RSSAC FAQ

This page contains questions and answers to many of the most commonly asked questions of the RSSAC. It will be updated as the answers change, or as new questions become frequent.

If you have a question that is not listed below, or for further information or clarification, you may send a mail directly to ask-rssac@icann.org. If you wish to refer to a question in this FAQ, please include the number and title of the question in your email.

Number of Operators

1. Why are there 13 Root Name Servers?

In 1985 there were four root servers. From 1987-1991 there were seven, and all were located in the U.S.A. By 1993 there were eight. At this point, a problem was encountered. RFC 1035 stipulates that "messages carried by UDP are restricted to 512 bytes (not counting the IP or UDP headers)." Adding more root name servers would result in a priming response that exceeded 512 bytes. RFC 1035 does not provide a rationale for the 512-byte limit, but it is also worth noting that, at the time, there was a common expectation that IP packets on the Internet were limited to 576 bytes.

Root server operators realized that more name servers could be added if they could take advantage of DNS name compression. Thus, the proposal was made to give the root servers names in the root-servers.net zone. By 1995 the nine existing root servers had been renamed and in 1997, four more had been added, bringing the total to 13 and again reaching the 512 byte limit.

Up to that point in time Dr. Jon Postel, as the administrator of IANA, had been the one to designate root server operators. Following his death in 1998 the number of operators has not changed, although a small number have changed hands over the years.

Since that time, we have changed the landscape in several ways. We have added IPv6 addresses for each root server and signed the zone with DNS Security Extensions (DNSSEC). We have also expanded the size of messages carried over UDP using the Extension Mechanisms for DNS (EDNS) protocol extension. Common Path Maximum Transmission Unit (PMTU) values in today's Internet are governed by the Maximum Transmission Unit (MTU) of an Ethernet frame, which is 1500 bytes including the IP header.

In 2002, Internet Systems Consortium (ISC) became the first root server operator to deploy IP Anycast. Over the years the other operators followed. Anycast allows each operator to provide the service from tens or hundreds of distinct instances. While today there remain 13 root server identities, there are in fact more than 800 anycast instances in operation throughout the world.

Anycast

2. Why do some operators have many Anycast instances while other operators have only a few?

The Root Server Operators (RSOs) are independent organizations with different mandates, different operational models, and different sources of funding. These differences can affect the number of Anycast instances, as well as other operational choices. All RSOs are committed to providing high quality root DNS service.

3. How do you ensure that the root zone is properly replicated? Is there any chance of the root zone files getting corrupted by any attack or malware?

The reason that the root zone is signed is to enable the receiver of a zone file or a resource record for a root zone record to know whether such corruption has occurred. One of the good arguments for having several operators and multiple servers per operator is to enable a requesting system to get the root zone or a resource record from another source.

Commented [1]: I find this answer lacking. Ideally we should be able to say (1) zone transfers are validated with transaction signatures; or (2) there is some out-of-band checksum; or (3) each operator performs DNSSEC validation of root zones before loading them.

4. Are the number of Anycast nodes unlimited, or limited to a certain number?

Anycast operation is defined and described in RFC 4786 “Operation of Anycast Services” and RFC 7094 “Architectural Considerations of IP Anycast”. There is no inherent limit on the number of nodes in an Anycast service.

5. The root servers are replicating the authoritative root zone and republishing it. Then the Anycast instances are republishing the data from them. What is the difference between these two kinds of republishing?

RSOs receive the authoritative zone data from the Root Zone Maintainer (RZM). Each RSO then uses its own internal system of distribution to deliver the zone to all of its sites and Anycast instances.

6. We host an Anycast instance of a root server in a local city. We are seeing that it is answering queries from all over the globe. How can I make it only answers queries from the local area?

This is really a matter of IP routing and how the RSO operates its service. Some RSOs configure their routers and peering sessions so that the Anycast instance only receives local traffic. Others configure them to receive global traffic, relying on the routing system to choose the best path through the network. If you observe undesirable behavior with a hosted server, get in touch with the RSO providing the service.

7. In 2016 there was a large attack on Dyn. Could the same thing happen to all the root server Anycast instances?

Yes, at least in theory. That is one of the reasons that the Root Server System (RSS) has many operators and many root server instances. The large number of Anycast instances increases the capacity of the RSS and certainly helps in attack situations.

Commented [2]: Here we could add some facts on Dyn (10s? of locations, 100s? of servers) vs Root (hundreds of locations, thousands of servers)?

8. Why should an IXP host more than one root server?

In the event of data corruption, as mentioned in question 2, the resolution is to ask a different RSO. One of the defenses of the Root Server System (RSS) is in diversity. Having multiple root servers in an Internet eXchange Point (IXP) assists in that defense and recovery.

Commented [3]: I have issues with this answer. (1) we should generally discourage "collecting of letters" as someone put it and (2) yes to diversity but they don't all have to be in the same location.

DNS and Networking

9. How do recursive servers choose which root server to query, and which root server identity should my recursive server prefer?

This is called the server selection algorithm. The DNS protocol does not specify how a recursive name server should choose from among a set for a particular query. Thus, each recursive software vendor can determine their own server selection algorithm. Some implementations will “lock on” to the server with least latency. Some choose the server at random each time, and some distribute the queries based on complicated formulas. A 2012 paper describes the algorithm of popular implementations at the time.

We strongly advise you to let your recursive software do its job as designed, rather than trying to influence it to prefer or avoid particular servers.

10. We know the DNS works on UDP 53, can you explain when DNS works on TCP 53?

Almost all DNS clients utilize UDP transport by default for queries. However, there are some situations when TCP might be used instead.

Perhaps the most common use of TCP happens when a UDP response is truncated. Such truncation occurs when a server’s response is too large to fit in a single UDP message. This depends on the client’s advertised UDP buffer size, and any response size limits that the server may place on itself. When a client receives a response with the truncated bit set, it should retry the query over TCP to get the full response.

Another use of TCP for DNS is zone transfers. Since whole zones are generally much larger than would fit in a single UDP message, it makes sense to perform these over TCP.

TCP can also come into play when a server finds itself under attack. The server might send clients truncated responses as a way to determine whether or not the sources are spoofed. Clients that establish TCP connections can be whitelisted as non-spoofed sources. Additionally, the technique known as

Response Rate Limiting (RRL) will occasionally send truncated responses so that legitimate clients have an opportunity to receive responses over TCP, whereas the attack traffic will not retry.

For additional information on DNS-over-TCP please refer to RFC 7766.

11. How can I decrease the latency between the recursive server I run and a root server?

First, we believe you should carefully consider whether your truly need to be closer to (more) root servers. Analyze the traffic leaving your recursive name server for queries that are sent to root name servers. If you see more traffic than expected, you may be able to fix your applications or network configurations, so they don't need to query the root so often. Use programs like the Unix *dig* utility to measure actual latencies. If at least a handful of root servers are within 100 milliseconds, we believe that should generally be sufficient.

Also use tools such as traceroute to explore the network path between your recursive server and the set of root servers. If you find something that doesn't make sense (such as routing through far away locations) ask your ISP if the routing can be adjusted.

If there are no reasonably nearby root servers, then you should try to identify a nearby exchange point or data center where a root server could be located. Ask one or more of the root server operators if they would be willing to place a server there. Note however, that if a location already has one root server, the operators usually won't want to place another one there. You can find operator contact information by visiting https://www.root-servers.org and locating the "Contact Email" buttons in the Root Servers section at the bottom of the page.

12. Can you setup a root server yourself by downloading the root zone file and validating the signature yourself?

RFC 7706 describes how to do this. Note that it requires DNSSEC validation. See also the LocalRoot Project.

13. How long will a recursive server cache information?

Every DNS record has a Time-To-Live (TTL) value assigned by the operator of the zone. This determines how long a recursive name server or other client may cache the data for reuse. After this time, the recursive name server is expected to contact an authoritative server again for fresh data.

In the case of the root zone, some records are served with a 24-hour TTL and others with a 48-hour TTL.

14. Because caching will give wrong information after time, how can a resolver be updated with the correct IP address?

If you suspect that the data in a recursive name server cache is stale, you can always flush its cache or restart the server process.

DNSSEC

15. Can DNSSEC protect us from fast flux and super fast flux attacks?

No, not really. DNSSEC is designed to protect against data tampering, but not fast-flux attacks.

16. Does DNSSEC complicate the possibility of someone running their own root server?

Yes, because the zone must be regularly updated before the DNSSEC signatures expire.

17. I agree that UDP is limited to 512, TCP is limited to 4096. If I sign my zone maybe the size will exceed MTU. Will it then get dropped by a firewall?

DNS over UDP is no longer limited to 512 bytes. The Extension Mechanisms for DNS (EDNS), described in RFC 6891, defines how clients and servers can indicate support for message sizes greater than 512 bytes.

TCP is in no way limited to 4096 bytes. It is designed to deliver data of an arbitrary size.

There are some legitimate concerns about the size of signed responses. When a DNS-over-UDP response exceeds the network MTU size, it will be fragmented. Some firewall products will block these fragments. For this reason, modern recursive name servers are designed to retry queries with lower advertised EDNS buffer sizes. When the buffer size becomes low enough, the recursive name server will either receive a nonfragmented response, or a response with the truncated bit set, indicating it should retry over TCP.

RSSAC

18. How are RSSAC and RZERC related to one another? Is the RZERC a subset of the RSSAC?

The Root Server System Advisory Committee (RSSAC) and the Root Zone Evolution Review Committee (RZERC) are separate committees within ICANN, although there are liaisons between them and individuals may serve on both committees.

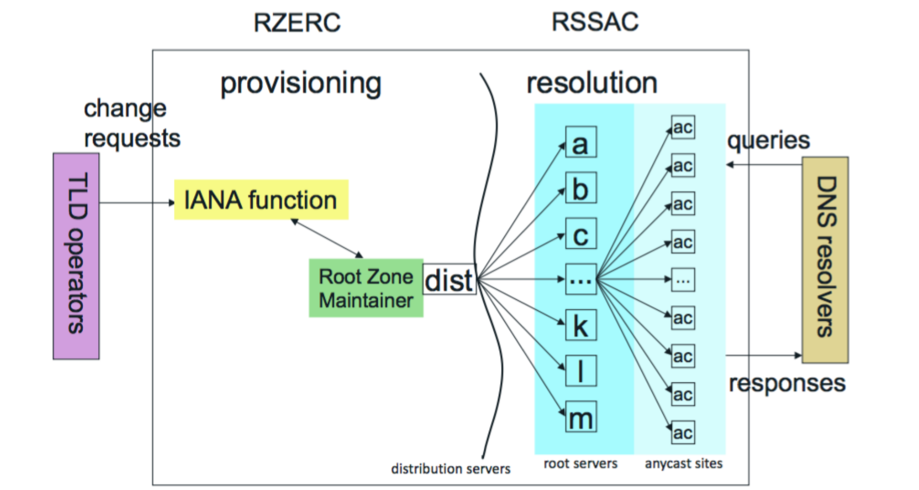
The RSSAC charter states that it:

> “..advises the ICANN Board and community on matters relating to the operation, administration, security, and integrity of the root server system.”

The RZERC charter states that it:

> “..is expected to review proposed architectural changes to the content of the DNS root zone, the systems including both hardware and software components used in executing changes to the DNS root zone, and the mechanisms used for distribution of the DNS root zone.“

The following graphic helps to explain the roles of each group.



19. Is there a timeline on when we know the number of root servers RSSAC wants to have? When will the evaluation happen to determine the number of letters?

RSSAC has no preconceptions on the number of root servers, or the number of Root Service Operators, there should be. The current limit on the number of operators is technical, not administrative.

20. Why don't we introduce the concept of every country having their own root server? So that every person can run one in their university or where ever.

Because that is not the structure of the DNS. In the telephone system, each country (identified by a country code) has an independent telephone number registry, and relationships between those registries is bilateral. In the DNS, there is a common root, which connects the world to Top Level Domain registries, and from there to Secondary Level Domains. Changing the system to have a Root Server Operator per country reduces the security and resilience of the system, because in the event of data corruption detected using DNSSEC, there is no second source of resource records. It also makes the job of a TLD registry more complex, in that it has to register in many national roots instead of the single global root.

Commented [4]: This answer seems to confuse the desire for a root server with the desire for a per-country root *zone*.

Commented [5]: Agreed. The answer is for a different question. I will leave this question out until a better answer can be given.

RSSAC Caucus

21. Is there a limit to how many RSSAC Caucus members there can be?

No.

22. What are the time requirements of RSSAC Caucus members?

RSSAC Caucus members are expected to take part in work parties and to work in the system. However, the requirements of each project differ. Thus, time requirements depend on the member and the work parties she or he joins.

Common Misunderstandings

23. Do root servers control where Internet traffic goes?

No, routers and the BGP protocol determine the path that packets take through the network on their way from source to destination.

24. Are most DNS queries handled by a root server?

No, almost all of the queries received by root servers result in a referral response which tells the recursive name server where next to ask its question.

25. Are administration of the root zone and service provisioning of the root zone the same thing?

Administration of the root zone is separate from service provision.

26. Do any of the root server identities have special meaning?

None of the root server identities are special.

27. Are there only 13 root servers?

There are more than 800 servers globally, but only 13 technical identities.

28. Do the root server operators conduct operations independently?

The RSOs do operate independently, but they also coordinate closely with each other via RSSAC and other forums.

29. Do the root servers only receive the TLD portion of the DNS query?

Historically, root servers (and indeed all DNS servers) received the entire query name in the DNS request. In 2016, the IETF published RFC 7816, which describes how DNS clients can send only the smallest necessary part of the query name. This is called Query Name Minimisation.