RSSAC00X version 1
Technical Analysis of the Naming Scheme Used For Individual Root Servers

An Advisory from the ICANN Root Server System Advisory Committee (RSSAC)
13 October 2016

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 conducted a technical analysis of the naming scheme used for individual root servers.

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

The Domain Name System (DNS) is supported by root servers that serve the root zone. Individual root servers were named under the "root-servers.net" domain in 1995. The root-servers.net zone is delegated to the root servers.

This naming scheme has worked well for root servers and the Internet community at large for over two decades. However, given today's Internet environment, the RSSAC would like to study the naming scheme used for individual root servers and consider whether changes need to be made.

The study briefly documents the technical history of the names assigned to individual root servers since the creation of the root server system. It also documents and performs a risk analysis of different alternative naming schemes.

This analysis includes:

- Where the name resides in the DNS hierarchy
- Who administers the zone in which the names reside
- How the names can be validated with DNSSEC
- The size of priming responses

From the risk analysis, the document aims at providing:

- Recommendations toward signing the FQDNS associated with the root servers.
- Recommendation on the naming scheme for the root servers.
- Recommendation to root server operators, root zone management partners, and ICANN on whether changes should be made, and what those changes should be.

1.1 Scope of Work

On 9 July 2015 the RSSAC issued a scope of work that provided direction for the work described in this document. As a courtesy to reviewers, the specified scope is included below, together with commentary on the treatment of each point provided in this document.

RSSAC Scope of Work	Response
Document the technical history of the names assigned to individual root servers since the creation of the root server system.	*See Section 4*
Consider changes to the current naming scheme, in particular whether the names assigned to individual root servers should be moved into the root zone from the ROOT-SERVERS.NET zone.	*See section 5*
Consider the impact on the priming response of including	*See section 5 and*

DNSSEC signatures over root server address records.	*Appendix A*
Perform a risk analysis.	*See section 6*
Make recommendations to root server operators, root zone management partners and ICANN on whether changes should be made, and what those changes should be.	*See section 7*

2. Terminology

In addition to the below terms, this document also uses common DNS terms from RFC 7719.

Authoritative server – A system that responds to DNS queries with information about zones for which it has been configured to answer with the Authoritative Answer (AA) flag in the response header set to 1. It is a server that has authority over one or more DNS zones.

Delegation – A delegation is indicated by the presence of an NS RRset which associates a domain name (on the left side) to a server name (on the right side). It indicates that the server names present in this RRset are authoritative for all labels below this domain name (unless there is a further delegation).

DNSSEC priming resolution – The act of a resolver fetching its initial set of DNS root server address records, including any DNSSEC metadata associated with those records.

Glue records – Resource records within a response that are not part of authoritative data but are necessary in order to enable a resolver to complete the query resolution process under certain cases. (RFC 1034, section 4.2.1)

In-zone – Records are in-zone for a server if that server is authoritative for those records.

Key signing key (KSK) – DNSSEC keys that only sign the apex DNSKEY RRset in a zone. KSKs have the Secure Entry Point (SEP) flag set to 1. (RFC 6781)

Priming resolution – The act of a resolver getting its initial set of addresses for the DNS root servers. The reasons that a recursive resolver needs this information, and the mechanisms it can use to get it, are covered in https://datatracker.ietf.org/doc/draft-ietf-dnsop-resolver-priming/.

Resolver – A program that retrieves information from name servers in response to client requests. (Quoted from [RFC1034], section 2.4) A resolver performs queries for a name, type, and class, and receives answers. The logical function is called "resolution".

Resource Record Set (RRset) – A set of resource records with the same label, class and type, but with different data. (RFC 2181)

Zone signing key (ZSK) – DNSSEC keys that can be used to sign all the RRsets in a zone that require signatures, other than the apex DNSKEY RRset. (RFC 6781)

3. Brief Functional Description of Root Servers

The root servers are the authoritative servers for the root zone and are designated by a combination of NS and A/AAAA RRsets. The NS RRsets provide the domain names and the A/AAAA records provide the IP addresses for each record in the NS RRset.

Resolvers fetch the full list of root NS and A/AAAA resource records as part of the priming resolution process. The ability to start the DNS lookup process for a given name from any root name server adds resilience to the DNS lookup process.

The responses for NS and A/AAAA records may or may not contain DNSSEC records. The presence of DNSSEC-signed records enables the resolver to protect itself from various name-based attacks. Currently, the root zone itself is signed, but the zone that contains the root server names (root-servers.net) is not. Therefore, responses in the priming resolution currently contain DNSSEC meta-data for the NS but not the A/AAAA resource record sets.

4. Brief History of Names Assigned to Individual Root Servers

This section is an excerpt from the still-in-progress *RSSAC History of the Root Server System*.

RFC 1034 and RFC 1035 were published in November 1987. Following that time, nine root servers were assigned; their names are preserved in comments still published in the root hints file: NS.INTERNIC.NET, NS1.ISI.EDU, C.PSI.NET, TERP.UMD.EDU, NS.NASA.GOV, NS.ISC.ORG, NS.NIC.DDN.MIL, AOS.ARL.ARMY.MIL, NIC.NORDU.NET.

By April 1993, the number of root name servers had grown to an extent where the size of a root hints response was approaching the limit of 512 bytes. The limitation is specified in RFC 1035 because at the time there were networks that could not handle DNS packets larger than 512 bytes without fragmenting, as well as known firewall rules to drop DNS packets more than 512 bytes in size.

To address this issue, Bill Manning and Paul Vixie developed a plan to rename all root servers under the root-servers.net domain. This would allow the use of DNS label compression to fit all the names within 512 bytes. Domain name compression was

introduced in RFC1035 as an optional protocol feature and later mandated by RFC1123, domain name compression allows an entire domain name or a list of labels at the end of a domain name be replaced with a pointer to a prior occurrence of the same name in the same message, thus eliminating the repetition of domain names in a message and reducing the size of the message. In the case of responses to root server priming queries, the domain root-servers.net appears only once in the response, instead of one time for each root server.

Postel (IANA) agreed with the plan and Mark Kosters began the renaming phases in 1995. Table 1 below lists this renaming.

Table 1: Renaming of Root Servers in 1995

Original Name	New Name	Organization
NS.INTERNIC.NET	A.ROOT-SERVERS.NET	InterNIC (operated by NSI)
NS1.ISI.EDU	B.ROOT-SERVERS.NET	Information Sciences Institute
C.PSI.NET	C.ROOT-SERVERS.NET	PSINet
TERP.UMD.EDU	D.ROOT-SERVERS.NET	University of Maryland
NS.NASA.GOV	E.ROOT-SERVERS.NET	NASA Ames Research Center
NS.ISC.ORG	F.ROOT-SERVERS.NET	Internet Software Consortium (ISC)
NS.NIC.DDN.MIL	G.ROOT-SERVERS.NET	GSI (operated by NSI)
AOS.ARL.ARMY.MIL	H.ROOT-SERVERS.NET	Army Research Lab (ARL)
NIC.NORDU.NET	I.ROOT-SERVERS.NET	NORDUnet

By moving to root-servers.net, operators were able to take advantage of DNS label compression. This enabled four additional root servers to be added to fit within a 512 byte DNS response. In January 1997, servers J-Root, K-Root, L-Root, and M-Root, were added as root server systems.

5. Analysis of Naming Schemes

This section describes various naming schemes for the root zone and associated root servers, including the current naming scheme. There are many characteristics that need to be considered when evaluating a naming scheme:

- Where the name resides in the DNS hierarchy
- Who administers the zone in which the names reside
- How the names can be validated with DNSSEC
- The size of priming responses

This section looks at different naming schemes, including:

1. The current naming scheme
2. The current naming scheme with that zone signed
3. In-zone NS RRset
4. Shared delegated TLD
5. Names delegated to each operator
6. Single shared label for all operators

Each of the schemes is further described from section 5.1 to section 5.6. Appendix A shows how recent authoritative servers would act for each of the scenaros given.

Other than the first scheme, all schemes result in the addresses of the root zone's nameservers to be DNSSEC signed (if no delegation occurs), or a signed delegation (unsigned NS records plus signed DS record(s)).

In order to maintain compatibility with current resolvers, this list does not include any proposal that would cause the response to a priming query that includes all 13 of the current root servers' IPv4 addresses to be larger than 512 bytes.

In the schemes that use new short labels in the root, "a", "b" and so on are used because those are the same names that are used today for the root server operators. Further study might be needed to see if those short labels in the root will cause any significant problems.

Fragmentation may cause problems that result in lost packets, either due to loss of fragments, or due to network equipment that blocks fragments. Resolvers should be able to recover from such losses such as by using smaller requested UDP sizes and retrying or by retrying over TCP. Individual root server operators may make different decisions on whether fragmentation is something they want to allow or to prevent fragmentation by offering a lower UDP size.

Regardless of the scheme, the size of UDP responses is controlled by a negotiation between the resolver and the individual root server receiving the query. The size used will be the smaller of the configured value on the root server, and the size requested by the resolver. Individual root server operators may configure different sizes. Depending on

the scheme, smaller negotiated values may result in exclusion of RRSIGs in the Additional section, or even truncation (with the response having TC=1 set) if the answer will not fit in the UDP response; such a response would require retry over TCP. The exclusion of RRSIGs may result in resolvers performing additional queries in order to obtain signatures.

5.1 The Current Naming Scheme

In the current naming scheme, the authoritative servers for the root zone have the names "[a-m].root-servers.net". The root-servers.net zone is served by name servers that also serve the root zone. In this scheme, the root-servers.net zone continues to be not signed.

Advantages of the current scheme are:

- The zone split of the root-servers.net zone follows the traditional DNS rules and limits the risk of any misinterpretation.
- Each root zone operator has control over assignment of the IP addresses for their name servers.

Drawbacks of the current scheme are:

- The root and root-servers.net zones need to be synchronized, and stay synchronized, because information associated with the root servers is located in two different places.
- Root servers are not authoritative for the .net zone. This means that if the authoritative servers for the .net zone were down, it could prevent the resolution of the root-servers.net zone.
- Because the root server names are not signed, there is the possibility for other DNS-based attacks on the root server infrastructure.

5.2 The Current Naming Scheme, with DNSSEC

This is the same as the preceding scheme, but with root-servers.net being signed by the zone's maintainer.

Glue records are included in the root zone distributed by IANA. However, because the root zone is not authoritative for these glue records, the root zone would not contain their associated RRSIG records; in this scheme, the corresponding RRSIGs would be hosted in the root-servers.net zone. Different authoritative server software will act differently with respect to those glue records. Some authoritative server software will include the RRSIGs, others won't.

Possible advantages of this scheme are:

- The zone split of the root-servers.net follows the traditional DNS rules thereby limiting risk of any misinterpretation.
- Each root zone operator has control over the assignment of IP addresses for their name servers.

- Signing the root-servers.net zone enables DNSSEC-aware resolvers to protect themselves against DNS-based attacks on the root server infrastructure.

Possible drawbacks of this scheme are:

- The root, root-servers.net and net zones need to be synchronized, and stay synchronized, because information associated with the root servers is located in three different places.
- Root servers are not authoritative for the .net zone. This means that if the authoritative servers for the net zone were down, it could prevent the resolution of the root-servers.net zone.
- If the servers for the net zone were unavailable, the DS records for root-servers.net zone would not be obtainable and validation of the priming response would fail.
- After the priming query, a validating recursive resolver must query the net zone for the NS and DS records, and then query root-servers.net in order to get the DNSSEC data. This results in additional round trips for the resolver.

5.3 In-zone NS RRset

The root zone will have an NS RRset consisting of in-zone names pointing to the A and AAAA records of the root servers. Because the records are maintained in the root zone, there would be no delegation points and the root zone would be authoritative for all content required for a priming query response. In this proposal, the names can either have all records under a common undelegated label (for example, the names “a.root-servers”, “b.root-servers”, and so on) or can be short labels in the root zone (for example, the names “a”, “b”, and so on).

Depending on the name server software and configuration, the response to a priming query would contain an Answer section with 13 NS records and an Additional section that may contain all 13 A and AAAA glue records and 26 RRSIG records.

Possible advantages of this scheme are:

- The names could be similar to the current lettering scheme.
- All data is protected by DNSSEC.
- The DNSSEC data could be returned in the first query. There is no DNSSEC chain to follow; and, in an ideal situation, all RRSIG records would be contained in the response.
- Authentication of priming query responses requires only a single key. There are no additional DS records or additional keys for subordinate zones.
- It is syntactically elegant because the zone is clearly authoritative for its own name servers. There is no ambiguity regarding where the content could be found.
- Administration is simplified, since changes only require one entity.

Possible drawbacks of this scheme are:

- There may be name collisions from search lists (similar to the possibility of name collisions that happen any time a new TLD is added to the root zone) for this new common undelegated domain or the short labels.
- The response size with a full additional section of a standard priming query would far exceed the common MTU sizes for both IPv4 (1500) and IPv6 (1280). There is evidence that many networks drop IPv6 extention headers (and thus may also drop fragmented IPv6 packets) as well as dropping ICMPv6 packets.

5.4 Shared Delegated TLD

The root zone will have an NS RRset that consists of 13 domain names that share a new common delegated TLD (for example, the names “a.root-servers”, “b.root-servers”, and so on). There will be 13 records in the root zone’s NS RRset pointing to the root server nameserver instances. The new shared TLD will be delegated to the same set of nameservers.

The response to a priming query has an Answer section with 13 NS records and an RRSIG for the NS RRset, and an Additional section with all the A and AAAA glue. Name server implementations differ in their behavior on whether the RRSIGs for these A and AAAA records are returned in the priming response. If the RRSIG RRset for the addresses is missing, a validating recursive resolver must query the root for shared TLD’s NS RRset and then query the shared TLD for the A and AAAA RRsets.

It is possible to use an existing TLD that is hosted by the root servers, .arpa, for this proposal. However, that zone is administered by a different organization, the Internet Architecture Board (IAB), and thus using that TLD instead of a new one would mean that changes would need to be synchronized and approved by an external body.

Possible advantages of this scheme are:

- The names could be similar to the current lettering scheme.
- All data is protected by DNSSEC.
- The DNSSEC signatures all come from just one entity.
- Administration is simplified as changes only require one entity.

Possible drawbacks of this scheme are:

- As part of the priming query, a validating recursive resolver must query the root for the NS records, then query the shared TLD in order to get the DNSSEC data.
- There may be name collisions from search lists (similar to the possibility of name collisions that happen any time a new TLD is added to the root zone) for this new shared TLD name.

5.5 Names Delegated to Each Operator

A new domain will be delegated to each root server operator. The root zone will have an NS RRset consisting of 13 domain names that are managed by the corresponding root

server operators. The names for this proposal can either have all records under a common label (for example, the names "a.root-servers", "b.root-servers", and so on) or can be short labels in the root zone (for example, the names "a", "b", and so on). No other delegations are involved.

The response to a priming query has an Answer section with 13 NS records and an RRSIG for the NS RRset, and an Additional section with all the A and AAAA glue, but no RRSIG records. To get the RRSIG RRset, a validating recursive resolver must query the nameserver for each individual operator.

Possible advantages of this scheme are:

- The names could be similar to the current lettering scheme.
- Each root zone operator has control over assignment of the IP addresses for their name servers.
- All data is protected by DNSSEC.

Possible drawbacks of this scheme are:

- After the priming query, a validating recursive resolver must query the root for the NS records for each operator's TLD, then query the nameserver for each operator in order to get the DNSSEC data.
- There may be name collisions from search lists (similar to the possibility of name collisions that happen any time a new TLD is added to the root zone) for this new common domain or the short labels.
- Instead of just one entity signing a zone, each root zone operator needs to sign its own zone. This greatly increases the chances of operational error during the signing process, which may lead to some resolvers being unable to validate the priming queries.
- Some root server operators might not sign their zone, or might want to sign with different algorithms from the other operators, which may result in other security or operational implications that have yet to be studied.

5.6 Single Shared Label for All Operators

Instead of having individual names for each root server, the set of root servers could be given one name at the top level (such as "all-root-servers.") and that one name has the 13 IPv4 addresses and (currently) 12 IPv6 addresses of the root servers as two RRsets.

The response to a priming query has an Answer section with 1 NS record and an RRSIG, and an Additional section with all the A and AAAA glue and two RRSIG records (one each for the A and one for the AAAA RRsets).

Possible advantages of this scheme are:

- All data for the root servers is in only one place.
- Administration is simplified as changes only require one entity.

- The DNSSEC data could be returned in the first query: There is no DNSSEC chain to follow, and in an ideal situation all RRSIG records would be contained in the response
- Authentication of priming query responses requires only a single key. There are no additional DS records or additional keys for subordinate zones.
- It is syntactically elegant because the zone is clearly authoritative for its own name servers. There is no ambiguity regarding where the content could be found.

Possible drawbacks of this scheme are:

- If a priming query to any of the root servers results in a SERVFAIL or REFUSED response, resolvers might be unable to complete the priming query because they might not try to send queries to any of the other records in the A or AAAA RRset. Fixing this issue would require both protocol work and a full implementation rollout.
- There may be name collisions from search lists (similar to the possibility of name collisions that happen any time a new TLD is added to the root zone) for the single shared label.

6. Analysis of Benefits vs. Risks

The trade-offs between different naming alternatives are summarized in the table below.

Concerns	5.1 Current Naming Scheme	5.2 Current Naming Scheme with DNSSEC	5.3 In-zone NS RRset	5.4 Shared delegated TLD	5.5 Names delegated to each operator	5.6 Single Shared Label for all operators
Need to synchronize data in multiple zones	X	X		X	X	
External dependency on a zone not considered part of the root server infrastructure	X	X				
Exposure to DNS-based attacks on the root server infrastructure	X					

Increased workload associated with validating a longer authentication chain		X		X	X	
Increased round-trip delay associated with validating the priming response		X		X (some systems)	X	
Increase in priming response size		X	X	X	X	X
Corner cases and potential for errors					X	X
Name collision with search lists			X	X	X	X
Reduced root server operator autonomy						X

See Appendix A for a for a list of sizes of responses for each proposed scheme. Note that the sizes changes depending on the type of authoritative software used, and configuration parameters chosen, by the root server operator.

The current naming scheme (5.1) suffers from having a dependency on the root-servers.net and net zone, which creates the potential for inconsistencies. Furthermore, when the root-servers.net zone is unsigned, it exposes the DNS infrastructure to DNS-based attacks on the root server infrastructure. However this naming scheme is known to work with the current resolver population. Maintaining the current status quo is an option if the risks associated with making changes to the root naming infrastructure outweigh the risks of re-delegation attack or expected benefits from a new naming scheme..

The risks associated with unsigned root server names can be mitigated by signing the zone that is authoritative for these names. A number of different naming schemes are possible here, and each scheme has its own unique set of concerns.

The option that is likely to involve the least change to the existing root name server infrastructure is that of signing the root-servers.net zone (5.2). However, this approach brings with it the continued dependence on the “net” zone, with the added burden of having to ensure that the secure delegation from net to root-servers.net remains valid.

The dependency on the “net” zone can be removed by moving the root server names to the root zone (5.3) or to a new TLD under the root zone (5.4). There are trade-offs associated with each alternative. In the case of 5.3 the priming response size is largest on average. However, the additional information in the larger response also enables a validating resolver to authenticate the name server names without the need for any additional lookups. In addition, since the root server names are authoritative data in the root zone, there is no secure delegation to follow while verifying the signatures covering these names.

In the case of 5.4 there is an additional overhead associated with managing and verifying the secure delegation from the root zone to the shared TLD. In option 5.4 the shared TLD and the root zone are both served by the root servers. However, different name server implementations differ on whether or not they return RRSIG information for the name server names within the shared TLD. In cases where these signatures are not returned there is an additional lookup overhead associated with fetching this information. In cases where these signatures are returned, the response size increases.

The advantage of option 5.4 is that it fails more gracefully if fragmented responses prove to be a problem. In the worst case, if a root server returns the aggregated information in the priming response there is little difference in the response sizes between 5.3 and 5.4. However, in cases where the polled root server's implementation does not include the complete set of A/AAAA information with signatures, fragmentation may not occur and clients may not see this breakage.

It is important to note that the potential of 5.4 to fail gracefully is only conjecture at this time. Additional studies are needed to verify this claim empirically.

Another variant, in which a separate delegation is made to each root server operator (5.5), may afford the root server operators greater flexibility and autonomy over the definition of the root server names. However this flexibility comes at the cost of increasing the round-trip delay and overhead associated with signing and operating multiple signed zones, and for validating the A/AAAA resource record set for each root server operator managed zone. (There is currently experimentation with this scenario being performed by the Yeti DNS Project.)

The final variant (5.6) trades the overhead associated with managing multiple root name server names for a larger A and AAAA RRset size. Because the number of RRSIGs covering the A/AAAA records is far fewer, this option also produces the smallest signed priming response that contains the full set of A and AAAA records associated with the root name servers. However, this alternative may also result in new corner cases, such as in the way that query load is distributed across various root name servers if resolvers identify different root servers through their names rather than their IP addresses.

All naming schemes that introduce a new TLD or a new name in the root zone increase the potential of name collisions with existing resolver search lists. Similarly, all naming

schemes that involve a signed namespace for the root server names produce a concomitant effect on the (signed) DNS response size. However, the level of increase is different for the different options, as summarized in Appendix A.

7. RSSAC Caucus Recommendations

7.1 General Design recommendations

Recommendation 1: The root server names should be signed with DNSSEC to enable a resolver to authenticate resource records within the priming response.

Attackers have targeted the DNS in a number of ways in the past. Even though the root zone is signed, leaving the root-servers.net zone unsigned exposes the DNS infrastructure to a vulnerability that may be exploited in the future. It seems prudent to fix this vulnerability in a proactive manner, rather than in response to an actual attack when there is less time to plan any changes to the root zone.

Recommendation 2: Because the root server address information and the root zone are heavily correlated, both sets of information should be hosted on the same servers.

This can be done using delegation or including the root server names in the root zone. All information necessary to validate the root-servers' A/AAAA RRsets and the root zone SHOULD be hosted on the root servers.

7.2 Design recommendations for the current naming scheme

Recommendation 3: The root server names should be signed in a way that reduces the potential for operational breakage.

In the selection of a naming scheme for the root server names, it seems prudent to prefer alternatives that are less likely to produce new modes of operational breakage. Similarly, any unnecessary dependencies that could introduce new errors should be removed. In particular, if there is a desire for enabling DNSSEC for the root server names, there are better options to accomplish this than signing the root-servers.net zone. Although signing root-servers.net remains a valid option for having root zone related information signed, the RSSAC Caucus recommends that signing be done using a naming scheme that better fits the DNSSEC requirements.

Recommendation 4: Preferred Alternative

Among the various options considered in this document, options 5.3 and 5.4 are both viable for signing the root server names. Additional studies are needed to determine which of these options, if any, would be more favorable than the other in practice.

Recommendation 5: Additional studies on reducing the response size should be conducted.

When considering priming response under DNSSEC, the single root server FQDN scheme generated the smallest possible size, as expected. However, since the DNS protocol does not support this configuration, that result is not relevant. Future work in this area could include modeling and proposing protocol changes to support this configuration, noting that the total cost shown by such a model might outweigh the accompanying total benefit.

The RSSAC Caucus recommends further study be made to reduce the response size by considering:

- Using different cryptographic algorithms
- Advertising what is expected in the Additional section (this would require modifying the DNS protocol)
- Having a single key for the root zone instead of the current KSK + ZSK scheme
- Choosing a naming scheme with a single root name server FQDN
- Testing the consequences of all large responses having the TC bit set
- Backward-compatible protocol enhancements using EDNS0 that would support a priming-specific single signature over the entire priming set (NS, A, AAAA, DNSKEYs)

7.3 Further Studies

To better understand the findings of this report, DNS researchers should look into the following topics that have been covered earlier in this document. The operational differences between options 5.3 and 5.4 are particularly relevant for such further research. Some topics that would be of interest include:

- The acceptable response size (beyond the normal MTU) for priming queries requires further study. For example, IoT devices that are acting as validating recursive resolvers might not be able to receive long priming responses.
- Different resolvers will respond differently when answers contain a reduced set of glue records.
- In the unusual case that a recursive resolver uses a DNS search list, using a single label for the root servers may interfere with that search list mechanism unless the final '.' is given in the searched-for names.

8. 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.

8.1 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
Joe Abley (work party leader)
John Bond (work party leader)
Brian Dickson
Paul Hoffman
Suresh Krishnaswamy
Warren Kumari
Matt Larson
Declan Ma
Bill Manning
Jim Martin
Robert Martin-Legene
Daniel Migault
Shinta Sato
Arturo Servin
Davey Song
William Sotomayor
Paul Vixie
Wesley Wang
Suzanne Woolf

ICANN Support Staff
Andrew McConachie
Kathy Schnitt
Steve Sheng (editor)

8.2 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

8.3 Dissents

There were no dissents.

8.4 Withdrawals

There were no withdrawals.

9. Revision History

9.1 Version 1

Current version.

Appendix A: Results from Testing Common Authoritative Servers

The test bed consists of very recent versions of popular authoritative servers running with very minimal configurations.

The servers are running:

- BIND 9.10.3
- Knot 2.2.1
- Knot 2.3.0
- NSD 4.1.13

The zone files corresponding to the proposals were created by John Bond. The zone files can be AXFR'd from the addresses given in the configuration files.

Configuration Files

The configuration files used are listed on the following pages.

Proposal 5.1

```
knot.conf:
    server:
      listen: 0.0.0.0@53
      listen: ::@53
    remote:
      - id: master
        address: 2001:41c8:101::51
    zone:
      - domain: "."
        master: master
      - domain: "root-servers.net"
        master: master

named.conf:
    options { recursion no; empty-zones-enable no ; dnssec-enable yes;
      listen-on { any; }; listen-on-v6 { any; }; };
    zone "." { type slave; masters {2001:41c8:101::51;}; };
    zone "root-servers.net." { type slave; masters {2001:41c8:101::51;}; };

nsd.conf:
    zone:
      name: "."
      request-xfr: 2001:41c8:101::51 NOKEY
      allow-notify: 2001:41c8:101::51 NOKEY
    zone:
      name: "root-servers.net"
      request-xfr: 2001:41c8:101::51 NOKEY
      allow-notify: 2001:41c8:101::51 NOKEY
```

Proposal 5.2

```
knot.conf:
    server:
      listen: 0.0.0.0@53
      listen: ::@53
    remote:
      - id: master
        address: 2001:41c8:101::52
    zone:
      - domain: "."
        master: master
      - domain: "root-servers.net"
        master: master

named.conf:
    options { recursion no; empty-zones-enable no ; dnssec-enable yes;
      listen-on { any; }; listen-on-v6 { any; }; };
    zone "." { type slave; masters {2001:41c8:101::52;}; };
    zone "root-servers.net." { type slave; masters {2001:41c8:101::52;}; };

nsd.conf:
    zone:
      name: "."
      request-xfr: 2001:41c8:101::52 NOKEY
      allow-notify: 2001:41c8:101::52 NOKEY
    zone:
      name: "root-servers.net"
      request-xfr: 2001:41c8:101::52 NOKEY
      allow-notify: 2001:41c8:101::52 NOKEY
```

Proposal 5.3

```
knot.conf:
    server:
      listen: 0.0.0.0@53
      listen: ::@53
    remote:
      - id: master
        address: 2001:41c8:101::53
    zone:
      - domain: "."
        master: master

named.conf:
    options { recursion no; empty-zones-enable no ; dnssec-enable yes;
      listen-on { any; }; listen-on-v6 { any; }; };
    zone "." { type slave; masters {2001:41c8:101::53;}; };

nsd.conf:
    zone:
      name: "."
      request-xfr: 2001:41c8:101::53 NOKEY
      allow-notify: 2001:41c8:101::53 NOKEY
```

Proposal 5.4

```
knot.conf:
    server:
      listen: 0.0.0.0@53
      listen: ::@53
    remote:
      - id: master
        address: 2001:41c8:101::54
    zone:
      - domain: "."
        master: master
      - domain: "root-servers"
        master: master

named.conf:
    options { recursion no; empty-zones-enable no ; dnssec-enable yes;
      listen-on { any; }; listen-on-v6 { any; }; };
    zone "." { type slave; masters {2001:41c8:101::54;}; };
    zone "root-servers." { type slave; masters {2001:41c8:101::54;}; };

nsd.conf:
    zone:
      name: "."
      request-xfr: 2001:41c8:101::54 NOKEY
      allow-notify: 2001:41c8:101::54 NOKEY
    zone:
      name: "root-servers"
      request-xfr: 2001:41c8:101::54 NOKEY
      allow-notify: 2001:41c8:101::54 NOKEY
```

Proposal 5.5

```
knot.conf:
    server:
      listen: 0.0.0.0@53
      listen: ::@53
    remote:
      - id: master
        address: 2001:41c8:101::55
    zone:
      - domain: "."
        master: master
      - domain: "a.root-servers"
        master: master

named.conf:
    options { recursion no; empty-zones-enable no ; dnssec-enable yes;
      listen-on { any; }; listen-on-v6 { any; }; };
    zone "." { type slave; masters {2001:41c8:101::55;}; };
    zone "a.root-servers." { type slave; masters {2001:41c8:101::55;}; };

nsd.conf:
    zone:
      name: "."
      request-xfr: 2001:41c8:101::55 NOKEY
      allow-notify: 2001:41c8:101::55 NOKEY
    zone:
      name: "a.root-servers"
      request-xfr: 2001:41c8:101::55 NOKEY
      allow-notify: 2001:41c8:101::55 NOKEY
```

Proposal 5.6

```
knot.conf:
    server:
      listen: 0.0.0.0@53
      listen: ::@53
    remote:
      - id: master
        address: 2001:41c8:101::56
    zone:
      - domain: "."
        master: master

named.conf:
    options { recursion no; empty-zones-enable no ; dnssec-enable yes;
      listen-on { any; }; listen-on-v6 { any; }; };
    zone "." { type slave; masters {2001:41c8:101::56;}; };

nsd.conf:
    zone:
      name: "."
      request-xfr: 2001:41c8:101::56 NOKEY
      allow-notify: 2001:41c8:101::56 NOKEY
```

BIND 9.10.3

	No EDNS	v4 no DNSSEC MTU 1480	v4 no DNSSEC MTU 4096	v4 DNSSEC MTU 1480	v4 DNSSEC MTU 4096	v6 DNSSEC MTU 1220	v6 DNSSEC MTU 4096
5.1	496	755	755	913	913	913	913
5.2	496	755	755	1441	4081	1089	4081
5.3	492	751	751	1386	4089	1068	4089
5.4	492	751	751	1425	4005	1081	4005
5.5	268	279	279	785	785	785	785
5.6	250	569	569	1045	1045	1045	1045

NSD 4.1.13

	No EDNS	v4 no DNSSEC MTU 1480	v4 no DNSSEC MTU 4096	v4 DNSSEC MTU 1480	v4 DNSSEC MTU 4096	v6 DNSSEC MTU 1220	v6 DNSSEC MTU 4096
5.1	492	755	755	913	913	913	913
5.2	492	755	755	913	913	913	913
5.3	488	751	751	1443	1443	1141	1141
5.4	488	751	751	909	909	909	909
5.5	488	751	751	909	909	909	909
5.6	250	569	569	1045	1045	1045	1045

Knot 2.2.1

	No EDNS	v4 no DNSSEC MTU 1480	v4 no DNSSEC MTU 4096	v4 DNSSEC MTU 1480	v4 DNSSEC MTU 4096	v6 DNSSEC MTU 1220	v6 DNSSEC MTU 4096
5.1	512	755	755	913	913	913	913
5.2	512	755	755	913	913	913	913
5.3	508	751	751	1386	4089	1068	4089
5.4	508	751	751	909	909	909	909
5.5	508	751	751	909	909	909	909
5.6	250	569	569	1049	1049	1049	1049

Knot 2.3.0

	No EDNS	v4 no DNSSEC MTU 1480	v4 no DNSSEC MTU 4096	v4 DNSSEC MTU 1480	v4 DNSSEC MTU 4096	v6 DNSSEC MTU 1220	v6 DNSSEC MTU 4096
5.1	228	239	239	397	397	397	397
5.2	228	239	239	397	397	397	397
5.3	508	751	751	1386	4089	1068	4089
5.4	224	235	235	393	393	393	393
5.5	224	235	235	393	393	393	393
5.6	250	569	569	1045	1045	1045	1045