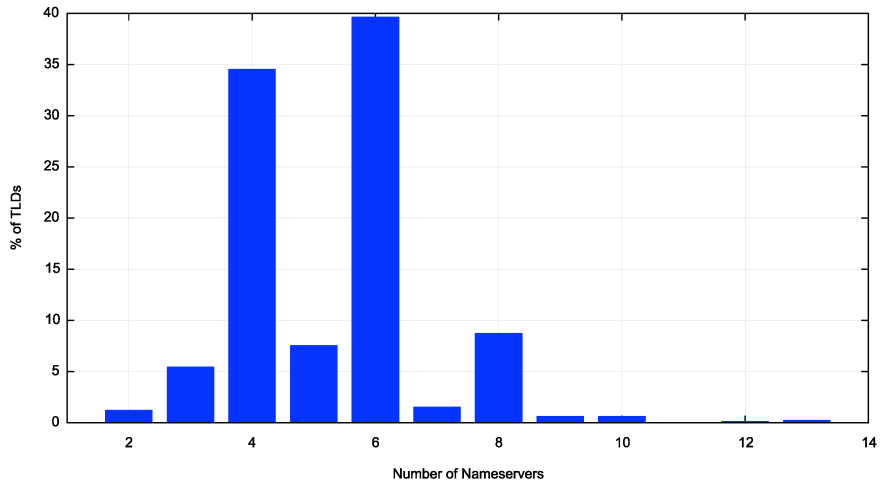


*Figure 1 – Distribution of Nameservers per Delegated Domain*

Averages can sometimes be misleading, and the distribution of the number of nameservers per delegated domain is shown in Figure 1. There is a strong preference for using either 4 or 6 nameservers per domain in the root zone, with a slight preference for using 6 nameservers over 4.

Conversely, each nameserver name is used by an average of 1.3 top level domains (TLDs). Again, averages can be misleading, and the distribution of the number of TLDs served by each nameserver name is shown in Figure 2.

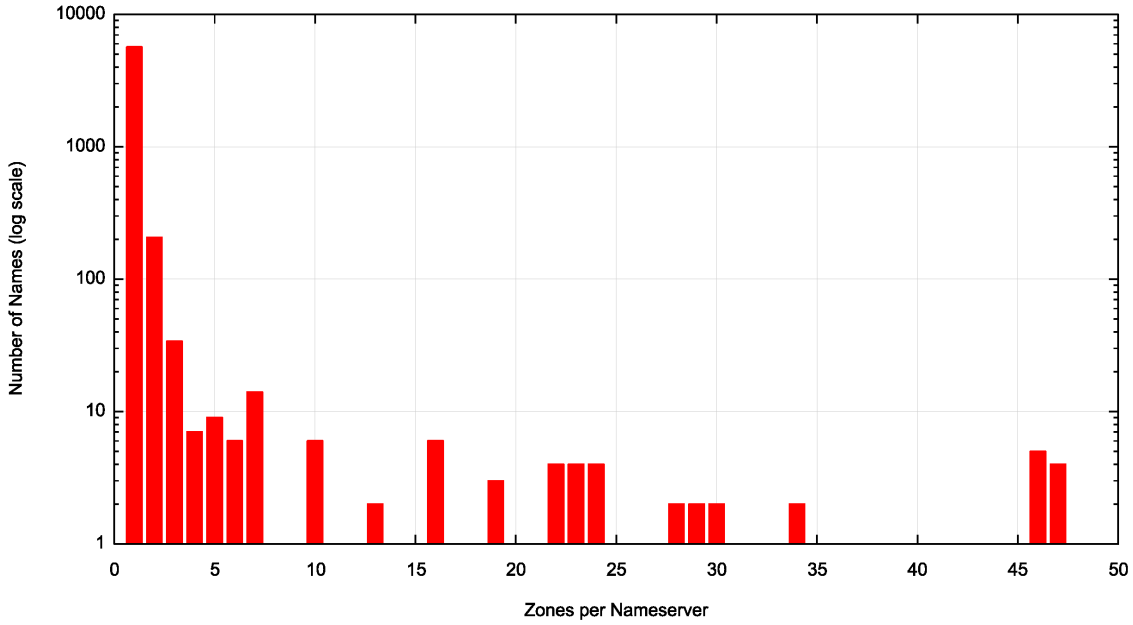


*Figure 2 – Distribution of TLDs per Nameserver*

The majority of nameservers (5,673 out of 6,012 unique nameserver names) serve only a single zone. (This is potentially a misleading statement as it specifically refers to the use of nameserver names, not the nameservers themselves. There are a number of nameserver names that have glue records that have a common IP address.)

A further 206 nameserver names are authoritative for 2 zones, and 34 nameserver names are authoritative for 3 zones. The highest count is four nameservers that are each authoritative for 47 zones. One of these nameservers is operated by the Japanese TLD operator, GMO Registry and the other is operated by Google's Registry service, using the nameserver name `charlestonroadregistry.com`.

Most of these nameservers are provisioned using dual stack platforms, and a total of 5,692 nameservers out of 6,012 are dual-stack. Some 317 nameservers are IPv4-only and just 3 nameservers have only an IPv6 address. A small number of nameservers (15) have more than a single IPv4 and/or IPv6 address. One nameserver, `mzizi.kenic.or.ke.`, has 4 IPv4 addresses and a single IPv6 address, which is the highest number of IP addresses per nameserver name.

The root zone contains 9,037 unique IP addresses for nameservers, which implies that a number of nameserver names in the root zone resolve to a common IP address. While 8,383 IP addresses are associated with a single nameserver name, the remaining 656 IP addresses are associated with 10 or more nameserver names. There are 6 IP addresses that are associated with 90 nameserver names, and a further 6 that are associated with 95 nameserver names. We can combine this data with the mapping of TLDs to their nameserver names to describe the number of served TLDs per IP address (Figure 3).

These figures show that the domains in the root zone have little in the way of single critical points of common reliance, which is a very positive aspect in terms of engineering for resilience at the top level of the DNS name hierarchy.

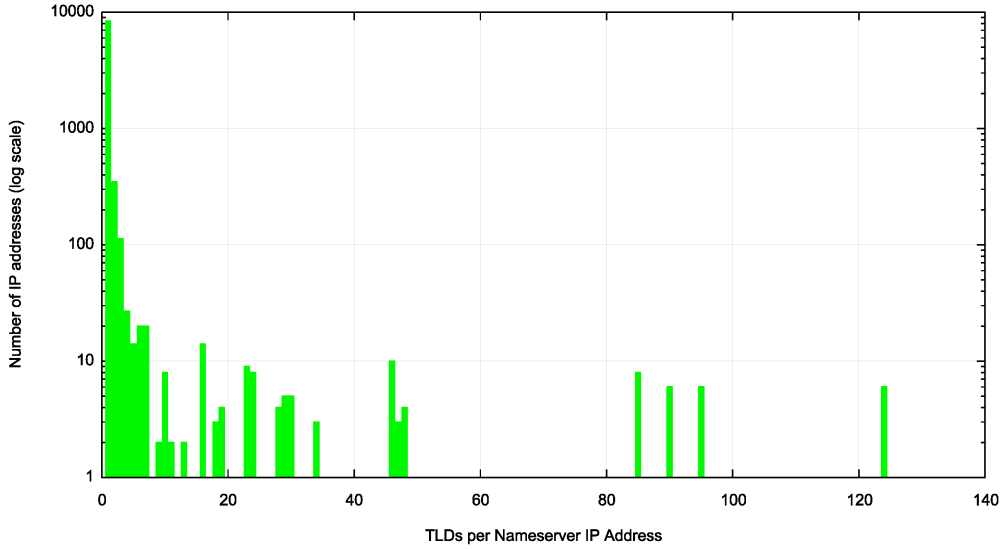


*Figure 3 – Distribution of TLDs per Nameserver IP address*

## Anycast vs Unicast for TLD Nameservers

As we've noted in the previous study on recursive resolver behaviour, recursive resolvers are, on the whole, not very good at optimising for performance and resilience when choosing which nameserver to query when given a choice of a number of unicast nameservers. This means that the task of optimising DNS query performance is better left to the combination of an anycast service platform and routing-based server selection process. How many of these 9,037 IP addresses are configured into an anycast service cloud and how many are using unicast services?

A measurement approach to distinguish between unicast and anycast service platforms is to use a set of diverse test points and query the nameserver IP addresses from each of these test points. The DNS query used here was to ask the nameserver for its Nameserver Identification (NSID) value, and the measurement recorded both the returned NSID value, and the time taken to perform the query. Here we've used queries from platforms located in Atlanta in the US, Frankfurt in Germany, Sao Paulo in Brazil, Brisbane in Australia and Singapore to give us a suitably diverse set of query perspectives. If the NSID value is constant when queried from these five locations, and the DNS transaction times show a high level of variance (greater than 150ms between slowest and fastest DNS transaction time), then it is reasonable to assume that the IP address is a unicast address. If the NSID values differ, then it's likely that the IP address is an anycast address. However, a DNS server "farm" in a single location could also result in different NSID values when queried from different locations. We also need to use the variance in the DNS transaction times when queried from these locations even if the returned NSID values differ. We term the platform a "diverse" anycast platform if the variance in query times is smaller than 150ms between slowest and fastest DNS transaction times, and in other cases of higher variance use the description of a "limited" anycast platform.

The results of this measurement for the IP addresses used for nameservers in the root zone are shown in Table 1.

| | |
|---|---|
| Unicast IP Addresses | 587 |
| "Limited" Anycast | 5,891 |
| "Diverse" Anycast | 2,559 |

*Table 1 – Distribution of Root Zone Nameserver Platform types*

We can relate this back to the TLDs that are served by these nameserver platforms. There are just 8 TLDs that appear to be served exclusively by unicast nameservers, namely **by**, **ck**, **et**, **fk**, **gh**, **hm**, **mp**

and **xn--90ais**. These are all cc TLDS (**xn--90ais** is the IDN variant of **by**). The complete distribution of TLDs and the characteristics of the nameservers are shown in Table 2.

| | |
|---|---|
| Unicast-only platform | 8 |
| Mixed Unicast and Anycast platforms | 378 |
| Anycast-only platform | 1,059 |
| Diverse Anycast | 289 |
| Limited Anycast | 202 |
| Mixed Diverse and Limited Anycast | 568 |

*Table 2 – Distribution of TLDs by Nameserver Platform types*

Almost all of the TLDs are now served, wholly or in part, by anycast service platforms, and the role of passing a query to the "closest" nameserver is now a role that is performed by the routing system, so the resolver's nameserver selection algorithm is no longer of critical importance in this context of performance of resolution of TLD labels.

## Diversity and Resilience

An important aspect of service resilience is diversity, and while anycast platforms can exhibit a certain level of resiliency, it is generally felt that multiple anycast platforms can significantly improve the operational resilience of a service. While Figure 1 shows that each TLD is most commonly serviced by either 4 or 6 named nameservers, what is the picture when we map each nameserver to its IP addresses, and map these IP addresses to their origin AS?

Given that the majority of nameservers used by TLDs are dual stack nameservers, and most TLDs have either 4 or 6 nameservers, then it should be unsurprising that the average number of IP addresses that serve a TLD is 10.1 IP addresses.

The quest for operational resilience typically entails some effort to increase the levels of diversity in infrastructure provisioning. This includes the use of both IP protocols (dual stack nameservers) and also includes the use of nameserver IP addresses that are separately announced into the routing system (a major service platform outage a few years ago was caused by having all of their domain's nameservers announced from the same IPv4 address prefix), also potentially using multiple nameserver platforms and multiple platform operators. The overall approach is to reduce the potential for single critical points of dependence.

Potentially, one quick way to look at the level of operational diversity in nameserver provisioning is to look at the number of different networks that serve this domain, by looking at the number of Autonomous System (AS) numbers that announce these IP addresses into the routing system. When we then map these nameserver IP addresses to the origin AS (the AS that announces these addresses into the routing system), then the average number of origin AS's that serve each TLD is 3.5 which is lower than 4, indicating that a number of these per-address anycast service platforms are operated by the same network operator and use the same origin AS.

The distribution of Origin AS's per TLD nameserver set is shown in Figure 4. As is evident from this figure, there is a strong preference for two distinct anycast platforms (43% of TLDs) and secondly for four distinct platforms (28% of TLDs).

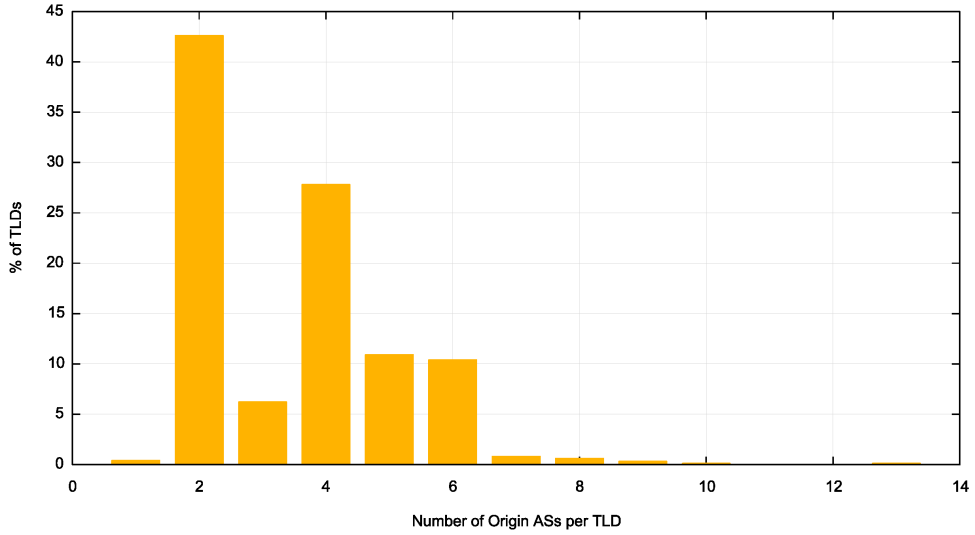


*Figure 4 – Distribution of Nameserver Providers per TLD by Origin AS*

However, its useful to ask the question whether all these origin ASes are fully independent networks, or whether they are multiple platforms with different AS numbers but operated by a common entity. It is quite common for DNS providers to operate multiple AS's in the routing system, and spread the IP addresses across these different AS's. This achieves some level of routing separation but does not necessarily ensure that the platforms are truly mutually independent. They could share the same physical locations, the same set of network adjacencies and a single nameserver platform both in hardware and software.

Table 3 shows the 15 "top" origin AS numbers sorted by the number of TLDs that they provide a nameserver platform service and the names of the AS.

| TLDs | AS | AS Name, CC |
|---|---|---|
| 478 | 12041 | AS-AFILIAS1, US |
| 472 | 207266 | AFILIAS-SECONDARY-DNS, IE |
| 385 | 397239 | SECURITYSERVICES, US |
| 382 | 397241 | SECURITYSERVICES, US |
| 381 | 397220 | SECURITYSERVICES, US |
| 294 | 397232 | SECURITYSERVICES, US |
| 193 | 397213 | SECURITYSERVICES, US |
| 154 | 42 | WOODYNET-1, US |
| 114 | 199330 | CENTRALNIC-ANYCAST-A CentralNic Anycast-A AS Number, GB |
| 114 | 60890 | CENTRALNIC-ANYCAST-B CentralNic Anycast-B AS Number, GB |
| 113 | 201304 | CENTRALNIC-ANYCAST-E, GB |
| 113 | 201303 | CENTRALNIC-ANYCAST-F, GB |
| 88 | 137502 | NOMINET-AS-AP NOMINET UK, GB |
| 88 | 43519 | NOMINETANYCAST, GB |
| 75 | 8674 | NETNOD-IX Netnod AB, SE |

*Table 3 – 15 "top" AS Nameserver Platforms*

The first two ASes, AS12041 and AS207266, are both operated by an entity formerly known as Afilias (subsequently acquired by Donuts and now known as Identity Digital). This entity appears to have a commercial; interest in some 264 TLDs and provides the nameserver service platform for a further 200 or so TLDs. The next five AS's are all operated by an entity formerly known as Neustar, whose domain name registry business was acquired by Godaddy in 2020.

A number of DNS service platforms used by TLDs operate multiple anycast platforms. Such a setup certainly has a positive impact on resilience, in that disruptive efforts intended to disrupt DNS service

availability have to be mounted to attack all these anycast addresses. On the other hand, a single service operator has a greater likelihood of single points of potential failure though potential use of a single service platform implementation and potentially a common set of anycast locations across all the anycast networks. A diversity of anycast service platforms and platform operators is more likely to provide a more resilient overall service.

It may be informative to condense this list be treating the collection of ASes operated by a single entity as a single AS. One way to do this is to use the holder account field in the extended daily stats file reports generated by each of the Regional Internet Registries, where multiple AS numbers, and IP address holdings share a common account field. If we apply this common holding account field to the AS numbers in Table 3 we then come up with the following top 15 (Table 4).

| TLDs | AS | AS Name, CC |
|---|---|---|
| 478 | 12041 | AS-AFILIAS1, US |
| 386 | 397239 | SECURITYSERVICES, US |
| 154 | 42 | WOODYNET-1, US |
| 114 | 60890 | CENTRALNIC-ANYCAST-B CentralNic, GB |
| 88 | 43519 | NOMINETANYCAST, GB |
| 77 | 8674 | NETNOD-IX Netnod AB, SE |
| 55 | 55195 | CIRA-CLOUD1, CA |
| 46 | 43515 | YOUTUBE YOUTUBE, IE |
| 46 | 15169 | GOOGLE, US |
| 39 | 2484 | NIC-FR-DNS-ANYCAST-AFNIC AFNIC, FR |
| 35 | 8561 | KNIPPWORLDWI, DE |
| 34 | 393818 | TUCOWS-TRS-DNS1, CA |
| 32 | 1921 | RCODEZERO-ANYCAST-SEC1-TLD RcodeZero Anycast DNS, AT |
| 30 | 197000 | RIPE-NCC-AUTHDNS-AS RIPE NCC, NL |
| 29 | 37177 | AFRINIC-ANYCAST, MU |

*Table 4 – 15 "top" AS Nameserver Platform Groups*

This grouping has a major effect on the level of multi-platform support in this set of TLD nameservers. If we use this entity-based grouping of ASes, we can look at the number of distinct entities used to operate the nameservers for each TLD. This distribution is shown in Figure 5.

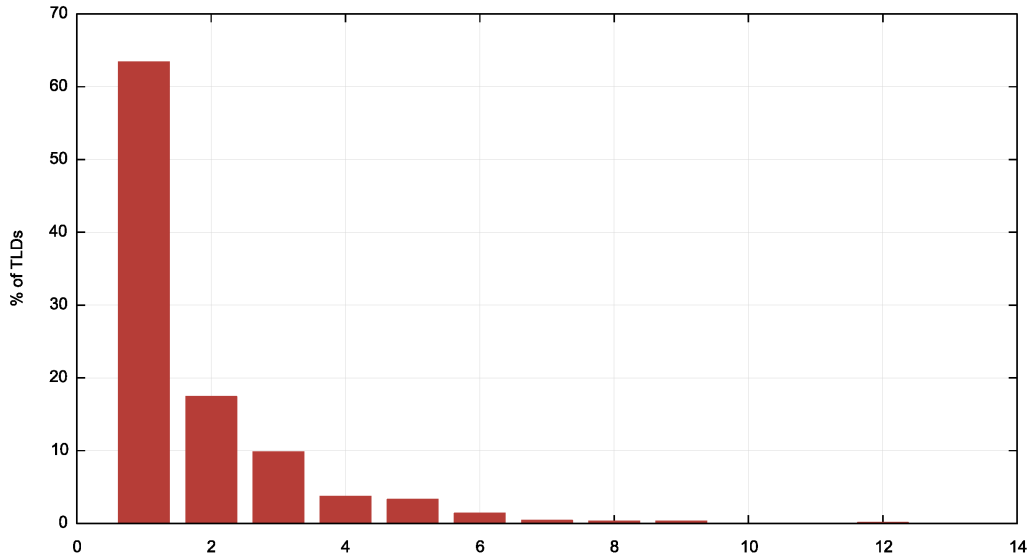


*Figure 5 – Distribution of Nameserver Providers per TLD*

Some 916 TLDs are served by a single service provider entity, and 251 by two providers, and there are 4 tlds with 8 distinct providers (**lk**, **se**, **jp** and **vn**), 4 with 9 providers (**tw**, **hk**, **xn--j6w193g** and **fi**) and 1

tld (**arpa**) with nine distinct providers. Given the limited failover behaviour of most recursive resolvers it is of decreasing benefit once the number of nameserver platforms exceeds 2, so from this perspective some 63% of TLDs are provisioned with a single name service platform, while the remaining 37% have some level of diversity which includes mutual failover capacity which is inherent in the DNS protocol's resolution behaviour.

## Nameservers for the Tranco Top 1M Domains

It could be argued that the root zone is "special" in many ways and it's probable that far more care and attention (and money) is paid to service performance and resilience of these TLDs than is the case for the larger collection of names that are at lower levels in the DNS hierarchy. The DNS is a heavy-tail distribution in many ways where a very small collection of domains attract the majority of user interest (see Cloudflare Radar's domain report as an example).

For our second collection of domain names to examine, we take the Tranco Top 1M domain list (https://tranco-list.eu/) and perform a similar analysis of their nameserver configuration.

Figure 6 shows the distribution of the number of nameservers per domain. In any very large set of domains, it is to be expected that not all names are visible at any point in time, and in this case some 3% of these 1M domain names were not resolvable by our DNS client (shown as a 0 count in Figure 6).

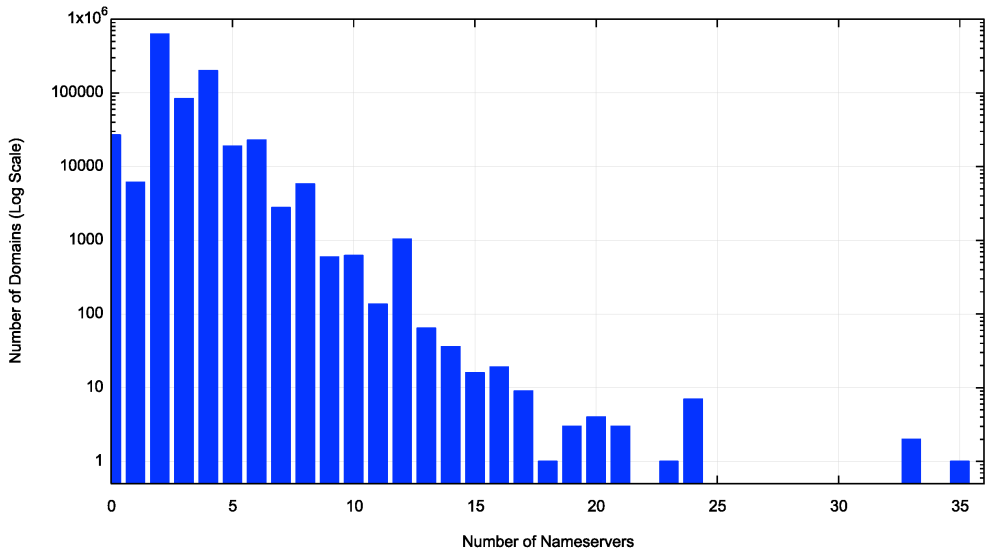


*Figure 6 – Distribution of Nameservers per Domain*

While the domains in the root zone show a strong preference for being served by 4 or 6 nameservers, this larger list of domains shows a very strong preference for being served by two nameservers (63%), then four nameservers (20%). There is also a small collection of anomalous outliers with 57, 61, 64 and 88 nameservers!

Of these 265,010 uniquely-named nameservers, some 196,296 nameserver names resolve to a single IP address (75% of nameservers), 55,837 have 2 IP addresses (21.5%) and the remaining 7,917 have three or more IP addresses. There are three extreme outlier nameservers with 176, 186 and 201 nameserver IP addresses.

Some 201,887 nameservers have only IPv4 addresses, 1,051 have only IPv6 addresses and 57,112 have both IPv4 and IPv6 addresses. This is a radical departure from the picture of the nameservers that are used in the root zone, and points to a significant lag in the commodity volume domain service market to adopt an IPv6 transition plan. I suspect that, as with many commodity markets, we are dealing with a very cost-sensitive market here and any additional cost in platform provisioning that cannot be accompanied by a comparable increase in revenue is strongly resisted by the incumbent providers.

In the root zone the majority of nameservers (5,673 out of 6,012 unique nameserver names, or 94%) serve only a single zone. In this larger set of domains there are 265,010 uniquely named nameservers, of which some 190,328 nameservers serve a single domain (72%). The progression of the number of nameservers for 2 or more domains roughly follows an exponential decay function, culminating with 265 nameservers serving 19 domains. The distribution of the number of domains served by each nameserver is shown in Figure 7.

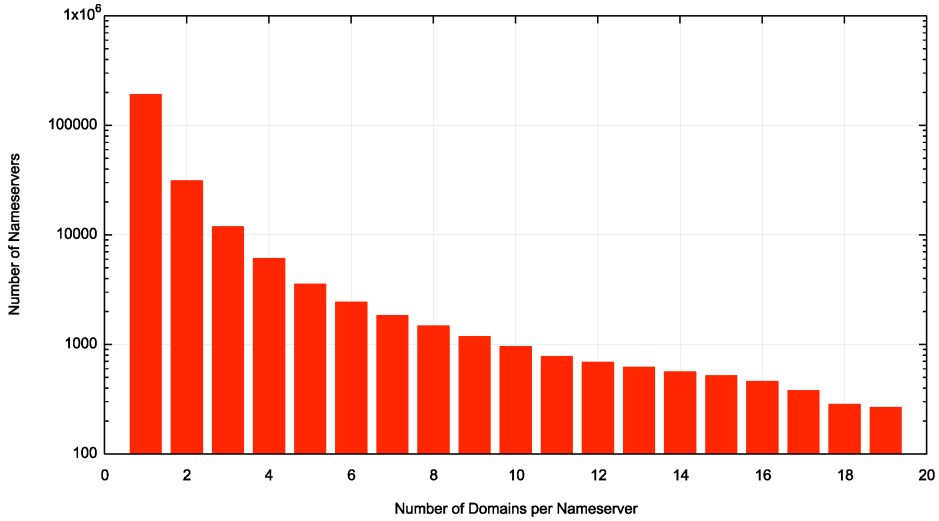


*Figure 7 – Number of Domains per Nameserver Name*

In this data set of domain names there are a total of 265,010 uniquely named nameservers that can be resolved to one or more IP addresses. These resolvers map to 227,846 IP addresses. 81% of these IP addresses (186,096) are associated with just 1 nameserver name, while at the other end some 13 IP addresses are used by 700 or more nameserver names.

This then allows us to count the number of domains served by each IP address. This distribution is shown in Figure 8.

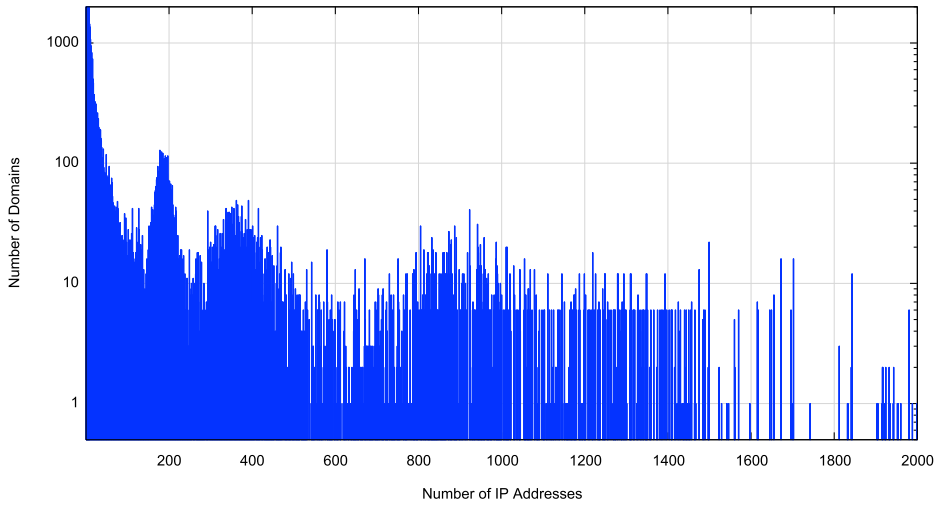


*Figure 8 – Distribution of Domains per Nameserver IP address*

This is a somewhat skewed distribution, where 119,544 domains, or 12% of the total domain set, are each served by a (different) single IP address! This is not exactly a highly resilient configuration, even if the server platform uses anycast. A further 44,229 domains are served by just two IP addresses, and a further 13,498 domains are served by just three IP addresses. At the other end of this distribution, there

are two IP addresses that each serve 13,278 domains and a further four IP addresses that serve some 12,400 domains.

If we move on from individual IP addresses and look at the AS numbers behind these addresses, we get a clear picture of the level of concentration in the DNS service provider space. Table 5 lists the top 25 ASes, and the number of domains from this Tranco 1M domain name set for which they provide nameserver services.

| Domains | AS | AS name, CC |
|---|---|---|
| 364,918 | 13335 | CLOUDFLARENET, US |
| 109,766 | 16509 | AMAZON-02, US |
| 51,642 | 44273 | GODADDY-DNS, DE |
| 23,539 | 397239 | SECURITYSERVICES, US |
| 15,212 | 16276 | OVH, FR |
| 14,155 | 15169 | GOOGLE, US |
| 13,710 | 8075 | MICROSOFT, US |
| 11,637 | 24940 | HETZNER-AS, DE |
| 10,731 | 37963 | ALIBABA-CN-NET, CN |
| 10,198 | 21342 | AKAMAI-ASN2, NL |
| 9,775 | 16552 | TIGGEE, US |
| 8,263 | 8560 | IONOS-AS, DE |
| 7,881 | 62597 | NSONE, US |
| 7,546 | 203391 | CLOUDNSNET, BG |
| 4,776 | 197695 | AS-REG, RU |
| 3,970 | 209453 | GANDI-LIVEDNS, FR |
| 3,960 | 1921 | RCODEZERO-ANYCAST-SEC1, AT |
| 3,908 | 207021 | RCODEZERO-ANYCAST-SEC2, AT |
| 3,689 | 198610 | BEGET-AS, RU |
| 3,558 | 63949 | AKAMAI-LINODE-AP, SG |
| 3,389 | 14061 | DIGITALOCEAN-ASN, US |
| 3,190 | 396982 | GOOGLE-CLOUD-PLATFORM, US |
| 2,946 | 55907 | GMO Internet Group, JP |
| 2,926 | 14618 | AMAZON-AES, US |
| 2,681 | 45102 | ALIBABA-CN-NET, CN |

*Table 5 – Count of Domains served by the top 25 network Platform ASs*

Clearly this space is dominated by Cloudflare, which hosts some 36% of these 1M domain names, followed by Amazon, Godaddy, Vercara (formerly Neustar), OVH (a major French cloud platform), Google and Microsoft.

The second summary view is the number of AS platforms used to serve each domain name, shown in Table 6.

| AS Count | Domain Count |
|---|---|
| 1 | 760,121 |
| 2 | 124,623 |
| 3 | 57,611 |
| 4 | 12,368 |
| 5 | 6,307 |
| 6 | 2,231 |
| 7 | 1,834 |
| 8 | 865 |
| 9 | 81 |
| 10 | 71 |
| 11 | 121 |
| 12 | 2,055 |
| 13 | 1,124 |

| | |
|---|---|
| 14 | 13 |
| 15 | 9 |
| 20 | 1 |

*Table 6 – Count of the number of distinct platforms used to serve domains*

The majority of domain names (76%) are served by a single network platform. There are the inevitable outliers with a dozen of more network platforms being used, but as we observed with the study on recursive resolver behaviour, it is uncommon for a DNS resolution environment to pause while the DNS queries so many nameservers, so the extravagant level of over-provisioning is largely a wasted effort!

## Anycast vs Unicast for the Tranco Top 1M Domains

There are 227,846 IP addresses used to serve the domains in this data set. We used the same methodology as for the TLD nameservers, querying each of these DNS servers for their NSID values from each of the measurement points. Some 28,290 servers were unresponsive to our DNS queries.

A server was categorised as "Unicast" if we observed the same NSID value from all the measurement points and the variance in DNS query times was greater than 150ms. A server was categorised as "Diverse Anycast" if we observed varying NSID values and the variance in DNS query times from each of the measurement points was less than 100ms. If the variance in DNS query times was greater than this value we term this "Limited Anycast".

The results of this measurement for the IP addresses used for nameservers in the Tranco top 1M domain collection shown in Table 7.

| | |
|---|---|
| Unicast IP Addresses | 158,722 |
| "Limited" Anycast | 21,393 |
| "Diverse" Anycast | 19,441 |

*Table 7 – Distribution of Root Zone Nameserver Platform types*

Unlike the collection of nameservers that serve TLDs, this set of nameservers for the Tranco top 1M domain names is strongly dominated by unicast servers. Again this result is strongly reflective of the commodity nature of servicing this part of the DNS market, which has high volume in aggregate, but on the whole, low value per domain name.

We can then look at each domain and characterise its set of nameserver platforms. The results are shown in Table 8.

| | |
|---|---|
| Unicast-only platform | 205,204 |
| Mixed Unicast and Anycast platforms | 80,442 |
| Anycast-only platform | 562,364 |
| Diverse Anycast | 369,254 |
| Limited Anycast | 102,882 |
| Mixed Diverse and Limited Anycast | 90,228 |

*Table 8 – Distribution of TLDs by Nameserver Platform types*

A number of providers, notably Cloudflare, have managed to provide a service platform that offers a diverse anycast nameserver at low cost (including an option for a zero-cost name hosting service), which helps to explain its dominant 36% market share in this Tranco 1M domain name set.

In the TLD domain set there were just a handful of unicast-only service platforms (8 out of 1,445 domains, there are some 205,000 unicast-only domains in the Tranco 1M domain set.

## Conclusions

The DNS appears to be a good example of a bi-modal market, where there are small collection of highly valued and valuable domain names (let's call them "pearls"), and a far larger collection of all the other domain names (which I'm tempted to use the collective term "dross", even though it has perhaps unnecessarily pejorative overtimes!). In aggregate, it's likely that both name collections have a similar aggregate value, but the approaches to these market sectors differ markedly.

The "pearls", typified by the TLD domain set, are often managed as hand-crafted artisanal objects, the most extreme of which is the investment in the operation of the root zone itself. They are typically supported by dedicated teams of DNS experts and their operational parameters tend to reflect an obsessive level of attention to performance and availability. Much of the evolution of the DNS is reflected in the efforts to improve the overall performance of these "pearl" domains. It's no surprise that these domains are served by anycast platforms, which can compensate for the shortcomings in many recursive resolver implementations, and the level of duplication in these domains' operational platforms reflects a desire to achieve high service availability. They have a preference for highly capable customised service platforms which cater to their specialised needs. While the available budgets foe the operation of these TLDs is not limitless, it is certainly far greater, per domain, than the budgets for the other class of domains, to the level of orders of magnitude.

The other class of DNS domains is managed, in the whole by mass market DNS services. The platforms are highly automated and rely on economies of scale to operate profitably, if at all. Often, they are cross subsidised by other name service functions, including name registration, web and mail services. These DNS platforms are often conservative in their engineering approach (as evidenced by the continued heavy reliance on IPv4 unicast nameserver platforms).

Where might this head? The DNS is not immune from the pressure of consolidation and centralisation in the networked space, and the lure of "winner takes everything off the table" is certainly an ongoing factor. However, I suspect that the fate of the name server service market is captive to the ultimate fate of domain names themselves. In a space crowded by search engines, social tools, and AI-based synthetic summarisation, domain names appear to have the role of a convenient human-use oriented tag to lead users to access goods and services, and as such its way too early to predict its demise, imminent or otherwise! A price-based race to the bottom has been curtailed by the presence of free services, similar to web dissemination, so further competition in a commodity market based on price alone has largely been neutralised. The aim of the large volume actors appears to be to track the progress of domains and be extract further value from the domain name if the name manages to attain some level of value that distinguishes it from its myriads of name peers.

I personally suspect that we will continue with this two-speed DNS world for some time to come. The small clique of high-valued names attracts the bulk of the engineering attention in terms of performance, utility, and availability, while the bulk of the domain name set takes far longer to integrate any such innovations into the commodity service offerings.

I would however comment that the market lacks some basic common standards for name service and the rationale behind any such standards. How many nameservers are "enough"? How many are just too many? How can we compare anycast service platforms? What are the engineering factors behind service resilience? What should a consumer be looking for from a name service provider? And how are name service platforms measured? How can a consumer compare various service offerings? While the pearls of the DNS attract the overwhelming majority of engineering (and standards) attention, it seems that all the rest are being collectively ignored, and the dearth of relevant standards is the inevitable outcome.

There is RFC2182 on "Selection and Operation of Secondary DNS Servers", but it was written back in 1997 and appears to have been written in a pre-anycast world, so the information is dated, to say the least. There are also some guidelines available on the KINDNS website, which are helpful, but the guidelines tend to be prescriptive and tend to lack associated rationales.

So, when all fails, the last resort of the desperate is of course AI these days, so let me quote Google's generative AI response to the query about a BCP for DNS Service provision:

> A BCP (Best Current Practice) for a DNS service refers to a set of guidelines and recommendations outlining the best operational practices for managing and maintaining a Domain Name System (DNS) service, ensuring high availability, reliability, and security in the face of potential disruptions or failures; essentially, a plan to maintain DNS functionality even during an incident.
>
> Key aspects of a DNS BCP might include:
>
> - **Redundancy and Failover:**
>   Implementing multiple, geographically dispersed DNS servers to act as primary and secondary authoritative name servers.
>   Utilizing load balancing to distribute queries across multiple servers.
>   Automatic failover mechanisms to seamlessly switch to backup servers in case of primary server failure.
> - **Monitoring and Alerting:**
>   Continuous monitoring of DNS server health and performance metrics (response times, query volume, error rates).
>   Real-time alerts for critical issues like server outages, high error rates, or suspicious activity.
> - **Data Backup and Replication:**
>   Regularly backing up DNS zone files to ensure data recovery in case of corruption or accidental deletion.
>   Implementing replication mechanisms to maintain consistent DNS records across different server locations.
> - **Security Practices:**
>   Implementing DNS Security Extensions (DNSSEC) to protect against DNS spoofing and cache poisoning attacks.
>   Filtering malicious DNS queries to block access to known harmful websites.
>   Regularly updating DNS server software to address security vulnerabilities.
> - **Change Management:**
>   Controlled processes for updating DNS records, including testing in a staging environment before deploying to production.
>   Documentation of all DNS configurations and changes to facilitate troubleshooting.
> - **Incident Response Plan:**
>   Defined procedures for identifying, isolating, and resolving DNS issues quickly.
>   Communication plan to notify relevant stakeholders about DNS disruptions and updates.
> - Relevant BCP standards:
>   **BCP 40 (RFC 7720):** This document outlines best practices for operating the DNS root name service, a critical component of the internet's DNS infrastructure.

It may not be all we might want for a BCP about what makes an acceptable DNS service platform, but it's a good start!

## Disclaimer

The above views do not necessarily represent the views or positions of the Asia Pacific Network Information Centre.

## Author

*Geoff Huston* AM, M.Sc., is the Chief Scientist at APNIC, the Regional Internet Registry serving the Asia Pacific region.

*www.potaroo.net*