Best Practices For the Distribution of Anycast Instances of the Root Name Service

THIS IS THE LATEST DRAFT FROM THE RSSAC CAUCUS. THE WORK REMAINS UNFINISHED AND MANY OF THE STUDY QUESTIONS ARE UNANSWERED. THIS IS NOT AN RSSAC PUBLICATION.

An Advisory from the ICANN Root Server System Advisory Committee (RSSAC)
5 March 2018

Preface

This is a report to the Internet Corporation for Assigned Names and Numbers (ICANN) Board of Directors and the Internet community more broadly, from the ICANN Root Server System Advisory Committee (RSSAC). In this report, RSSAC provides advice on best practices for the distribution of anycast instances of the root name service.

The RSSAC seeks to advise the ICANN community and board on matters relating to the operation, administration, security and integrity of the Internet's root server system. This includes communicating on matters relating to the operation of the root servers and their multiple instances with the technical and ICANN community, gathering and articulating requirements to offer those engaged in technical revisions of the protocols and best common practices related to the operation of DNS servers, engaging in ongoing threat assessment and risk analysis of the root server system and recommending any necessary audit activity to assess the current status of root servers and the root zone. The RSSAC has no authority to regulate, enforce or adjudicate; those functions belong to others and the advice offered here should be evaluated on its merit.

A list of the contributors to this report, references to RSSAC Caucus members' statements of interest and objections to the findings or recommendations in this report can be found near the end of this document.

Table of Contents

1. Introduction 4
1.1 Scope of Work.......... 4

2. Background 5
2.1 Root DNS Service Anycast 5

3. Anycast and Resiliency Against Denial of Service 6

4. Latency 7

5. Coordination 9
5.1 The current state of Coordination.......... 9
5.2 Benefits of Coordination 9
5.3. Areas of Coordination 10
5.3.1 Underserved Regions.......... 10
5.3.2 Shared Fate and Redundancy.......... 10
5.3.3 Coordination during Attacks and Catastrophic Events 11

6. Security 11
6.1 Mitigating Influence of BGP Route Instability 11

7. Ways to Improve Anycast DNS Resilience 12
7.1 Increasing Anycast Instance's Link or Site Capacity.......... 13
7.2 Increasing the Number of Anycast Instances 14
7.3 Increasing Topological Diversity 14
7.4 Increasing Software Diversity 15
7.5 Enabling Site-Specific Protections.......... 15

8. Recommendations for Further Study 16
8.1 Understanding the Effect of Increasing Number of Instances.......... 16
8.2 Understanding the Effect of Diversity 16
8.3 Understanding Effects of Latency on Stub Resolvers 16

9. Acknowledgments, Disclosures of Interest, Dissents, and Withdrawals.......... 18
9.1 Acknowledgments 18
9.2 Statements of Interest 19
9.3 Dissents 19
9.4 Withdrawals 19

10. Revision History 19
10.1 Version 1 19

1. Introduction

The root DNS service is provided by thirteen independent root identities, each with a letter a-m. Each root identity consists of a number of anycast service instances distributed across the Internet. The number of anycast instances per identity varies; at this time, there are between a couple to over 150 instances per identity.[1]

Large numbers of anycast instances can improve the resiliency of the root service by increasing the number of available servers, answering queries closer to users, and diversifying interconnectivity between resolvers and root servers.

As the deployment of anycast by root server operators continues, the RSSAC wishes to investigate best practices to optimize the distribution of root server instances in order to maximize overall root service resiliency, and to reduce the Round-Trip Time (RTT) between recursive servers and root servers.

1.1 Scope of Work

On October 10, 2016 the RSSAC issued a scope of work that provided direction for the work described in this document. As a courtesy to readers, the specified scope is included below, together with commentary on the treatment of each point provided in this document.

RSSAC Scope of Work	**Response**
Given the state of current Internet technology, what is the maximum latency a relying party should experience when transacting with the DNS root service as opposed to with a single root server?	Unanswered, but see discussions in section 4
Will adding more instances in more topologically diverse locations make the system more resilient to Denial Of Service (DOS) attacks?	Sections 3 and 7
If root operators were to coordinate their deployments of anycast instances, what considerations should be contemplated?	Sections 5 and 7
Are there any regional or global technological risks (or benefits) if only a subset of operators (versus all or the majority of root operators) deploy anycast instances?	Unanswered

[1] See http://www.root-servers.org/

2. Background

2.1 Root DNS Service Anycast

The root DNS service is provided by thirteen independent root identities, each with a letter a-m. Each root identity consists of a number of Anycast service instances distributed across the Internet all using the same IP addresses. The number of Anycast instances per identity varies from two locations up to several tens of instances per identity. Table 1 below lists the anycast instances per identity, and table 2 lists the geographical distribution of the anycast instances, both as of July 2017.[2]

Table 1: Number of anycast instances by root server organization (July 2017)

Root Server Organization	Number of Anycast Instances
Cogent Communications	8
ICANN	143
Information Sciences Institute	2
Internet Systems Consortium, Inc.	137
NASA Ames Research Center	83
Netnod	52
RIPE NCC	52
U.S. Army Research Lab	2
U.S. DOD Network Information Center	6
University of Maryland	111
Verisign, Inc.	124
WIDE Project	5
Total Anycast Instances	725

Table 2: Number of anycast Instances by Continent (July 2017)

Continents	Number of Anycast Instances
Africa	68
Asia	157
Europe	202
North America	189
Oceania	44
South America	65

[2] The latest information on anycast instances can be found at http://root-servers.org/.

Total Anycast Instances	725

3. Anycast and Resiliency Against Denial of Service

From the point of view of a DNS recursive resolver, the root DNS service is available as long as it is able to obtain an answer from at least one of the root server identities. Conversely for the same resolver, the DNS root service is unavailable if it cannot obtain an answer from any of the root server identities within some time period determined by a combination of timeouts and retry attempts. Since the resolver and the root server perspectives are both important in order to understand the notion of DNS service, it is important to consider these two perspectives when also trying to understand the notion of DNS Root service denial.

From the resolver's perspective service unavailability may be a consequence of local characteristics, such that a root identity may be unavailable even if a number of anycast instances for that identity are still functioning correctly. For example, connectivity issues local to a resolver may prevent that resolver from reaching all anycast instances of a given identity.

Conversely, from the root server perspective, a Denial of Service (DOS) event could result when either a significant proportion of servers responsible for serving the root zone are unable to return answers in a timely manner, or when a significant proportion of end users are unable to reach a root server while access to their other Internet services remains unaffected.

In the first case, a DOS event can occur when a software related bug is triggered, which then renders a number of anycast instances unavailable simultaneously, or when a number of anycast instances are overwhelmed by requests preventing a timely response to DNS queries. Both of these events are unlikely if anycasting is properly employed.

In the second case, a DOS event may occur if there are issues that prevent DNS queries from reaching any root DNS server instance. For example, if a route-origination attack targets the prefixes associated with the root server IP addresses and affects reachability to all legitimate root DNS servers. Or if loss of physical connectivity results in a network convergence event that disrupts network layer reachability to multiple root servers.

A single anycast node can fail for a number of reasons, but as long as there are other nodes capable of providing answers resolvers won't be aware of any failure. The use of anycast and the removal of route advertisements for inoperative nodes makes this largely transparent to resolvers. If a given identity has all of its nodes fail, resolvers will switch to another. Unless all anycast nodes for all identities are unreachable by all recursive servers on the Internet at the same time, a highly unlikely event, any DOS event will be limited in scope. Also, this event will be best understood by measuring absence of connectivity via either physical(i.e. geographical) or logical(i.e. Layer 3 network connectivity) dimensions, because such an event will be limited in scope along these dimensions.

While certain service disruption events could be global, it is more likely that DOS events will be geographically concentrated or identity limited. Geographical concentration of service failure may occur when there is no redundancy, while whole identity failure could result from a directed attack on one anycast IP address or software fault impacting the software choices of a single root server operator. Failures could also be cascading, where a DOS event that targets one or more identities results in the service unavailability of other instances because the other identities, while not directly targeted, are unable to handle the additional query volume associated with query fallback from the non-responding server instances.

Given the different perspectives surrounding root DNS provisioning and use, there is likely not a precise point at which the DNS root service level, either for a single root service provider or for the root service as a composite, degrades from being available to being unavailable. Since level of service is essentially a user oriented construct, a useful metric for measuring degradation of service might be the change in the number of times over a standard period that a given root server fails to respond. While having such a metric might be interesting, it will likely not help in examining and understanding the characteristics of the root DNS service in the face of DOS attacks and how changing the number of instances or the geographical location of anycast instances is likely to increase resilience.

4. Latency

It is difficult to estimate how important latency is to end users of the DNS. Assuming there is always a recursive DNS server between a user and any DNS root server instance, any latency that might exist between the recursive resolver and the root server will likely be mitigated by technologies located within the recursive resolver. Modern recursive DNS resolvers are the product of decades of research into resolving DNS queries as quickly as possible. Technologies such as caching, negative caching,[3] pre-fetching/HAMMER,[4] and aggressive NSEC caching[5] have been developed to increase the speed with which recursive DNS resolvers complete their lookup operation.

Schmidt et al[6] measured the latency of anycast sites of several root letters from 7900 measurement points. The following graph shows the latency from four root server operators.

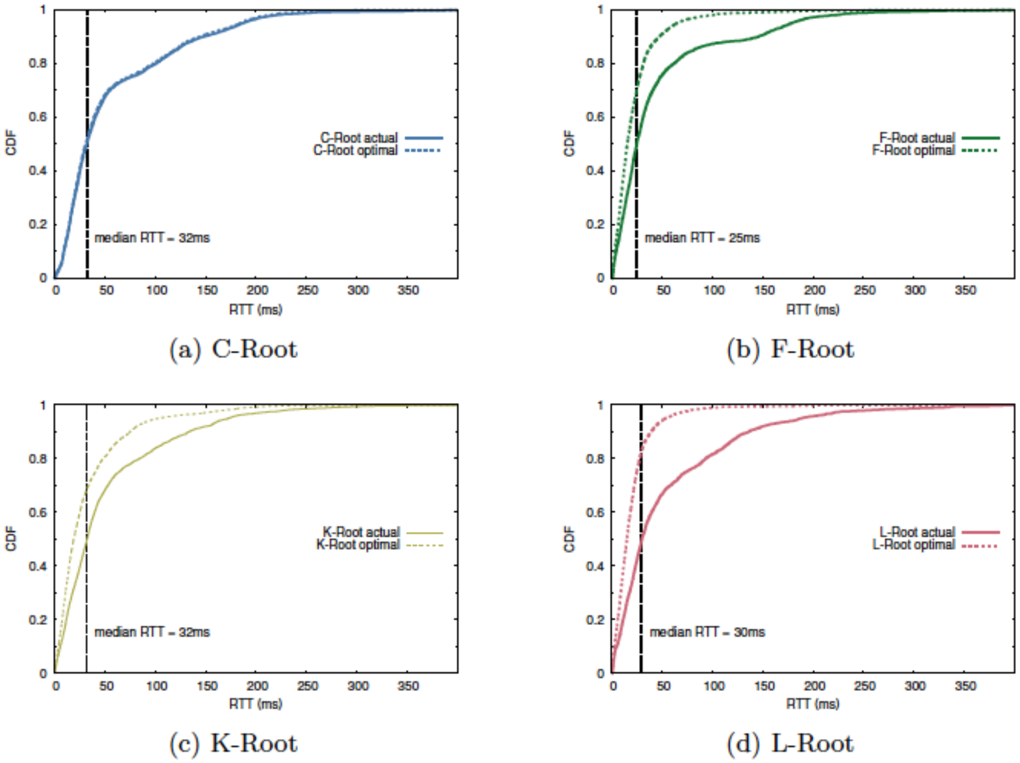
[3] See https://tools.ietf.org/html/rfc2308

[4] See https://datatracker.ietf.org/doc/draft-wkumari-dnsop-hammer/

[5] See https://tools.ietf.org/html/rfc8198

[6] See de Oliveira Schmidt, Ricardo, John Heidemann, and Jan Harm Kuipers. "Anycast Latency: How Many Sites Are Enough?" In International Conference on Passive and Active Network Measurement, pp. 188-200. Springer, Cham, 2017.

Figure 1: DNS root server Round Trip Time (RTT)



(a) C-Root

(b) F-Root

(c) K-Root

(d) L-Root

As shown in Figure 1 above, the median round trip time for the root servers are 25ms - 32ms.

According to Schmit et al, specific to latency, DNS resolution of names located lower in the hierarchy matter more(e.g., www.example.com) , every millisecond can matter. However, names at the root (e.g., .com) are easily cacheable and do not change often. There are only around 1000 names and they allow caching for two days, so shared caches at recursive resolvers are very effective. We consider 30 ms to be a low latency and 100 ms can be considered a high latency. More study is needed to understand the relationship between Root DNS performance and user-perceived latency to provide definitive thresholds.[7]

The RSSAC asks: Given the state of current Internet technology, what is the maximum latency a relying party should experience when transacting with the DNS root service as opposed to with a single root server?

Given the lack of known causality between decreasing latency between root and recursive servers, and any observable effect on DNS users' experience, it is difficult to propose latency reduction interventions for anycast root servers. Further research determining the impact on DNS stub resolvers, and their users, of root server to recursive server latency

[7] When designing studies, they should consider the guidance provided in http://root-servers.org/news/20170918-DNS.Statistics.pdf.

reduction is needed.

Furthermore, it is also necessary to evaluate the circumstances under which such latency reduction measures are being considered. For example, the considerations that are given to improve latency to the DNS root service within underserved regions might be different than the considerations that are given to improve latency during times of a Denial of Service (DOS) attack on one or more root name server instances.

Finally, even when the reasons for improving latency are made clear, it is not the case that adding one or more anycast instances will automatically reduce latency to the DNS root service. Latency depends on the path that the DNS requests take towards the root name servers, and an increased latency may be more a reflection of the peering relationships between ISPs that take such packets over a longer path than the non-availability of a root anycast instance at a given location. Latency also depends on how well certain responses can be cached. Lower Time-To-Live (TTL) values for cretain resource records or uncachable NXDOMAIN responses may result in higher latency for some users.

5. Coordination

5.1 The current state of Coordination

The 13 identities are operated by 12 independent organizations as described at http://www.root-servers.net/. Root operators meet regularly and also share information about their infrastructure, however, they operate independently.

5.2 Benefits of Coordination

The root server system is fairly unique in that it is operated by 12 distinct organizations who all have their own budget, priorities and desires. This individuality has allowed each organization to develop their infrastructure and architecture independently, thereby allowing each organization to innovate without being required to adhere to group oriented design. NLNetLabs' NSD[8] and anycast itself are arguably both examples of this innovation. This independence also allows for a level of political protections, ensuring that geopolitical issues affecting the decision process of one root server do not have the same effect on all organizations.

Having accepted that some level of independence is a benefit to the overall design of the root server system, we also acknowledge that some level of coordination could further improve it. If we look at the root server system today we see a large geographic disparity between where root servers are installed. For example, Europe has roughly 200 root server instances, while the Asia Pacific region has closer to 100. We also see many areas that are represented by multiple operators(e.g. Johannesburg ZA). It is likely that the root server system would benefit from some limited loose coordination to ensure resources are

[8] See https://www.nlnetlabs.nl/projects/nsd/.

spent in regions that are underserved, as well as trying to ensure that root server instances reduce the amount of shared potential fate.

5.3. Areas of Coordination

5.3.1 Underserved Regions

In order for root server operators to work together and prioritize underserved regions it is first necessary to define what an underserved region is. For example, there are many more root servers instances in Europe than there are in Asia, but when discussing underserved regions a more nuanced approach is necessary. We must also understand how well a given instance serves the region in which it is installed. Installing infrastructure into a regional Internet Exchange (IX) is likely to provide a quick win to local ISP's and business. However, IX's are not popular in many regions and therefore it may be required to install multiple instances in many regional ISP's to achieve the same effect that a single IX location may have.

Local routing policy within a given region may also affect latency in some instances. A region may have good proximity to numerous fast anycast nodes, but for routing reasons recursive resolvers in that region may not use them, or queries may be routed across distant links and back again causing increased latency.

We also have to be aware of Internet penetration numbers. Roughly 80% of Europe[9] has Internet connectivity vs 31% in Africa.[10] It therefore makes some sense for Europe to have more instances. As a simple comparison of populations nearby instances is not necessarily an appropriate measure of need.

Further research is needed to better define what an underserved area is and how better to identify these areas. High average resolver to root server latency within a given region may be a good indicator of an underserved region. It may also be the case that DOS attacks repeatedly affecting a specific region may require the deployment of more anycast nodes, or that inter-region routing policies impact query response times negatively. Besides the obvious request by local organizations for the placement of local anycast nodes, there is no clear method for determining underserved areas to aid in anycast node placement.

5.3.2 Shared Fate and Redundancy

The data on www.root-servers.org displays that there are many locations where multiple letters are represented with instances. This may be desirable, but it also creates situations where a catastrophic event occurring in this location negatively impacts all instances at this location. Seemingly geographically diverse instances can also share fate due to similarity in vendors, electricity grid, geopolitics, or large catastrophic events affecting multiple locations (e.g., hurricanes, floods).

[9] See http://www.internetworldstats.com/stats4.htm.

[10] See http://www.internetworldstats.com/stats1.htm.

Recommendation 1: RSOs should continue to discuss and share lists of components and vendors for the purposes of avoiding unintentional shared fate. This will give all operators a better picture of cases where shared fate exists, and allow them to coordinate between each other to remove common points of failure. Each operator should decide what information to share, and analyze shared information independently, according to their own practices.

5.3.3 Coordination during Attacks and Catastrophic Events

In addition to coordination when things are going well, operators should be prepared, and have redundant communication channels in place, to coordinate in times of outages or DOS attacks. This kind of coordination requires operators to establish effective and trustworthy communication methods, as well as when to use them, prior to any event that requires their use.

Recommendation 2: RSOs should establish or maintain existing backup communications methods necessary in the event of catastrophe. Sharing of contact information and any cryptographic information necessary for authentication and identity should be kept up to date, and regular testing should be carried out to ensure backup communications channels will still function when needed.

6. Security

6.1 Mitigating Influence of BGP Route Instability

IP routing works on the principle of Longest Prefix Match (LPM) whereby the next-hop for packets is determined by the longest prefix advertised. If an attacker wanted to prevent traffic from reaching a specific root server identity, that attacker could potentially trick network operators into accepting forged route advertisements with longer prefixes than the valid ones. This attack is commonly known as a Border Gateway Protocol (BGP) route hijack.

If a router receives an advertisement with a longer length prefix for a root server identity it would automatically choose this advertisement over all others for the same identity. However, most network operators place an upper-limit on the length of prefix they will accept from their BGP peers. For example, most network operators will not accept an advertisement for any IPv4 prefix longer than 24 bits or any IPv6 prefix longer than 48 bits. This is done partly to ensure that their routers have enough space in memory to store the entire routing table and also to prevent route hijacking attempts. As of July 2017, all RSOs originate a 24 bit IPv4 prefix and most RSOs originate a 48 bit IPv6 prefix for their respective root server instances.

Anycast routing adds another aspect to this kind of attack because anycast routing exploits the fact that most destination prefixes appear to have multiple next-hops, regardless of whether or not that destination prefix is being advertised from multiple topological end-points on the Internet(i.e. anycast). In theory, a router will always choose the next-hop associated with the topologically closest instance of any root server identity.

Given this, an attacker wishing to trick routers into accepting forged route advertisements with equal length prefixes would need to originate them topologically closer than all other instances of that identity. This means that an attacker would need to be topologically close to all instances of a given identity to redirect traffic away from all of its instances.

Recommendation 3: The RSSAC Caucus should investigate and assess the value of the Resource Public Key Infrastructure (RPKI) as a possible framework for validating the route advertisements of RSOs.

Recommendation 4: RSOs should originate the longest IPv4 and IPv6 address prefixes accepted by the vast majority of BGP speakers on the Internet. Currently, and for the foreseeable future, this is 24 bits for IPv4. The IPv6 value is likely more fluid, but for the time being is /48 bits.[11]

Recommendation 5: RSOs should monitor the reception of their BGP route advertisements at multiple topologically diverse locations for attempted route hijacking attempts.

Recommendation 6: Recursive resolver operators concerned with route hijack attacks should consider RFC 7706 as a fallback mechanism in case of emergency.

7. Ways to Improve Anycast DNS Resilience

Increasing service resilience from the resolver perspective is likely to come from the resolver's ability to make better decisions about which identity to choose when service level degrades, under what conditions to retry connections, when to give up on an identity, and ensuring that requests are sent to a legitimate DNS root instance. Resolver-level measures for improving resilience, however, is largely out of scope for this document.

From the provisioning side, the resilience of the root DNS anycast system can be described along four dimensions. These are:

- Ability to withstand attacks. This refers to the amount of excess capacity that is built into the system such that failure of some proportion of nodes will not drastically (measured in response time) affect the root DNS service as a whole.

- Ability to degrade gracefully. When service degrades (which is essentially a qualitative metric, but could be described in terms of changes in connectivity) the failure states are reached gradually, which would enable some form of intervention before total loss of service occurs.

[11] See https://tools.ietf.org/html/rfc7454#page-12.

- Ability to contain faults. This refers to the extent to which faults propagate to multiple nodes and identities. A well contained fault will affect as few as possible nodes and identities.

- Ability to respond to and recover from attacks quickly. While some part of service resilience speaks to the ability of the system to automatically adapt and recover from failure conditions, a large part of the response today requires human intervention to triage and contain faults. So this aspect of resilience refers to the ability of service operators to detect and respond to events in a way that maintains the availability of the service as a whole.

Resilience of the root DNS service can be improved by strengthening resilience along each of the aforementioned dimensions. Specific measures that could be used to increase resilience at the service provisioning end are listed in the sub-sections below. Each measure has certain trade-offs associated with it. Thus they are described in terms of their advantages and disadvantages.

7.1 Increasing Anycast Instance's Link or Site Capacity

Capacity relates to the volume of traffic that a given anycast node is able to sustain either in terms of the number of packets or in terms of processing capacity. Link capacity can be enhanced through interconnection agreements with upstream ISPs, while computing capacity can be improved through more powerful processors or scaled up computing capabilities.

Advantages

- Increases the ability of a specific instance to withstand a larger volume of attacks, thereby increasing the ability to withstand attacks for the specific identity, and root DNS service as a whole.

Disadvantages

- If a highly provisioned node fails because it is overwhelmed, the service degradation may be abrupt if the other nodes are unable to provide the same level of DNS service. This can result in cascading failure as nodes already burdened with traffic become burdened with the new traffic of the failed node.
- The failure of the provisioned load may result in second-order failures of other nodes that are unable to sustain the shifting query load.
- Other node operators may lack visibility and hence the ability to respond to the impending failure of their nodes on account of second-order effects from failure of the well-provisioned node.

7.2 Increasing the Number of Anycast Instances

[COMMENT: This section is making a lot of implicit assumptions and seems to ignore some of the current practice when it comes to anycast use by root operators. It also seems to confuse anycast instances (i.e. servers per letter) with the different root letters operations. This also assumes that any additional anycast instances will make a difference without even attempting to define what the current number of instances is and what percentage of increase is likely to have any impact. With the current global spread over hundreds of locations globally, any impact may well be insignificant unless the number of locations is increased up into the thousands of instances. Do we have any data to support this? An additional aspect is that in reality, any increased number of anycast instances will likely come with increased topological diversity, so 2.2.2 and 2.2.3 are somewhat hard to separate.]

Advantages

- Increases spare capacity if the query load is evenly distributed across all related instances.
- May improve responsiveness, in theory recursive resolvers will receive responses faster with more Anycast instances.
- May result in more graceful degradation of service if failure of a few nodes can be easily mitigated by the other nodes.
- May enable fault containment if attacks/fault-trigger can be directed to some small number of nodes. Even if such nodes fail the larger user population can still reach other nodes.

Disadvantages

- Justification of cost towards deploying a new node purely on the basis of increasing spare capacity may be difficult for some operators.
- Greater risk for failure due to systemic problems if this increase in Anycast instances would lead to reduced diversity between nodes. However, when applied wisely by operators this will unlikely be an issue in practice.

7.3 Increasing Topological Diversity

Topological diversity relates to the isolation of one anycast instance from network faults on the path to other anycast instances.

Advantages

- Service disruptions can be contained closer to where DOS attacks originate.
- Source of DOS attacks can be detected with more precision.
- DOS attacks originating within a topological area can be more easily contained within that area.

Disadvantages

- Greater need to coordinate between operators to detect impending failures.

7.4 Increasing Software Diversity

The software here primarily relates to the name server software that is used to serve the root authoritative name server instance. However, it could encompass other types of software within the root server ecosystem, including the different flavors of operating systems that run the various name server instances as well as routing solutions.

Advantages

- Reduces systemic dependencies by varying software execution paths.
- Reduces chance that one software fault will cause a significant number of nodes to fail.

Disadvantages

- Increases number of software execution paths thereby increasing risk of software faults manifesting, albeit with more limited effects given the reduced exposure.
- Increases the level of effort required to configure and manage multiple heterogeneous applications at scale.

7.5 Enabling Site-Specific Protections

Site-specific measures include the use of specific technologies including response rate limiting measures, or the use of vendor-provided DoS protection and mitigation services.

Advantages

- Increases the ability of the system to service a greater number of legitimate DNS resolvers.
- Service is likely to degrade more gracefully under attack conditions, although it may not prevent failure conditions through second-order cascading failures.

Disadvantages

- Introduces a systemic dependency. If there is a problem with the site-specific mechanism, then all nodes that implement it are impacted simultaneously.

8. Recommendations for Further Study

In most cases there is insufficient data to describe specific resilience properties of the current anycast root DNS service, so this section will mainly describe the types of studies that will need to be performed in order to develop that understanding.

In addition, information on site-specific measures such as increasing link/site capacity and enabling specific protection mechanisms are not likely to be made public, so in this section we only comment on resilience studies that relate to increasing the number of anycast instances or increasing the diversity.

8.1 Understanding the Effect of Increasing Number of Instances

The types of studies that can be performed to increase our understanding of resilience in relation to the number of anycast instances include the following.

- Description of observed and published anycast instances per identity.
- Comparison of response times for identities that have a greater number of anycast instances against those that have fewer, all other factors considered equal.
- Does increasing (reducing) the number of nodes help in better (poorer) containment of faults?
- How much does increasing (reducing) the number of anycast nodes decrease (increase) the potential for effects to cascade to other (un-related) instances?
- How can underserved areas be identified to better determine the placement of new anycast nodes?

8.2 Understanding the Effect of Diversity

The types of studies that can be performed to increase our understanding of resilience in relation to diversity of anycast instance deployment include the following.

- Description of geographical distribution and topological (upstream ISP) diversity of observed anycast instances per identity and for the service as a whole
- Measuring locality of service (might be able to leverage existing studies)

8.3 Understanding Effects of Latency on Stub Resolvers

The types of studies that can be performed to increase our understanding of how an end user's experience can drive decisions of anycast deployment include the following.

- Does increasing the number of anycast nodes help in stub resolvers resolving names more quickly?

- Does decreasing latency between a root server and a user's recursive resolver change the user's Internet experience significantly? How?

9. Acknowledgments, Disclosures of Interest, Dissents, and Withdrawals

In the interest of transparency, these sections provide the reader with information about four aspects of the RSSAC process. The Acknowledgments section lists the RSSAC caucus members, outside experts, and ICANN staff who contributed directly to this particular document. The Statement of Interest section points to the biographies of all RSSAC Caucus members. The Dissents section provides a place for individual members to describe any disagreement that they may have with the content of this document or the process for preparing it. The Withdrawals section identifies individual members who have recused themselves from discussion of the topic with which this Advisory is concerned. Except for members listed in the Dissents and Withdrawals sections, this document has the consensus approval of the RSSAC.

9.1 Acknowledgments

RSSAC thanks the following members of the RSSAC Caucus and external experts for their time, contributions, and review in producing this report.

RSSAC Caucus members
Ray Bellis
Marc Blanchet
John Bond
Ray Gilstrap
Shane Kerr
Ramet Khalili
Suresh Krishnaswamy
Warren Kumari
Robert Martin-Legene
Daniel Migault
Paul Muchene
Russ Mundy
Abby Pan
Rao Naveed Bin Rais
Anand Raje
Kaveh Ranjbar
David Song
William Sotomayor
Ryan Stephenson
Ondrej Sury
Suzanne Woolf
Romeo Zwart

ICANN Support Staff
Andrew McConachie (editor)
Kathy Schnitt

Steve Sheng (editor)

9.2 Statements of Interest

RSSAC Caucus member biographical information and Statements of Interests are available at:
https://community.icann.org/display/RSI/RSSAC+Caucus+Statements+of+Interest

9.3 Dissents

There were no dissents.

9.4 Withdrawals

There were no withdrawals.

10. Revision History

10.1 Version 1

Current version.