DNS Root Name Servers
Frequently Asked Questions

ISOC MEMBER BRIEFING #20

http://www.isoc.org/briefings/020/

January, 2005

by Daniel Karrenberg

DNS Root Name Server FAQ

This is Daniel Karrenberg's personal FAQ about the root name server system. It is based on questions he had to answer over the past few years of "Internet Governance" debate.

Daniel brought the second DNS root name server, k.root-servers.net, to Europe in 1997 and he has been responsible for its operation in the first years. Today he advises the operations team. Daniel has also helped to build significant parts of the European Internet in the 1980s; this included helping with the establishment of many ccTLDs in the area. In the 1990s Daniel led the establishment of the RIPE NCC, the first of the regional Internet registries. During this time Daniel helped to create the policy development process for Internet number resources in the RIPE region and as CEO of the RIPE NCC he has been responsible for the implementation of those policies. Through this effort he has become a practitioner at what others often refer to as "Internet governance". He prefers to be an engineer and pragmatist rather than fully engaging in the process of public policy making. However, he strongly believes that policy making should be based on as much relevant information as humanly possible. Hence this FAQ.

Q: What is it that root name servers do exactly?

A: They are part of the Domain Name System (DNS), a worldwide distributed database that is used to translate worldwide unique domain names such as www.isoc.org to other identifiers. The DNS is an important part of the Internet because it is used by almost all Internet applications.

The root name servers publish the root zone file to other DNS servers and clients on the Internet. The root zone file describes where the authoritative servers for the DNS top-level domains (TLD) are located; in other words: which server one has to ask for names ending in one of 258 (December 2004) TLDs, such as ORG, NET, NL or AU. For a detailed description of how the DNS works and the role of the root name servers see: http://www.isoc.org/briefings/016/index.shtml

Version 1 - January 27th 2005

Expanded Coverage from ISOC

A concise summary of the material covered in this FAQ is available in ISOC member briefing #19.

In-depth articles, papers, links and other resources on a variety of topics are available from the ISOC site at: www.isoc.org/internet/issues

Acknowledgments

I thank all root name server operators for providing the quantitative information contained this FAQ. The following individuals have provided substantive and useful comments which have improved the answers I give: Brian Carpenter, Steve Crocker, James Galvin, Patrik Faltstrom, Thomas de Haan, Johan Ihren and Mirjam Kuehne. However these answers as well as any errors and omissions remain my personal responsibility. I also thank the RIPE NCC for providing the resources for the work on documents like this.

Q: So the root name server operators determine who gets to operate TLDs?

A: No, absolutely and positively not! The root zone file is just published by the root name server operators. The file is edited by the IANA according to a process described on the IANA web site. The root name server operators publish the file as received from the IANA. See: http://www.iana.org/root-management.htm

Q: Does all Internet traffic pass through the root name servers?

A: No Internet traffic passes through the root name servers at all. They have nothing to do with routing, note the difference in spelling. Name servers just answer queries from other parts of the DNS.

Q: Do the root name servers store all information in the DNS?

A: No, DNS is a distributed database. Storing all the information in one place would be totally infeasible today. This is exactly why the DNS was developed as a distributed database. For a detailed description of how the DNS works and the role of the root name servers see: http://www.isoc.org/briefings/016/index.shtml

Q: Are the root name servers queried every time I browse the web or send mail?

A: No, information is cached in the DNS. Your computer will query a caching DNS server to resolve domain names. A well behaved DNS server needs to query the root name servers only once every 48 hours for each particular TLD. In the meantime it can resolve names for that TLD without involvement of the root name servers. Because of this caching almost all DNS queries are answered without involvement of the root name servers.

For a detailed description of how the DNS works and the role of the root name servers see:
http://www.isoc.org/briefings/016/index.shtml

Q: Who are the root name server operators?

A: There currently are 12 organisations providing root name service at 13 unique IPv4 addresses. They are:

A - VeriSign Global Registry Services
B - University of Southern California - Information Sciences Institute
C - Cogent Communications
D - University of Maryland
E - NASA Ames Research Center

About the Author

Daniel Karrenberg currently serves the RIPE NCC as Chief Scientist. His interests include Internet measurements, the development of the DNS and the evolution of what others often call "Internet Governance".

Daniel is one of the founders of RIPE In the 1990s Daniel led the establishment of the RIPE NCC, the first of the Regional Internet Registries. He has helped to shape Internet address space distribution policy, transferring both policy development and implementation to the region.

Daniel helped to design NSD, designed and implemented dnsmon and deployed the initial K-root server.

In the 1980s Daniel helped to build EUnet and led the effort to transition it to Internet protocols, making EUnet the first pan-European ISP and bringing Internet connections to many places in and around Europe.

Acknowledgments

The ISOC Member Briefing series is made possible through the

F - Internet Systems Consortium, Inc.
G - U.S. DOD Network Information Center
H - U.S. Army Research Lab
I - Autonomica/NORDUnet
J - VeriSign Global Registry Services
K - RIPE NCC
L - ICANN
M - WIDE Project

Information about most operators can be found via http://www.root-servers.org/, or specifically via http://X.root-servers.org/ where X stands for one of the letters listed above.

Q: What is the meaning of the letters A-M?

A: In the past each letter identified a particular server machine. Currently each letter identifies a single IPv4 address at which the service is provided under the responsibility of a single root name server operator. Some operators still provide the service from one location with one or more physical machines. Other operators provide the service from multiple locations using a method called "anycast". See below for an explanation.

Q: So where are those root name servers anyway?

A: Where in what sense? In the geographical sense there are root name servers in more than 80 locations within 34 countries (ISO3166 definition of country) worldwide (December 2004). Before you ask: the majority of them are outside the United States of America. In terms of Internet topology the servers tend to be either in very well connected places so that they can serve a maximum number of clients; others are in relatively isolated places to provide reliable service to the local community while reducing non-local DNS traffic. The exact locations of many servers are often not published for fear of physical attacks.

Q: So you mean that no one knows where all of them exactly are?

A: Yes, does any one person need to know that? I certainly do not want to know!

Q: So do you speak for all letters?

A: No! No one can do that. See further down for an explanation why this is. I speak here on personal title. I would not say things that would cause the other root name server operators to stop talking to me; I actually like the folks I work with. ;-) I try my best to keep the answers restricted to factual information; but of course they reflect who I am and where I come from. I am always open to suggestions on how to better answer these questions and for new questions, of course.

generous assistance of ISOC's

Platinum Program Sponsors: Afilias, APNIC, ARIN, Microsoft, and Ripe NCC, Sida. *More information on the Platinum Sponsorship Program*: http://www.isoc.org/isoc/membership/platinum.shtml

About the Background Paper Series

Published by:
The Internet Society
1775 Wiehle Avenue,
Suite 102
Reston, Virginia 20190
USA
Tel: +1 703 326 9880
Fax: +1 703 326 9881

4, rue des Falaises
CH-1205 Geneva
Switzerland
Tel: +41 22 807 1444
Fax: +41 22 807 1445

Email: info@isoc.org
Web:
http://www.isoc.org/

Series Editor: Martin Kupres

Q: So the root name server operators are all volunteers?

A: In the distant past, more than 10 years ago, root name server operators could be described like that. Today no root name server operator is a volunteer in any sense of the word. None of them is an individual anymore. All of them are organisations that acknowledge the obligation to provide this service. Root name server operation has not depended on single individuals for a long time. See below for answers regarding the motivation of root name server operators to provide good service.

Q: Who selects the root name server operators?

A: All root name server operators have been selected by the IANA. In the distant past there was consensus that the IANA had full discretion in the matter. Currently the IANA has no agreed process to perform this selection and I know of no specific effort currently underway to achieve consensus about an appropriate process. The authority of the IANA to make the selection is also challenged by some. Consequently the current operators are "stuck" with the task until global consensus is again achieved about the selection process.

Q: What is "IANA" anyway?

A: It stands for "Internet Assigned Numbers Authority" (or sometimes, "Internet Assigned Names and Numbers Authority"). Its job is to maintain lists of predefined numbers and names that have to be agreed by everyone for the Internet to work. The numerical network addresses of the DNS root servers are just one type of predefined number among many.

Q: So IANA controls the operations of the root name servers?

A: No; after selecting an operator, the IANA has always respected the operational authority of that operator. This is how diversity is maintained.

Q: Why has IANA given two servers to VeriSign?

A: This answer needs a little bit of history: When the number of possible letters was increased to 13, IANA asked USC ISI and Network Solutions Inc. to set up additional servers with the intention to move them to suitable operators quickly thereafter. J&K were set up at Network Solutions on the US east coast, L&M at USC ISI on the west coast. Both K and M moved further east and west respectively soon thereafter. However as time progressed, moving a server became subject of increasingly inconclusive debates. Still IANA succeeded in moving L to ICANN. Some say this worked because ICANN was in the same building as both ISI and the IANA, a physical move was not immediately required and operations could be supported by the people operating B already. ;-) More likely it

succeeded because ICANN at the time was the only organisation about which at least some consensus could be achieved. After that nothing moved anymore and J remained with VeriSign who had acquired Network Solutions.

Q: You mean K got their server from VeriSign?

A: Certainly not. All equipment and software for K was purchased by the RIPE NCC and installed at the London Internet Exchange (LINX). Subsequently the service was transferred to the new K at a new address. This server was operated by the RIPE NCC with local help from the LINX. I know for sure because I piled the boxes into a London taxicab after ferrying them from Amsterdam.

Q: The letter C used to be operated by the now defunct PSInet. What happened?

A: PSINet kept operating C with help from some other root name server operators. In April 2002, the major U.S. assets of PSINet were acquired by Cogent Communications. Those assets included the customer base and all the equipment supporting the network, including the existing C root server. Cogent took over the responsibility of operating C and has since augmented the C root server system.

Q: But isn't it wrong to regard a root name servers as an asset that can be bought?

A: Maybe, but see the questions regarding selection of root name server operators.

Q: Isn't it dangerous to have so many servers concentrated on the US east cost?

A: Root name servers are operated at more than 80 locations in 34 countries, most of them outside the United States of America (December 2004). See below for details.

Q: Isn't it unfair to the rest of the world that the majority of root name server operators are US entities?

A: This is a reflection of Internet history. In the late 1990s the IANA had begun to spread responsibility for root name server operations following the spread of the Internet around the globe. See also the questions regarding selection of root name server operators.

Q: Isn't it operationally dangerous that the majority of root name server operators are US entities?

A: It is not dangerous in an operational sense. The physical servers are located in more than 80 locations in 34 countries all over the planet (December 2004). See below for details on this. The US organisations involved are very diverse. Personally I do not

consider this a pressing problem. See also the questions about root name server operator selection.

Q: Who funds root name server operations?

A: The root name server operators fund root name server operations. The sources for this funding are specific to each operator. There is a high level of diversity in this funding. This diversity is an important way to make the operation of the root name server system stable and lessen its susceptibility to capture. If funding came from a central source, that source could easily introduce flawed common operational policies or even determine the content of the root zone.

For example the RIPE NCC is an association of more than 3500 Internet service providers from more than 90 countries in Europe and surrounding areas. The businesses of our members are dependent on the functioning of the DNS. They fund the operation of k.root-servers.net through their membership fee. We also deploy local instances of k.root-servers.net that serve a well defined local community; that local community bears the part of operational costs directly associated with their local instance.

Other operators have different funding mechanisms ranging from public funds provided by governments to corporate funds provided by corporations whose business directly depends on stable operation of the DNS.

Q: Who controls root name server operations?

A: There is no central authority that controls the operation of all root name servers. Each root name server operator has executive authority over the operation of the servers they operate. Currently no one has executive authority over more than two letters. This diversity is an important element of the root name server system. It makes the system stable and limits its susceptibility to capture. Speaking for the RIPE NCC as operator of k.root-servers.net: we have a membership-elected board of directors overseeing the association. Both the members and the Internet community in our region closely follow our actions. The membership and the board have the statutory means to act decisively should they ever lose confidence in the way we operate.

This organisational framework ensures that sufficient resources and oversight are provided for responsible operation of k.root-servers.net. Local responsibilities and oversight structures of other DNS root name server operators are obviously different; they vary from responsibility to shareholders of corporations whose success depends on the DNS to direct responsibility to the United States government. I can assure you from personal experience that all of the operators without exception strongly feel a moral responsibility to the Internet community as a whole.

Q: So ICANN does not control root name server operations?

A: No. Neither the IANA nor ICANN have any executive authority over the operation of root name servers. The establishment of such authority has been on ICANN's agenda from the start. It is mentioned in various guises in the MoU between ICANN and the US DoC. However none of this has ever been implemented. I do not believe ICANN, or anyone, should have control over the operation of all root name servers. So this goal should be removed from ICANN's agenda.

Q: But don't we need some central authority responsible for root name server operations?

A: For what purpose specifically? And would this authority not become a single point of failure or a mechanism for capture and abuse? Doing this while maintaining the diversity that the current system has in all aspects including operations, funding and oversight will be impossible. Yet this diversity is an essential reason for its success, if not the most important part. I cannot see any need or reason for such a central authority.

Q: But who do we hold responsible if the root name servers fail?

A: See also below for information about realistic failure modes. Should a letter fail in some way or deliver unacceptable service, the operator of that letter should be held responsible. Creating a central authority to hold responsible will require that this authority has authority (sic) over the operation of the root name servers. It is unlikely that a reasonable entity would accept any responsibility without such authority. Such an authority would introduce a single point of failure and a prominent target for attack and attempts at capture. These side effects are too grave to accept just for creating a convenient target for blame assignment.

Q: But how can governments hold root server operators accountable in the public interest?

A: Now this is an interesting question! There is ample time to study that question because the root name servers have been working well since deployment of the DNS and they are working well at the moment too. There is no need to jump to conclusions and come up with the wrong answers to this question. Read on for some more things to consider.

Q: What are the motivations for root name server operators to provide good service?

A: These are diverse too. The RIPE NCC does it primarily on behalf of our 3500+ members, mostly Internet service providers. The businesses of all our members depend on the Internet and a working DNS. They realise that a root name server is best operated

by a neutral and professional organisation like the RIPE NCC. The member's wishes are the decisive motivation in an association. Other operator's motivations are different. They often include what one of us has described as "relevance": operating a root name server carries a certain standing in different parts of the Internet community. This has a downside too of course because these days deficiencies in the service, however minor and inconsequential, can quickly cause negative standing. I have to add that all the individuals I have worked with in this area are motivated by a strong sense of duty towards the Internet community at large. I believe that this sense of duty is also shared by their organisations.

Q: So what prevents root name server operators from just stopping to provide service?

A: The answer is a combination of the previous couple of answers. In short: The organisations have accepted the responsibility and are stuck with the job. They have the means and the local oversight necessary. Stopping would mean de-stabilising the DNS and the Internet; the potential bad publicity associated with that alone is a big pressure. Also look at the track record of the system. It has never stopped working so far.

Q: So what if a letter stops operation, intentionally or not?

A: The load will be absorbed by the remaining letters and Internet users will not notice at all.

Q: What will happen if half of the letters will stop answering queries?

A: The load will be absorbed by the remaining letters and Internet users will not notice at all. However the operational "headroom" to absorb significant load increases, whatever their cause, will be reduced.

Q: Have more than half of the letters failed before?

A: Many reports about a DDoS attack in October 2002 say that more than half of the root name servers were rendered unavailable for as much as an hour by the attack. Yet the reports do not agree about which of the servers were affected because it depends from where in the Internet you measure. Reports tend to list 'distant' servers as unavailable and 'close-by' servers as available. See the questions about monitoring for an explanation. All reports agree that the the attack caused no disruption of DNS service.

Q: Yes but what if there is a software bug?

A: There is significant software diversity across the root name servers. There are at least four major DNS implementations being used: bind8, bind9, NSD and a proprietary implementation by Verisign. The servers also run on very diverse hardware and

operating system platforms. Actually maintaining this diversity is a major part of the coordination going on between root name server operators.

Q: So root name server operators coordinate to be diverse?

A: Yes indeed. To preserve diversity on all levels, root name server operators are careful not to coordinate anything that does not absolutely have to be coordinated. There is even reluctance to share details about operating practices because that could lead to unwanted similarities in them. Also there is really no need for operators to know details about the operation of other servers for which they are not responsible.

Q: What if all root name serves would stop answering queries?

A: Now you are stretching it. How likely is that? The diversity in the system will prevent that from happening. But let's treat it as a hypothetical case: In that hypothetical case the Internet will not suddenly grind to a halt. If absolutely nothing is done to correct the situation every hour about 2% of all queries will not be answered, 2% at the end of the first hour, 4% at the end of the second hour and so forth until 48h after the root name servers stop answering queries no DNS names can be resolved anymore. However it is even more hypothetical to assume that nothing will be done to correct this hypothetical situation.

Even in the hypothetically hypothetical case that the root name server operators would do nothing to correct the situation, the IANA, TLD operators, ISPs and others would have the motivation and the means to take corrective action.

Again: this is very hypothetical. DNS failures outside the root name servers are much more likely. Name service for the vast majority of top-level domains is very much less redundant than that of the root name servers. Whole top-level domains and major corporations have been unreachable for significant amounts of time because of DNS failures. Name service for the root zone has always been available.

Q: What are realistic scenarios for root name service degradation then?

A: The main concern are denial of service attacks or just plain increased load. The monthly average load of all root name servers is around 90000 queries per *second* (December 2004) with regular peaks at several times the average which are handled gracefully. This is more than 8 *billion* (8x10^9) queries on *average* every day. I would be interested to hear about database or web applications that receive a similar query rate. These days load induced service degradations are more likely caused by network problems than by overload of the servers themselves:

servers continue to answer all queries that get to them but not all queries may get there. Serious DDoS attacks can overload parts of the network infrastructure.

Q: This figure seems much too high, why is that?

A: Indeed the expected load from well behaved root name server clients is much lower. For each TLD they should only need to query the root name servers about once every 48 hours. In practice the majority of the present load is coming from misconfigured or broken DNS clients. There are also regular deliberate attacks on the root name servers. Since the root name server operators cannot decide which queries are 'valid' they have little choice but to answer all queries. The capacity of the system has to be designed to meet the load, whether the queries are 'valid' or not.

Q: Why can't the root name server operators just drop invalid queries?

A: It is impossible to decide clearly what valid queries are. Making assumptions leads down a very slippery slope ending in preferring queries from your friends. The root name server operators do not want to come near this slippery slope. Dropping queries at the server would not solve the problem of the network load these queries cause. Finally it turns out to be easier just to answer all queries than to spend resources trying to decide which ones to drop.

Q: How do the root name operators meet the load challenge?

A: The traditional way is to constantly upgrade both the servers themselves and their network connectivity. The K server at the LINX is currently on the fourth total replacement of hardware since 1997. Its connectivity has increased similarly. Another way of dealing with load is to use anycasting; six letters are currently anycasted.

Q: Can you explain anycasting please?

A: Having sufficient network capacity to reach the servers is a big concern under high load. One way to address this is to shorten the distance between clients and servers by distributing the servers in the network. This way queries and responses have to travel shorter distances and thus use less network resources. Potential congestion near relatively few busy servers is spread out and more servers can be effectively deployed.

The number of addresses at which root name service is provided is limited to 13 by the current DNS protocol. In order to deploy servers at additional locations one has to re-use the addresses. This is done by announcing network routes, note different spelling and meaning from roots, towards the same address from all places where servers are deployed; the routing system then takes care of

selecting which server receives the traffic; generally this is the one closest to the client in the network topology.

Anycasting is not free, additional server instances have to be deployed and operated reliably at remote locations; management and monitoring becomes significantly more involved and expensive. Service problems are harder to diagnose because a problem has to be traced to a specific instance and often the root (pun intended) cause of a problem is in packet routing rather than operation of the server itself.

Using anycast the number of operational server locations has grown from 13 in 4 countries (2002) to more than 80 in 34 countries (December 2004). This has made the root name server system much more resilient to denial of service attacks and has also improved service quality in many regions.

Q: Is there a hierarchy or dependency between the different anycast instances of a letter?

A: No there is not. If one of them fails the others will continue to operate. The remaining instances will provide service to the clients of the failed instance whenever Internet routing has changed accordingly. Until this happens these clients will be served by other letters.

Q: So there is no "main" server for an anycasted letter?

A: No there is not. Arranging things this way would mean to introduce an unnecessary single point of failure.

Q: But surely some anycast instances are more important than others?

A: That depends on your definition of "important". An anycast instance mainly serving a local community can be very important to that community but is of little importance to the rest of the Internet. An anycast instance serving a larger geographical area could be regarded as more important, but with the addition of further instances its relative "importance" is bound to decline.

Q: Isn't it worrying that the root name operators introduced anycasting without approval from the IANA or ICANN or ....?

A: Not it is not. Each operator is responsible for the operation of its letter. No one else has authority or responsibility for the way in which the service is operated. The introduction of anycasting has been approved by the local oversight mechanism of all operators that use it. This step has also been widely announced and discussed in the appropriate fora. For instance the Root Server System Advisory Committee of ICANN has been informed at all times.

In fact diversity pays here again, because I personally doubt that anycast instances would be deployed at this time if a central oversight authority would have had to sign off on it. Take, for example the process and the time it took the IANA to approve something as simple as the introduction of IPv6 glue in TLD delegations. Extending these process requirements to something as complex as anycasting would mean much longer delays. This is not necessarily the fault of the central authority. Requirements for due process and diligence have to be high because errors in the actions of a central authority affect the whole system. A diverse system with distributed authority can react more flexibly with less risk and thus less process involved.

Q: If anycasting makes it possible to deploy multiple servers at the same address, why not operate 100s of servers or have anyone deploy their own root name server?

A: Technically this is possible, but operationally this is a nightmare. Suppose you would get a wrong answer for where the .org name servers were and consequently when going to http://www.isoc.org/ you would end up seeing some very objectionable material. How could you or your ISP ever diagnose where the wrong answer came from if there are 1000s of servers operated by 100s of organisations? It would be impossible to make sure that all those servers have up-to-date authentic copies of the root zone file.

Q: But what prevents anyone from simply setting up their own server at the address of one of the letters?

A: In principle nothing more than what prevents anyone from hijacking any address space. In practice however the routes to the service addresses of the root name servers receive a high degree of attention in ISPs routing systems and any impostor is bound to be caught quickly. All root name server operators which use anycasting deploy only anycast instances that remain under their full administrative and operational control. Operators jealously defend their exclusive right to determine who can introduce routes towards the service addresses.

Q: Who sets standards for root name server operations?

A: The IETF has published several RFCs setting minimum standards. Root name server operators set additional standards for the operation of their particular letter.

Q: Who monitors root name server operation?

A: A lot of people do. First of all the root name server operators themselves monitor the performance of the service they provide, both individually for their letter and often also for other letters. But there are quite a number of other efforts of all shapes and sizes that monitor availability and correctness of root name service. Allow me to mention one of them close to my heart:

http://dnsmon.ripe.net. There are others, like those mentioned in http://www.caida.org/outreach/papers/2004/dnspam/ and more can be found using your favourite Internet search engine.

Q: But the root name server operators could surely modify the file if they wished?

A: Currently this is technically true. But each root name server operator could manipulate only the information provided by the servers for the letter they are responsible for. This would affect only a fraction of all queries. In order to make such manipulations effective the vast majority of the operators would have to conspire. Given the organisational diversity that exists, this is extremely unlikely to occur. Again diversity turns out to be an essential part of the system. Whenever DNSSEC is widely deployed such manipulations become practically impossible.

Q: What is this DNSSEC?

A: DNSSEC (DNS Security) is a DNS protocol enhancement. It allows zone administrators such as the IANA to sign their zone files using public key cryptography. DNS users can then use these signatures to verify that the information they receive from DNS servers such as the root name servers is indeed authentic. This prevents manipulation of the data during storage on servers and during transmission.

Q; That sounds great, when will DNSSEC be available?

A: Unfortunately not for some time because deployment of this technology requires not only changes of software in all Internet hosts that want to benefit, but also changes of business practices and operational procedures throughout the DNS including registries, registrars and holders of domain names. A detailed explanation of this would be too long to place here. I estimate at least 3-4 years before DNSSEC has spread far enough to become really effective on a global scale. That does not mean everyone should wait and do nothing because then it will take much longer.

Q: Wouldn't DNSSEC make it feasible to have 100s of root name servers?

A: In principle yes. Since each client can check the validity of the data such a scenario is more feasible with DNSSEC. There are issues like ensuring that updates do propagate and servers do not serve stale data. But once DNSSEC is indeed widely deployed I expect the DNS to develop in this direction. The current root name servers could then move to the role of providing a basic level of service which could be augmented by others. There will be details I have not thought about yet, but in principle this is a possible and even likely scenario. It adds diversity while ensuring consistency; that is the Internet way. However, as pointed out earlier, this is not feasible without DNSSEC and even with DNSSEC there are issues to

resolve like monitoring, responsibilities and localising service problems.

Q: But that would make the root name servers much less important?

A: Yes and that is a good thing.

Q: OK, but let's assume that before we have DNSSEC one of the root name server operators decides to "go rogue" and change the root zone file. Let's say their government forces them to do so or terrorists threaten to blow up their favorite new workstation.

A: Any changes would be detected relatively quickly by the various monitoring efforts. If the root name server operator would not correct this there are ways to significantly limit the impact of it by preventing queries from reaching the affected servers. This would require a concerted effort by many parts of the Internet community, mainly the ISPs. I expect that it could be done if necessary. If this was easy to do however it would be a danger in itself. It requires the concerted effort of many players.

Q: The majority of the root name server operators are based in the United States of America. Couldn't the US government force them to make any changes it wants?

A: In principle I suppose the US government could do that. It is difficult to argue with one's government if the government is determined about something. However I consider this a highly unlikely scenario for several reasons of which I will just give the ones I find most convincing:

Firstly, any unilateral action like this, even by the US government, would mean that the DNS namespace fragments at that very instance. Other governments will decide that they do not like the changes imposed by the US and as a consequence some names will either not be visible everywhere on the Internet anymore or, worse, they may start to mean different things. In this situation everyone loses. So as long as all players remain rational, they will not go in this direction. But then there is the story of the goose that laid the golden egg.

Secondly, it would be much easier for the US government to influence the editing process by the IANA. This method would even keep working after deployment of DNSSEC while forcing root name server operators will not work with DNSSEC.

Q: What is it about that goose?

A: I am sure variants of this story exist all over the world. Here it goes: A man and his wife owned a very special goose. Every day the goose would lay a golden egg, which made the couple very rich.

"Just think," said the man, "if we could have all the golden eggs that are inside the goose, we could be richer much faster." "You're right," said his wife, "we wouldn't have to wait for the goose to lay her egg every day." So, the couple killed the goose and cut her open, only to find that she was just like every other goose. She had no golden eggs inside of her at all, and they had no more golden eggs.

Q: Isn't this whole system just built on (personal) trust of the operators?

A: It used to be, like much of the early Internet deployment was built on personal trust, even in the first years of commercialisation of the net. This is no longer the case. Root name server operators are reliable organisations with strong and diverse local oversight mechanisms and strong but diverse motivations to provide good service.

Q: Is the letter A special in any way?

A: No it is just one of the letters. All DNS root name servers are equally authoritative for the root zone. In the past the zone file was distributed to the other operators from this server. This was recognized as a prominent single point of failure many years ago. The distribution of the zone file was changed accordingly. Currently, due to deficiencies in some DNS implementations, A and B receive a slightly higher number of queries than the other letters.

Q: How is the root zone file distributed then?

A: After being produced by the IANA according to the process described on the IANA web page the file is stored on a number of distribution servers. These are often called hidden servers, as their Internet addresses and locations are not published in order to make them less susceptible to malicious attacks. The root name server operators fetch the file from these servers in a secure fashion. Each operator then distributes the file to the servers they operate in a manner they choose.

Q: What if the distribution servers fail?

A: There are a number of them, so total failure is unlikely. Also the zone file is a rather small file; it was 119KB in December 2004. This is less than the information your web browser needs to transfer to display the home page of ISOC at http://www.isoc.org. There is a lot of syntactic redundancy in the root zone file; compressed it is only about 20KB. The file does not change all that often; between 11-Nov-2004 and 12-Dec-2004 it changed only seven times and in the 12 months prior to 12-Dec-2004 it changed exactly 90 times. The individual changes are all localized and relatively small.

The timing of changes is also not very critical. DNS is designed and configured such that a typical root zone change will take two days

to fully propagate through all of the DNS. The editing process itself currently takes at least as long as that. So TLD operators tend not to rely on instant distribution of changes. ;-) Conceivably the root zone file could be distributed by any means: e-mail, telephone, sealed envelopes sent by courier are but a few of the alternatives. The important bit is for each operator to verify that the file they obtain is indeed from the IANA.

All this means that in case of distribution server failure there is ample time to switch to alternative means should the distribution servers remain unavailable. There is also ample time to make sure that any change messages are indeed authentic. So this is definitely not a problem.

Q: But isn't the IANA a single point of failure in the system?

A: To some extent it is. In any hierarchical naming system someone has to be in charge of maintaining the apex. There is no way around that. However this is not a very time critical function and the Internet will continue to work for months should the IANA fail to update the file. Some TLD administrators will be inconvenienced substantially but there are sufficient ways to keep up TLD service in the absence of changes by IANA.

Q: What are your most frightening nightmares related to operation of k.root-servers.net?

A: What gives me sleepless nights is not that k.root-servers.net will fail, embarrassing as that may be. The remaining root name servers will absorb the load without any Internet user noticing at all. The real nightmare is that there may be a common flaw in all DNS root name servers that will make them all fail, succumb to an attack or be captured at the same time. Such a failure is highly unlikely though because of the high level of diversity the root name server operators strive to maintain in the system. Adding a central point of authority for the operation of all server, as some suggest, would create new bad scenarios to worry about, not all of them technical in nature.

Q: So why are those root name servers so interesting?

A: I do not really know. It probably is because they serve the data that is the apex of a hierarchical naming system. There are extremely few things in the Internet that are organised along a clear hierarchy. One of the principles underlying Internet engineering is to distribute all functions as much as possible and to encourage diversity in implementation. This way the Internet grows much faster and is much more reliable than any centrally or hierarchically organised network can be. This is an essential part of the success of the Internet.

The DNS name space is one notable exception to this rule: it is hierarchical; so there needs to be global agreement on which TLDs

go into the top level and who is managing them. This is an area that obviously needs a globally agreed process.

The root name servers just publish this data that this process produces; yet they are still regarded as unique and valuable because they are often identified with control about the data they publish. Fortunately in reality there is also a lot of diversity in the root name server system which provides operational redundancy and resilience to capture.

In my opinion the same diversity makes it impossible for the current root name server operators to ever conspire strongly enough to really control the content of the root zone. But you have to form your own opinion.

When I am in a cynical mood I say that the root name servers are an object of the "Internet Governance" debate only because a hierarchy is the natural system "governors" think in. Distributed systems and distributed responsibility is much more difficult to govern and thus somewhat uncomfortable to "governors". However such distributed systems make the Internet work and be successful. Changing to a hierarchical mode just for the convenience of "Internet Governance" seems like a seriously wrong approach to me. I strongly believe that "Internet Governance" needs to follow the distributed approach of the Internet itself.

Certainly the debate about root name servers also serves (pun intended) to distract from the much more important debate about the process by which the content of the root zone file is determined.

Q: What can governments do to help?

A0: These are my personal opinions. I hope my reasons for arriving at those opinions are consistent with the more factual answers above. You should find all the motivations for these answers below in the answers above.

A1: Make sure that there is an agreed process for editing the root zone file. The second most frightening nightmare for any root name server operator is that one day there will be two ore more credible editors that offer their zone file for publication. Note that I am not saying that any government or governments should specify that process unilaterally. Governments, together with others, should take active part in establishing consensus about the editing process and the editor. Of course when it comes to implementation it would be appropriate to ask the root name server operators if a particular implementation of a process is feasible. In this context it is important to realise that in the future the editing process will involve signing the zone information cryptographically. So some attention to who holds the various cryptographic keys involved is necessary when designing editing procedures.

A2: Governments should vigorously prosecute the perpetrators of denial-of-service attacks on the Internet and encourage ISPs to take appropriate action to mitigate such attacks. I observe that simple steps that would significantly mitigate DoS attacks, like verifying IP source addresses at the edge of the network, are not taken by ISPs because there is no direct benefit to the ISP unless every ISP does this. In other words no ISP wants to bear the associated cost first while others profit and do not incur the cost. There is clearly an area for government action here.

A3: Refrain from adding features to the governance processes that unnecessarily reduce diversity in Internet operations and responsibilities. Diversity is an essential part of the Internet architecture. Supplanting distributed systems with hierarchical structures for the sake of convenient "governance" is a very dangerous thing to do.

A4: Help to achieve global consensus on the way that root name server operators are selected should the need arise. When doing that, avoid associating any operational authority with this process. Also strive to prevent a mechanism that reduces diversity by repeatedly choosing favourites of one particular group (aka 'seeding the high court'). In my opinion the question of how to move a root name server operator should be addressed *after* this consensus has been achieved.