ABU DHABI – How It Works: Internet Networking
Monday, October 30, 2017 – 13:30 to 15:00 GST
ICANN60 | Abu Dhabi, United Arab Emirates

STEVE CONTE: All right. I appreciate everyone coming and/or staying. This next session is a tutorial on the Root Server System. We have members from RSSAC here and we'll have some root server operators. We already have a couple in the room here who can answer any questions at the end of the session. We are going to do this in two parts and then we'll take questions at the end. So if you have any questions, there are some notepads right in front of you. Please note it down and we'll have the questions and we'll have some root server operators available who could answer and address the questions, too.

So, with that, I'm going to introduce you to Andrew McConaughey. Is that right?

ANDREW MCCONACHIE: McConachie.

STEVE CONTE: McConachie. So close. Every time.

ANDREW MCCONACHIE: Good enough.

STEVE CONTE: He's ICANN staff. He works with and supports the Root Server System Advisory Committee and I'm going to pass that on and I think that he'll pass it on to Steve Sheng at some point, too.

ANDREW MCCONACHIE: Yeah.

STEVE CONTE: Thank you.

ANDREW MCCONACHIE: Thanks, Steve. So, I'm Andrew McConachie. I work for ICANN and I support the RSSAC and I'm here giving this presentation on behalf of the RSSAC. It's going to go in two parts, as Steve mentioned. I'm going to go over the overview of the Domain Name System and then the Root Server System today and its features, kind of an update on what's going on with the Root Server System today. And then I'm going to hand it over to my colleague, Steve, who's going to give you an explanation of Anycast and some of the recent activities of RSSAC. And then in the end, we'll have time for questions to the root server operators.

So, first, a quick overview of the Domain Name System and root servers. If you have a bit of a technical background, this is going to be a bit of a review. If you don't have much of a technical background, this should be relatively new, but hopefully you can pick it up as I go.

So, first off, a bit of a recap. Identifiers on the Internet and IP addresses. IP addresses are the fundamental identifier in the Internet. They're a numerical label, which will become more important when we get into DNS and why we need DNS and how that relates to IP addresses. All hosts connected to the Internet do have IP addresses; they need them. And, of course, there are two kinds, two flavors, IPv4 and IPv6, IPv6 being the newer flavor. And if you, I guess if you were here for the previous discussion from Alain Durand, you know all about those two, so I'm not spending any time on that.

So, why DNS? Originally, we had this need for DNS, which is that IP addresses are hard to remember and that they change a lot. So, that was back in the '80s when DNS was being conceived, we had this need because people don't like remembering numbers, especially when they're four numbers separated by dots, kind of hard to remember. And they change a lot. I mean, some of them are static, some of them stay static for a long time. Other times, you have DHCP and whatnot, so they change.

The new problem, and this is the more modern problem, is that we have this kind of one-to-many and many-to-one problem where IP addresses may be shared, so you might have multiple devices that have a single IP address. Maybe they're behind a NAT or a CGNAT or whatnot. And then we also have multiple IP addresses may serve as entry points to a single service, so that's the many-to-one side of that problem. And we'll talk about Anycast later.

Okay. Here's something on the Domain Name System. This is about the data in DNS. DNS is a hierarchical structure. You could call it a database or it has a hierarchical layout. There's a root at the top and there's only one of those. And then if you spend any time at ICANN whatsoever, you've probably heard the term top-level domain, so here we have .edu and .mil and .uk. And then, of course, second-level domain, third-level domain. There's really no limit to the number of or the depth of this hierarchy and how deep it can go.

And DNS serves an important function of mapping these types of names to IP addresses. In addition, there's also things for mail servers like MX records, IPv6, the AAAA records, and, of course, reverse mappings where you go from IP address to domain name.

This is a pretty complex slide. There's a lot going on here, so I'm going to spend some time kind of walk through it. And it reads from right to left, which works because we're in an Arabic-speaking country. Normally I'm like this slide's backwards but luckily, people here read right to left, so it actually kind of works here. And over here, we're going to start over here with the person and this person is at a computer and they really want to go to example.com because they've got a great Website. What they're going to do first is they need to figure out the IP address of example.com. We're just going to walk through the resolution process for that.

The first thing is a query goes to what we call a recursive server and you send the query to the recursive server with a bit set that says don't send me anything until you figure out everything. Just go do all the resolution for this and then just send me back an IP address. I don't want to hear about the intermediary steps. Then the recursive server has to do a bunch of intermediary steps before it can send back an IP address.

We're assuming here that this recursive server has just been turned on, its cache is completely empty, and it basically knows nothing except for the address of the root servers. The first thing it's going to do, it's going to go to a root server and it's going to say, "I need the nameservers for .com." And then it's going to learn those and then it's going to go to the nameservers for .com

and it's going to say I need the nameserver for example.com. Then it's going to go to example.com and it's going to say, "I need the address for www.example.com." And only at that point is it going to go back to the user with an IP address and then the user can access that Webpage.

The key here or the two key things here, I guess, is that root servers only need to know the nameservers of the next lowest zone or the next lowest domain, so the TLDs. And then the recursive server will then go off and ask the nameservers for that TLD where to get to the second-level domain.

The other key thing here, which I mentioned kind of briefly is that in the previous example, we had this thing completely stupid. It had just turned on, its cache was empty, it had no information, so it had to start from scratch. And so it had to go to a root server to figure out the nameserver for .com. This almost never happens. Recursive server operators don't reboot their recursive servers between queries, so the cache tends to fill up rather quickly and it tends to get used a lot. So the vast majority of queries use the cache, and by doing so, recursive servers rarely have to go to a root server at all.

These are some modern refinements to DNS. You probably heard a bit about DNSSEC, the security extensions for DNS. There are kind of two parts to DNSSEC. By putting cryptographic

signatures on DNS data, the authoritative side, so the DNS server that is responding to queries, can sign the DNS data. And then in the recursive server what happens is there's a validation process. So the recursive server can validate that and make sure that it's the correct DNS data. So there's kind of a signing and a validation side to DNSSEC.

Privacy enhancements, there are two things to talk about here. I'm going to talk about two things which aren't really in production yet, but the IETF is working on them. The first one is DNS over TLS, which if you're familiar with TLS maybe from HTTPS, it basically creates an encrypted channel for the data to flow through, so it's like a generic encrypted channel. The idea with DNS over TLS is, the IETF is still working on it, but the general idea is that DNS traffic, the queries and the responses, will go over TLS and be encrypted on the wire.

The other thing to talk about here, which is up and coming, is something called QNAME minimization, which basically stops the recursive server from sending the whole query of www.example.com to the root server and the only thing the root server will see will be .com. And so that just [presents] less information on the wire.

The third thing here, and my colleague Steve will explain a lot more about Anycast in a minute. Anycast is in wide use by all the

root server operators and it does two things. You can think of Anycast as really doing two important things. First thing is it improves latency and resilience because you can have a server fail and there's always going to be another one around at the same address, so that's pretty handy. And it also puts the servers closer to the person doing the query. And the second thing that Anycast does, which is really important, is it protects against DDoS attacks. You have a DDoS attack, the server nearest the DDoSer will absorb the attack and other servers won't be so affected.

Now, this is kind of comparing and contrasting the root zone versus the root servers. The root zone is data, and the root servers are about serving that data. The root zone, in terms of the hierarchy that we pointed out earlier, it's a starting point. It's a list of the TLDs and their nameservers. It's managed by ICANN per community policy. It's compiled and distributed [by a] root zone maintainer and it's basically database content of the root servers. It's what they're serving.

The root servers, they respond to queries with responses from data from the root zone. Right? So they hold the root zone and they respond to queries on that. And then we have there are 13 identities for root servers and there are over 800 instances at physical locations worldwide, and the 13 identities are [a-

m].root-servers.net. Those are their names. And the root servers is a purely technical role to serve the root zone.

The root server operators consist of 12 different professional engineering groups that are really focused on reliability, stability, and accessibility for all Internet users. There's lots of technical cooperation between them. And it's a diverse group of organizations and that diversity extends both technically, so they'll use like different operating systems, different application software. There's technical diversity there. They're also organizationally diverse, so there are different types of organizations that are doing this, and they're geographically diverse.

Things that operators are not involved in. They are not involved in policymaking. They're also not involved in data modification of the root zone. They just answer queries. Operators are involved in careful operational evolution of service, so that means changing as things change, evaluating and deploying suggested technical modifications, and making every effort to ensure stability, robustness, and reachability.

So that was a bit of a background on DNS and a bit of a background on the root server system. Now we're going to talk about some root server systems today and some features, so it's a bit more kind of a modern update. Here's a bit of a history. You

can see in the ‘80s, it started out with four addresses. Nowadays, it’s up to about 13. Or no, excuse me, in 1998, it was at 13. Nowadays, it’s 26 because IPv6 was introduced.

And it is served from still 800 international instances. Those instances are spread around the world. I think last time this presentation was given, there were 600-plus instances, so it was – I don’t remember but the last time this presentation was given, there was 600 instances. Now there’s like 800, so we have to update that number every time we do the presentation. It keeps growing.

Here are some foundation principles of the root server system. Stability, reliability, resiliency. It operates for the common good of the Internet. And the IANA is the source of all DNS root data. They all serve the same root and it’s all coming from IANA. Architectural changes have been made so there’s some technical valuation and demonstrated technical need. And the expectations of the DNS are defined by the IETF, so the standards of how DNS works as well as the expectations of the DNS are defined by the Internet Engineering Task Force.

If you want to know a whole lot more about the history of the root server system, check out RSSAC024. It’s a document on the RSSAC Website. It’s pretty extensive. There’s a lot of good

information about the history of the root server system and why it looks like it does today.

These are these identities with their 26 addresses I was talking about. You can see in the first column you have [a-m].root-servers.net. And then here you have the 26 addresses in the second column. And on the left side of the second column, you got the IPv4, and then on the right side of the second column, you've got the IPv6, and they've all got both. And then on the third column, you can see the operator for each one of these identities.

Here's a slide from this Website. This is a really good website if you want to learn more about the root servers, root-servers.org. Again, over 800 instances around the world. And be careful when you're looking at this map because I mean it doesn't really mean that there's like 23 exactly right there. It's basically just an artifact of the software that's used to create the map and it makes these nice little bubbles of numbers around there, but they're spread all over the place. But if you go to this Website, you can look at where each one of the identities has servers and then see what cities they're in exactly.

This is another complex diagram, complex slide, so I'll spend a bit of time on it. Basically, it's kind of like a flow diagram, so I'm going to start over here. You can imagine you were a TLD

operator and you had a change that you wanted to make. So let's say you're a TLD operator and your nameserver changed for your zone. What you do is you contact IANA and you say hey, these are the new servers for my zone. Please update the root zone. IANA will make that and then they'll push it to the root zone maintainer, and the root zone maintainer kind of compiles it all and DNSSEC signs it, of course, where necessary. And then they distribute it to all the different identities and then they push it to all the instances.

And then over here, we've got the recursive resolvers issuing queries and the responses. And on the top of this, you see how there's like this squiggly line here. The squiggly line is kind of like a separation between the provisioning of the system or the provisioning of the root zone and the resolution of the root zone. You see at the very top, you've got the RZERC dealing with the provisioning in the ICANN world and then the RSSAC dealing with the resolution in the ICANN world.

Some of the features of root server operators. We talked earlier about diversity. Diversity of organization, organizational structure, as well as what types of organizations they are. Diversity of operational history, so they all have different histories. We talked about technical diversity with hardware and software, so different types of operating systems, different types of applications. Well, the same types of operating systems and

applications but say maybe somebody's using FreeBSD and somebody is using Linux so that if there's a bug in one, you won't find it in the other one. And different funding models.

But they do have shared best practices. So within that diversity, there's still a best practice of like good physical system security or the overprovisioning to deal with things like DDoS attacks and spikes in query rates and a professional and trusted staff.

The root server operators cooperate through a lot of industry meetings at these organizations like ICANN, IETF, the various NOGs, and they use Internet-based collaboration tools and they try to be, they're pretty transparent. There's a lot of coordination, as well, with infrastructure to respond to potential emergencies where they need to get in touch with one another and there's some kind of potential emergency. So they maintain phone bridges, mailing lists, and swapping of secure credentials. And they also have periodic activities to support this, to support activities in case they arise.

And as the Internet evolves, new requirements are put on the DNS system. We talked a little bit about DNSSEC and IPv6, so all root server operators now support IPv6. DNSSEC, of course, increases query responses. It increases size a little bit, so that's also something for people to think about. And increased robustness, responsiveness, and resilience. This number, this

800-plus keeps growing through Anycast to just ensure that this service is always available.

These are some myths as well as the realities. On the left-hand column, you have some kind of a mistaken assumption about what people might think about the RSOs and then on the right-hand side, you have the reality, so I'll just go through them.

Root servers do not control where Internet traffic goes. That's routers. Most DNS queries are handled by a root server. That's not true. Remember when I talked about caching and the influence of caching on the amount of queries that actually leave a recursive resolver is pretty immense. The vast majority of queries never leave a recursive resolver or at least don't get to a root server because the addresses of the root servers will be cached in the recursive.

Administration of the root zone and service provision are the same thing. That's not true. Administration of the root zone is separate from service provision. Remember when I talked about that squiggly line, and one side you had provision and on the other side you had resolution.

The root server identities do not have special meaning. There's no special meaning between A through M. There are only 13 root servers. Right now, there's over 800 and the number keeps growing. But there are only 13 technical identities. The root

server operators do collaborate and work together to ensure the service stays up.

This bottom one is an interesting one. I put a star here to remind myself to talk a little bit about QNAME minimization because the myth is that the root server operators only receive the TLD portion of a query. That myth is currently not true, it's still a myth but it might change in the future probably after a long time, not anytime soon. But at some point, that might actually change.

And now I'm going to turn it over to my colleague, Steve Sheng, who's going to give you the last half of this presentation.

STEVE SHENG: Thank you, Andrew. As Andrew mentioned, there are over 800 international instances of the root servers and they use a technology called Anycast, so I'm going to give an explanation of this Anycast technology. First, some distinction between Anycast versus Unicast. Unicast packets from sources all go to the same destination. So you can have multiple sources, but the packets all go to the same destination. And a single instance serves all the sources. The flipside of that means under a denial-of-service attack, all the attack traffic goes to that instance. So that's Unicast.

The difference from Anycast is that multiple instances serve the same data to all sources. Let me repeat that again. In an Anycast scenario, multiple instances serve the same data to all sources. So, for example, for the root servers, you have all these 800 instances serve the same data, which the root zone to all the sources. And the sources use destination-based through a routing policy and they get to the data faster and that has impact for denial-of-service attacks.

Let me illustrate that. This is a Unicast situation. This is a destination, single destination. You have one source there but you can have multiple sources, but all the sources go to that destination, single destination, and the traffic usually takes the shortest route there. So that's Unicast.

Anycast here is where you have multiple sources here. They're all advertising the same. They're all saying I offer this service. Please route the nearest traffic to me. And then the routing policy determines the destination from the source. So if the source is here, then the closest destination is here.

What this impacts is this increases resiliency because during a denial-of-service attack, the attacker here sends the attack traffic. And because of Anycast and the routing, they're routed to the nearest destination. So although this destination is flooded, these destinations continue to operate and serve. This overall

increases the resiliency. Also, it means having these destinations closer to the sources, it reduces the roundtrip time for the responses, so it both reduces the time and it increases the resiliency.

If you are a network operator and you're thinking what's the relationship of the root server system to your networks, here are a few things you can do. First of all, you want to have three or four nearby instances. As Andrew mentioned earlier, we have about over 800 international instances. You want to have three or four nearby instances.

Second, having an instance near you does not solve all the problems. You also you need to make good peering arrangements. Sometimes you have an instance near you but the traffic still goes across the world to a different server because of peering arrangements. So you want to increase the peering connections and you may also consider hosted root server instance in your network.

The second thing you could do is to deploy – this is a new IETF technology – 7706, which is to reduce the time to access a root server by running one on a loopback address. So essentially, for example, you might have a need to reduce the latency or for some privacy considerations, you do not want to review what data you send to querying the root service. So you can deploy

one running on the loopback. That increases the caching. So that's another consideration you can do.

If you can convince your recursive resolvers to turn on DNSSEC validation, that ensures you can validate the data you're receiving from the root service is on modified IANA data because of the signature.

And finally, you can participate and contribute to the RSSAC Caucus, which is a body of experts that are developing documents, making recommendations on how to improve the service, how to improve its resiliency, and other documents. So that's one area where we need input from experts around the world in addition to the root server experts.

Now I'm going to talk briefly about RSSAC. RSSAC stands for the Root Server System Advisory Committee. This is a committee in ICANN [land] that exists to advise the ICANN community and the Board on matters relating to the operation, administration, security, and integrity of the Internet Root Server System. It's a very narrow scope and focus on the Root Server System compared with other advisory committees and supporting organizations within ICANN.

The RSSAC is producing advice primarily to advise the Board and the community on matters relating to root servers. But there's another part. It does not involve itself in the operation of the

actual root servers. Looking at the ICANN community map, and that's where RSSAC is, there are three supporting organizations and four advisory committees, and RSSAC is one of those four advisory committees.

RSSAC is composed of the operators, appointed representatives, and also alternates. In addition, it has liaisons, for example, with the root zone management partners and with other technical bodies. The RSSAC also has a caucus. This is a body of subject matter experts, which they're confirmed by the RSSAC. You apply to that, went through a process. If confirmed by the RSSAC, you're on the caucus to help to produce documents and to write reports.

The current RSSAC co-chair is Brad Verd from Verisign. Is Brad here? No? And also, Tripti from University of Maryland. Tripti as at the back there. Okay. The liaisons from the RSSAC, we have two types of liaisons, inward-facing liaisons and outward-facing liaisons. So outward-facing liaisons are the liaisons that RSSAC appoints to other organizations. Those are to the ICANN Board, to the Nominating Committee, to the Customer Standing Committee, which is a body formed as a result of the IANA transition to oversee the performance of the PTI, and as Andrew mentioned before, the Root Zone Evolution Review Committee. This is a committee that considers architectural changes for the root zone.

The inward-facing liaisons, we have, as I mentioned, the IANA Functions Operator, which in that diagram that Andrew showed is a member of the root zone management partner. The other one is the root zone maintainer that compiles and DNSSEC signs the zone that distributes it twice a day. Important function. And in addition to that, the Internet Architecture Board and the Security and Stability Advisory Committee.

The RSSAC Caucus currently has 87 members as of October. It has been growing quite a lot lately. Each member has to submit a statement of interest that will be posted in public and for their work, they're given public credit. Every document that is produced by the RSSAC, at the end of that document, you have a list of contributors who actually contribute to the document. Its goal is to enlarge the pool of expertise to provide advice in this area in a transparent manner and with a framework to get work done.

Recently, the RSSAC published several reports. They have two reports on the workshop. The RSSAC has been for two years, maybe three years, have a series of workshops dedicated on the topic of the evolution of the root service. For each workshop, they publish a report. The Caucus has done a technical study analysis on the naming schemes used for individual root servers, and there's also an update to the operational procedures.

There will be a public session tomorrow where some of these documents will be explained in detail, so you're invited to come. I think that's 2:00 or 3:00. Currently, the Caucus is working on best practices for the distribution of Anycast instances for the root nameservers. What's the best way to distribute, to place these Anycast instances?

Harmonization of anonymization procedures for data collection. The root servers provide data to various venues for reporting and for research and in some countries, due to privacy laws, they have to anonymize some of these data. This work party to look at whether it's desirable to harmonize the practice across various servers for the anonymization procedures. And there's also the packet size in DNS. Again, these will be discussed in detail tomorrow.

Both the Root Server System Advisory Committee and the root server operators constantly aim to improve transparency and they have been making big strides of improvements in that area. So, for example, the RSSAC established a caucus, which is an open body. People can join and the mailing list discussions and the mailing list archives are open. The work is done in a transparent manner. Every RSSAC meeting, the reports, the minutes are published. We have a public RSSAC and caucus calendar. A list of the meetings, what's coming up next. At

ICANN, the RSSAC have public meetings as well with other community groups.

The RSSAC has been giving tutorials on the Root Server System, I think, for four or five meetings, informing the community about how the system works, how the different parts, how to participate, how to ask questions. And they have strengthened the liaison relationships. They have also formalized how they work through their operational procedures.

On the root server operator level, they are publishing the Root-Ops agendas. The Root-Ops meet at IETF meetings and they talk about technical issues and they publish the agendas of those meetings. Every operator now is publishing statistics, what we call in RSSAC002 statistics, just showing how many queries they're receiving. Those are published I think once a day in a query, the spread, IPv4, IPv6, and different responses to those, so those are available. And they are also participating in the RSSAC.

As Andrew mentioned earlier, the root-servers.org, that's a good entry point for you to find information about the Root Server System. You have the map about where these international instances are placed. You can drill down and find out where the RSSAC002 data are being held, and they also publish reports on major events. So, for example, I think it was June, there was a

distributed denial-of-service attack on the Root System, and then the operators get together and publish analysis and reports of these events.

And finally, RSSAC can respond. RSSAC is the front door, so at ICANN, you can ask questions and then those questions will be passed on to the root server operators.

That's the last slide for more information about RSSAC and the Caucus. That's all.

STEVE CONTE: Okay. We're going to start the question-and-answer session. I already have one hand raised.

STEVE SHENG: Yeah. Before you go, Steve, we have root server operators in the room, so they will be the ones, the experts to answer your questions.

STEVE CONTE: Steve, maybe we can play it like we did like yesterday, too.

STEVE SHENG: Sure. Of course.

UNIDENTIFIED MALE: Hi. This is [inaudible] from Pakistan. My question is about the root servers naming conventions. We have A to M. I'm assuming there are 13, so there must be some classification basis for that to divide them into 13 root servers. Is there any difference on what the root server A does and what root server F does? Secondly, I saw most of the operators are in the list that you mentioned of the root servers they are U.S.-based, so is there any particular reason for that?

STEVE SHENG: Thank you. One is about the naming scheme, whether A is different from others, and then, also, U.S.-based operators? Terry?

TERRY MANDERSON: Hi. I'm Terry Manderson. Thank you for your question. The lettering is simply lettering. It gives no insight at all, no priority, no differentiation between any of the root servers at all. So A does exactly the same thing that M does. The other question was U.S.-based. That's a fact of history. All of the operators make efforts to deploy infrastructure around the globe. In the early days of the Internet, the main people who were doing the Internet was the U.S. So it kind of stood to reason that they were the early participants. And it's a fact of history more than anything else.

STEVE CONTE: Terry, has anyone ever run an analysis on how many of the instances are in the U.S. versus out of the U.S. percentage-wise?

TERRY MANDERSON: You can look at the map.

STEVE CONTE: There you go.

UNIDENTIFIED MALE: I'm [inaudible]. You made mention that it's possible to run the root server on the lookback. I want to find out is it like mirroring or how is it done? Is it cloning? Then will the mirror continue to receive an update from the root server. If it's yes, is it manual or is it automatic?

STEVE SHENG: Okay. So I guess the question is about the RFC7706. Any root server [operator] who wants to answer that question? Wes?

WES HARDAKER: Hi. Wes Hardaker from USC. Running 7706 has been possible for a while because all you have to really do is configure your server to actually go pull the zones from one of the servers that actually

support doing XFRs. In fact, ICANN has two servers themselves that allow you to do that transfer. The tricky part for most people and I think the reason that people haven't done it is they don't know how to create that configuration to actually make that happen.

I'm going to be speaking on Wednesday, I think, at the DNSSEC workshop. I have a new project called LocalRoot that actually does that, so it actually allows you to create the configuration you need. It does it sort of automatically for you and then gives it to you and allows you to get notification so that you can do 7706 very, very easily. If you want, you're welcome to go to localroot.isi.edu. I've got to warn you, it's brand new, like alpha-level support at this point, but please do check it out if you want to play. I wouldn't use it in production at this point yet.

STEVE SHENG: Thank you.

STEVE CONTE: Thanks, Wes. We had a question here first and then I have a question here and all over the place. All right. You choose [inaudible].

STEVE SHENG: I'll run the mic. I'll start with you.

HAITHAM ALZAID: Yeah. Haitham Alzaid from STC. My question is I have actually two questions. The first question, what is the secret behind number 13? Why we have only 13 root servers? Second question, is not actually query. I would like to hear more about [inaudible] of DNS protocol. Where are we with this protocol? The RFC is already released or not? Is that mature enough so we could start deploying it for [DNS structure]?

STEVE SHENG: Okay, so the first question why number 13. And your second question is DNS over TLS. Okay. All right.

STEVE CONTE: Duane, you want to take it?

DUANE WESSELS: The answer to why 13 is actually related a little bit to a previous question. I forget exactly how many years ago but many, many, many years ago, the root servers had different names. They were actually named after their organizations and in order to expand the list, it was decided to give them letters in a single zone. And that allows them to use name compression and things like that.

But the 13 really comes from an artificial or a historical limit in the size of a DNS response packet. You may have heard that back in the days, a DNS response couldn't be bigger than about 512 bytes. And so 13 is how many names you can fit into that response size. And that limit is sort of no longer with us but it's a historical artifact.

STEVE SHENG: Second question, DNS over TLS.

DUANE WESSELS: Right. So DNS over TLS – did you want to say more, Terry? Okay. I'll say a little bit. Maybe we'll say the same thing. So DNS over TLS is an Internet RFC. There was a document that describes how to do that. However, it really only describes how to do that between a stub resolver and a recursive nameserver. So there is still more work to be done for the next step, which is between a recursive nameserver and an authoritative nameserver, such as a root nameserver. So it's probably coming but it's not quite done yet. Did you want to say more, Terry?

TERRY MANDERSON: RFC7858?

DUANE WESSELS: RFC7858 is the RFC that describes how to do that between the stub and the recursive.

STEVE SHENG: Quite a few questions, so I'll start with you and you and then here and then back. Okay.

UNIDENTIFIED MALE: [inaudible] from Tunisia. Do you agree with me that RSSAC is more democratic than SSAC looking to the way how member join this advisory committee? Since member are joining RSSAC by simple [inaudible] by rather than SSAC where member are appointed by the Board. And do you think that – I think that we should apply for this technical advisory committee the same model that the user that, for example, at the ALAC, so we may define membership by region in order to have this balance between region. Thank you.

STEVE SHENG: Thank you. That's a kind of an organizational question. As a policy staff, I can actually provide some answers. To join the Security and Stability Advisory Committee, what you also do is you can apply and you send it to the director and there is a membership committee that reviews the application and if it's approved, they make the recommendation to the Board. The

same for RSSAC. You have a membership committee that considers the application for the Caucus.

Regarding your suggestion to appoint membership by geographical regions, I think that's a policy question. These organizations are being reviewed. You can certainly submit that viewpoint to be considered. But I think from our perspective, supporting these communities, it is more important to place a premium on the technical skills than simple geographical representations. That's the experience we have so far. But again, there's opportunities to provide that input to the independent review. Okay. I'll start with you and then [inaudible].

UNIDENTIFIED MALE: This is [inaudible] from Kuwait. My question is related to Anycast. If an organization has to go to deploy Anycast for their DNS servers, how do you go about doing it? I mean, what's required for them to start with doing the Anycast? For Anycast. I mean, how to implement Anycast for any organization.

STEVE SHENG: Okay. Anyone? Liman?

LARS-JOHAN LIMAN: Lars-Johan Liman from Netnod. To operate an Anycast network, you have to deploy multiple servers using the same IP address in multiple locations. So you need multiple servers. You need to have access to these multiple locations, and you need to have access to the network in these locations so that you can transmit your reachability data.

You need to have BGP routing in these locations, so you have to operate a route yourself and you have to set up peering sessions with peers so that you can attract the traffic that you want to hit your server. And all that has to be maintained using a back channel going to your office so that you can maintain this machinery in the different places.

So there are many things that need to be in place and click but it's quite possible to do and it's done with many services, not only DNS, and it creates very good stability. But the thing is that you need to maintain relationship with very many sites and you have to do a lot of networking both social networking to find these places and find the willing hosts for these things, but also technical networking in order to get this pairing session up and running and to attract the traffic.

UNIDENTIFIED MALE: So you need to host your services probably from different locations, maybe hire a data center to host your servers at different locations?

LARS-JOHAN LIMAN: The whole point with Anycast is different locations. That's the entire idea. And there are, if it's just DNS services and you're willing to buy the service, there are several providers that will help you with that so [you don't have to be running] [inaudible].

STEVE SHENG: There's a question here and then at the back.

JAN SCHOLTE: Yeah, thanks very much. Jan Scholte, University of Gothenburg. I'm trying to get the right language as a nontechnical person. On the one hand, you have the core identifiers and on the other hand, you have the instances. Give me the right language that I should use and also I'm trying to imagine me talking to my students and I want to make it clear instance is a bit, anyway.

And then second question, is there any hierarchy either technical or administrative between those core and those instances, and what's the relationship between the instances and the root server operators? Does that make sense?

And then one question on the transparency. I do get all the transparency and that's very clear, but your meetings at ICANN are actually closed and why is that?

STEVE SHENG: So identities versus instances.

LARS-JOHAN LIMAN: Right, well, I'll have a go at that again. I'll move up here so you can all see me without breaking your necks. The server identities, which is actually the IP addresses of the servers, that's the only important part. The various IP addresses that you can send your packets towards and have a reply received from. These are the service points. These are the points where you can obtain the service.

When we talk about instances, we talk about one installation of equipment in one location that provides service from one specific set of IP addresses. Usually the v4 and v6 address for that. I will use the word that letter or the service operated by that operator.

These service points, the IP addresses are run by an operator. An operator has control over two IP addresses, one v4 and one v6.

And it puts instances, which are installations out where it can find hosts for these Anycast instances, and they all have the same IP address.

So when any client in the world sends a packet towards that specific IP address, it will reach the nearest one. Now, the nearest one is a technical specification here, so you may see some strange traffic but the general idea is it will reach the nearest one. The instances are the only ones providing service to the general Internet.

Now, behind that, there is a provisioning system that each operator uses to provide service from behind towards its instances. Every operator operates a group of instances, and each group of instances uses the same IP addresses and, if you wish, the same letter to provide the service. So there is no hierarchy.

The operators provide groups of instances and the entire set of instances from all operators, they all provide exactly the same service. No difference. If you can find a difference, come and tell me because then we're doing something wrong and we want to make that correct. You shouldn't be able to a difference between these. There was a second question.

STEVE SHENG: Second question regarding the closed RSSAC sessions.

LARS-JOHAN LIMAN: Ah, maybe that's for Brad or Tripti.

TRIPTI SINHA: Hi. Tripti Sinha, co-chair of RSSAC and operator from University of Maryland. To answer your question, the meetings were closed in the past but that is changing starting with this meeting. So I invite all of you to come to our meeting on Wednesday, our RSSAC meeting on Wednesday, which is an open meeting. Everyone is invited and our caucus meetings are open, as well, and you will likely see more and more open meetings as we move forward. It was just a matter of getting organized. Thank you for the question.

STEVE SHENG: Thank you, Tripti. Your question?

UNIDENTIFIED MALE: Thank you. [inaudible] from Pakistan. My question, is the root management ecosystem for the TLD and the ccTLD the same? The second question is that if there is operator of ccTLD and there is a redelegation process, and the redelegation process

posed the applicant is from [inaudible] maybe the government and the community and the application is endorsed by the IANA but the record all the things are with the ccTLD operator, the past one, what will happen? Thank you.

STEVE SHENG: Duane?

DUANE WESSELS: Your question is are gTLDs and ccTLDs handled the same? Yes, they absolutely are. From the Root Server System point of view, there is absolutely no difference. The second question about redelegating a TLD or whatnot, that's really not a question for this group. That's a question for IANA. That's their processes and procedures, so I don't have an answer to that.

STEVE SHENG: Follow up?

UNIDENTIFIED MALE: The IANA said they have no record of the ccTLDs in terms of the DNS and the consumers. It is with the operators.

DUANE WESSELS: IANA has no record of? Of the registry? Yeah, but it still doesn't sound like it's anything to do with the root servers. Maybe they are referencing the operators of that TLD. Yeah, so they're talking about the organization that operated that ccTLD, which is one level down or up, depending on your point of view, from this group, which operates the root nameservers. So those are different groups operating those systems.

STEVE SHENG: Those questions are regarding the provisioning of the servers.

UNIDENTIFIED MALE: Specifically, the one thing to know about the root servers is that the root servers serve data that is provided by IANA. So any changes to the data that's served by the Root Server System has to go through IANA because the root server operators pool all of their data from IANA, so they have no control over actually what's in the zone. That's entirely IANA.

UNIDENTIFIED MALE: But they have the view that they have the data of the TLD but in terms of ccTLD, [they don't have].

STEVE SHENG: That's probably an IANA question. Yeah. Do you have a question?

UNIDENTIFIED MALE: [inaudible] from Iran. Regarding zone updates, all of the updates are being propagated for all 800 instances at the same time or it's the rule, it's the flow that first the A root server gets the updates, after that B, C, D, or what is the flow?

STEVE SHENG: Propagation of the updates. Terry?

TERRY MANDERSON: All of the root server operators receive the root zone from the root zone maintainer at about the same time, and then all of the individual root operators then propagate the root zone out to all of their instances as quickly as possible. There are some statistics in RSSAC002 that are published describing the times that that takes. It's generally within seconds. It's quite quick. The root zone itself is less than a meg or [inaudible] meg. Oh, sorry, two to three meg. I stand corrected, thank you. So it's tiny. Considering the Facebook app is 100 meg last time I looked and growing, it's tiny data. Goes out very quickly.

UNIDENTIFIED MALE: Steve, we have a question right here.

UNIDENTIFIED MALE: [inaudible] from .cy Cyprus. You said that if we want to add a new DNS server, we need to ask IANA. This is done through a procedure or just with the configuration of our server?

STEVE SHENG: Sorry. Could you repeat your question?

UNIDENTIFIED MALE: If we need to add a new DNS server, you said that we need to go through IANA. Do we need a procedure for that or is that a configuration on our server?

STEVE SHENG: The IANA have procedures on how they interface with TLD operators, but that's kind of an IANA question, I feel.

UNIDENTIFIED MALE: Can you clarify? Are you looking to add a DNS server for a ccTLD or at a root server? CcTLD? Then yeah.

STEVE SHENG: Yeah. There's a process on the IANA Website. Go and check that. Thanks. Any other questions?

VINCENT CHEN: Thank you. Vincent Chen from Taiwan. I have a question. You mentioned about the RSSAC002 statistic data. My question is all of the statistical data is open to the public or just owned by every operator? Is the first question.

And then the second question is you mentioned about the RSSAC's current work, one of the current work is the harmonization of the anonymization procedures for the data, correct? The what kind of data is collected from the operators? Is it traffic? I mean, is there any privacy to the registrant or [inaudible] WHOIS database difference. I mean, my question is the what's the differences there?

STEVE SHENG: There are two questions. First question about RSSAC002 data.

UNIDENTIFIED MALE: Yeah, so the RSSAC002 data is public. To find it, you can go to the root-servers.org Website and then scroll down to the bottom. And if you click on each operator, there's a little button. I forget if it's green or blue but there's a little button that says RSSAC. If you click on that, it goes to each operator's page that has the data files, they are [YAML] files, actually. Liman, do you want to take the question about the harmonization of anonymization and explain what data that references?

UNIDENTIFIED MALE: Can I add one thing to that? The other option is there's actually a GitHub repository now called RSSAC-Caucus, and underneath there, there's a few repositories, one of which is a repository of all the data from all of the roots so that you can actually just go do a Git pull on it if you know how to use Git, and you can get them all at once without having to go fetch them individually from each one.

LARS-JOHAN LIMAN: Running over here. The anonymization project that RSSAC is running, the work party that we have for anonymization of data has nothing to do with the WHOIS data. Periodically, a DNS operations-related group called the DNS-OARC DNS Operations, Analysis, and Research Center, which deals with DNS operations in many aspects and only one of the aspects is root service. They ask the root server operators to collect all incoming queries to all instances, to all 800 servers for 48 hours, and to store them and to upload them to a central repository that is made available. It's not public but it's made available to researchers who want to do research on DNS traffic, how it changes over time.

We've been doing this for several years. They can watch trends and they can watch how the queries change over time, so what did the query material look like five years ago and what does it look like today, and what other trends and do research on that.

Now, these queries are typically exactly as they arrive at the root nameserver, which means that it contains the domain name that's being queried for. Some asks for the www.example.com. Well, that string is in there, but also, the exact IP address from which the query was sent. So you can identify that computer sent this query to the root server at this point in time.

Now, that can be conceived as kind of integrity-sensitive data. So some of us who do these things, especially we and the RIPE NCC, we operate within the European Union, so we're based in the European Union, where there are fairly strict laws against publishing integrity-sensitive data. So we've already taken upon us to anonymize the IP address. We modified the IP address so that this researcher cannot see exactly from which server this query was sent. They can still see the string but they don't know who sent it or which computer sent it.

And the idea we had was to make this a general thing. First, we just do it without much research behind it. We do the anonymization but we haven't researched that thing, so this is an effort to see is there a good way to do this, a better way than

we already do and is this that something that we should ask all the root server operators to do so that all data is anonymized in this data bank that the researchers have access to. That's what this project is about. It has nothing to do with the WHOIS data. Thanks.

STEVE SHENG: Another question.

UNIDENTIFIED MALE: Thank you. Just a little follow-up. But of those 800, of the 800 instances, who is operating most of them? I mean, you have 12 operators. Are all 12 taking the same amount or is it a few of you that are doing all of it and NASA sort of has one or two?

UNIDENTIFIED MALE: If you go to the www.root-servers.org Webpage, you will see at the bottom the list of instances or sites for each operator, and also I believe that it even counts the numbers for you. So you can see who operates the most sites, but that doesn't necessarily mean that the one with the most sites takes the most queries because that's also very much a function of how you set up your peering relationships at these various instances.

I don't think we have a comparison between the root server operators, not the modern one, at least, regarding who takes the most queries, but [inaudible] it's not the competition. We're out there to provide a stable service as a whole. We keep saying diversity is good, and we have diversity in how we approach this. Some of us try to deploy in very small instances and remote areas. Some deploy in large centers, so we try to cover all bases by working in different manners.

BRAD VERD: If I can add to that, I think there are a lot of researchers out there – I'm sorry, this is Brad Verd, co-chair of RSSAC, and Verisign operator. There are a lot of researchers out there who have done statistics aggregating the RSSAC002 data that is public and is available and shows the query counts. You can go out there and see what the query counts are should you want to, so I will add that.

Also, on just listening here, I think maybe I can add some clarifying pictures. I keep hearing instances and maybe some confusion around instances and identities. I think the other way to think about it is each operator operates its own cloud. Right? Each operator runs a cloud, which is made up of all the instances, and then all the operators make up the DNS service cloud. I think we all have a lot of experience of working with

cloud services and that's a way to think about it without getting hung up on a specific instance or a specific identity. So that's one way to think about it.

Also, as a follow-up to openness, as co-chair I've got to speak up for this, we had an open session on Saturday that was open. Tomorrow, we have a number of open sessions. We have a joint meeting with the ICANN Board that is open. We have a working session with the Caucus that is open tomorrow. We have the Caucus meeting, which is open tomorrow. We have a joint meeting with the Office of the CTO, which is open. And then on Wednesday, we have our monthly official RSSAC meeting, which is open for observation, also. So I hope that helps.

STEVE SHENG: Thank you, Brad. Any other questions?

STEVE CONTE: I'm not seeing any hands. I just want to thank Steve and Andrew and the root server operators for their time today. The slide deck is already online posted, so if you have an interest in the slide deck, it's in the schedule itself. If you drill down to the schedule for the session that you just joined, you'll be able to get a copy of the presentation. So with that, thank you both. I appreciate it.

STEVE SHENG: Thank you. Thanks for coming.

STEVE CONTE: We have our next session in about a half hour. It's kind of backwards today because we had some conflicts with the opening ceremony. It's going to be DNS Fundamentals, so it's going to cover mostly a lot of what Andrew covered in the very beginning of the slide deck of the resolution and resolving names to numbers or numbers to names and all that, so if you still have further interest, please join me at 5:00.

Otherwise, for transparency and everything else, we're conflicting directly with the first open public forum for this session or for this meeting down in, I believe, Hall 4, so no harm, no foul. I won't take it personal if you don't come and stay for the DNS thing because I know the public forum is interesting, too. So make good choices and hopefully, we'll see some of you in about a half hour.

[END OF TRANSCRIPTION]