ABU DHABI – How It Works: Root Server Operations
Sunday, October 29, 2017 – 15:15 to 16:45 GST
ICANN60 | Abu Dhabi, United Arab Emirates

STEVE CONTE: Hi. Based on the geographic diversity of this venue, we're going to give it a couple more minutes and see if people can get up here and find the room before we get started, so relax, make yourself at home. We'll wake you up when we're about to start, but it'll be a couple more minutes from now.

Test, test.

All right, we're going to go ahead and get started. Thank you all for making it today. Luckily, for those of you who aren't here, I'll speak to you directly, we're having this session again tomorrow so if you're not here now, raise your hand and we'll expect to see you tomorrow.

Thank you. It's our last session of the day for the How It Works series. This is always one of my favorite sessions – and I'm standing right in front of the mic – from the Root Server Stability Advisory Committee, Security Advisory Committee. I'll let Andrew correct me on that.

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.

ANDREW MCCONACHIE: Root Server System Advisory Committee.

STEVE CONTE: That's exactly it. It's been a long day. They always come up and they do a great presentation. They talk about the root servers, the Root Server Operators, the relationship to ICANN, and all kinds of stuff. So you're actually here for a good session.

We do have some Root Server Operators in the room who will be fielding questions. Can I get the RSOs to raise their hand? We've got four or five, five of them in the room today. So feel free. This is meant to be an open session. Questions are encouraged. I might demand them later if no one is asking questions. And we're going to hold the questions until the end of the presentation, but then we're hoping to have a dialogue at the end. So with that, I'm going to pass on to Andrew McConachie who is the RSSAC support person from ICANN to RSSAC.

ANDREW MCCONACHIE: Yep. Thanks, Steve. Hi, my name is Andrew McConachie. I work for ICANN. I do policy support for the RSSAC and the SSAC. And I'm going to be talking to you, along with my colleague, Steve Sheng. I'm going to be giving the first half of this presentation and then Steve will take over for the second half.

This is a tutorial on the Root Server System, and here is what we're going to be covering. I'll be taking the first two and Steve will take the second two. First, we'll do an overview of the Domain Name System as kind of an introduction to how the DNS works and how it interoperates with the Root Server System. Then we'll go over the Root Server System today and its features, so that's a bit more of a deeper dive onto the Root Server System and how it works today.

And then Steve will take over and give an explanation of Anycast. That will explain the benefits of Anycast and why the root servers use Anycast. And then we'll finish up with some of the recent activities of the RSSAC, some of the publications and some of the things the RSSAC has been doing.

So this is the overview of the DNS. It's pretty general. It doesn't require any kind of prior technical understanding of how the DNS works or anything, but if you do have that understanding, then this will hopefully be a good refresher.

So first, a bit of a recap on identifiers on the Internet and on IP addresses. Before we get to the DNS, we need to understand IP addresses.

IP addresses are the fundamental identifier on the Internet. If you need to get to a device, you need to know its IP address. All connected hosts on the Internet do have IP addresses and IP

addresses are a numerical label. And that'll become more important when it becomes apparent what it is that the DNS does and one of the functions that the DNS provides is to translate IP addresses and names back and forth because people don't like remembering numbers. They want to remember a name.

And then there are two kinds of IP addresses, IPv4, IPv6. You're probably familiar with both of those or have seen some reference to them in the past or at this ICANN or previous ICANNs.

Why DNS? So I talked about this a little bit in the last slide. What was the original problem that DNS was trying to solve? I'm going to move over here.

So the first problem that DNS was trying to solve was that IP addresses are hard to remember. I mentioned that IP addresses are numerical identifiers. People don't like remembering numbers. They like remembering names. So we have this mapping of IP addresses to names and names to IP addresses.

The other original problem was that IP addresses change a bunch. They're not static all the time. Sometimes they are. Sometimes a device will keep the same IP address for a long time. Sometimes they won't. Maybe it's using DHCP. Maybe the address just changes a bunch.

And now we're back to the modern problem, the Internet has changed. The Internet is not the same as it was when DNS was invented, so this is more of a take on the modern problem that DNS is trying to solve. And IP addresses may also be shared. And we'll get into that more when we talk about Anycast, but it's important to note that there was a time on the Internet when IP addresses were much more unique than they are now. Now they could be shared. You could have NAT involved. You could have CGNAT involved. It's a bigger problem.

And multiple IP addresses may serve as entry points to a single service, so you can look at these two bullets as like the one-to-many problem and the many-to-one problem. You can have many IP addresses for one device. You could have one device that has many IP addresses. DNS helps to deal with this problem.

So this is a quick overview of the data layout of what DNS is, the hierarchy of DNS. This is about the data. DNS is a look-up mechanism for translating objects into other objects, like I talked about IP addresses. It doesn't always have to be an IP address. DNS will provide translations for other things. There's many different types of resource records besides just A and Quad A records. But we talk about those the most because those are the most used and that's what people are most familiar with.

But here we have people are probably familiar with this. Does anyone have a laser? Whatever, I'll point. Up here, we have a root and then we have these things called Top-Level domains, which I'm sure if you spent any time at ICANN, you've heard the term Top-Level domain. And here are some examples, edu, mil, uk. And we have the second level and then all the way down to the third level. And there's really no limit to the amount of levels you can have.

But the important thing from this slide is that DNS is a hierarchy. And here we have the mapping and then we have some of the other mappings I was talking about.

There's a whole lot on this slide, so I'm going to spend a bit of time on this slide, walking through the process, walking through the resolution process. On the right, you see we have a human being sitting on a computer and then on the left, we have a bunch of computers.

So let's walk through this and it's maybe a little bit confusing because the human is on the right and we generally read from left to right. But luckily, we're in a country where this isn't always the case, so we get to read from right to left. So this is a good slide for a UAE.

So this is our user, our client, and they've got a computer and they really want to get to the web server at www.example.com.

And so what they do first is they contact their Recursive resolver, the Recursive Name Server. And the Recursive Name Server does a whole bunch of different stuff. Well, he sends multiple queries before he goes back to the user with a response. So the user is telling the Recursive Name Server, "Go out and figure out what the IP address of this name is and don't come back to me until you're done." That's what the user is telling the Recursive.

We're going to pretend for this experiment that the Recursive just turned on, has absolutely nothing in its cache, and needs to start from the beginning. So the first thing it does is it needs to figure out where .com is. It doesn't know. So it asks the root server, "Hey root server, tell me where .com is." The root server comes back. Now he knows where .com is.

And then he goes over to .com. he says, "Hey, tell me where example is," and the .com name server tells him that. And then he goes over to example.com and he says, "Hey, tell me where www.example.com is." So then he goes back and now he's got the whole thing.

And now we can go back to the user and the user now has an IP address for www.example.com and our user can visit a webpage now.

So like in the previous examples, the root servers only know who needs to be asked next. Right? The root servers don't know

where example.com is and they certainly don't know where www.example.com is. They only know the name servers for .com.

And here are just some examples for some popular TLDs. The .com will give you a list of com servers, .net will give you a list of net servers, that kind of thing.

And this is something I kind of left out of my previous example. Remember when I said we're going to assume that the cache is empty and the server just turned on and absolutely this is from the beginning? That is a very infrequent scenario that rarely happens.

Typically, Recursive Servers will have caches that are pretty large and answers already prepared for some of the most common queries because when they get a response back from an authoritative DNS server, whether it's a root server or the .com name server or whatever, they're going to cache it for a period of time and if somebody else then comes and asks that same question again, they're going to have it in the cache and they don't have to send another query. They can immediately respond.

Here are some very modern extensions to DNS. So the one you'll hear the most about is DNSSEC. DNSSEC creates cryptographic signatures on DNS data. It's really just about the data and it

doesn't actually encrypt the data. All it does is it's a signing and validation process.

So on the one end, on the authoritative side, the data is signed and then on the validation side when it gets to the Recursive Server, can validate that signature and then determine that it's the correct data. It is the data that the correct authoritative server really sent and it hasn't been forged somehow. It doesn't actually encrypt it.

Privacy enhancements. So queries can leak information, right? Because everything gets transmitted in the clear in terms of DNS. There's some stuff going on in the IETF right now, specifically in the DPRIVE Working Group, if you're interested, to do DNS Server TLS, so Transport Layer Security. It's HTTPS, if you're familiar with that. HTTPS uses TLS. TLS is just a generic transport layer that the IETF is currently working on using with DNS so that DNS can also be encrypted, and that's separate from DNSSEC.

The third thing here which is in vast use is Anycast. And the idea with Anycast is multiple servers share a single IP address. Anycast, really, I think I would say Anycast really provides two important functions. One, it gets root servers closer to the query, closer to the Recursive Server. And two, it protects against DDoS attacks. So it does those two really important things and my

colleague, Steve, will talk more about Anycast and do a deeper dive on that in his talk. But that's really like the two. You can think of Anycast as really doing those two important things.

Oh yeah, and for privacy enhancements, I forgot one called QNAME Minimization. And the interesting thing about QNAME Minimization is instead of sending – so remember when the Recursive Server goes to the root? Well, in the original DNS specification, the Recursive Server would send the whole www.example.com to the root even though he really only needed to send the .com to the root. He really only needs to know where the .com TLD name servers are, but he sent the whole query out there.

QNAME Minimization is a recent enhancement to DNS that's kind of working its way through deployment, it's brand new so it isn't all that widely deployed. But with QNAME Minimization, the Recursive Server only sends the .com, so it doesn't send the www.example part, so there's less on the wire, so there's more privacy.

The root zone versus the root servers, this is really about the difference between the data and the serving of the data. So the root zone is the data itself and the root servers, they publish that data and answer queries about that data. So in the root zone, we can think of that as the top of the hierarchy. It includes the TLDs

and the name servers. It's managed by ICANN per community policy and it's compiled and distributed by the Root Zone Maintainer to all of the Root Server Operators. Again, we can think of it as the database content that the root servers are holding.

The root servers, they're responding with data from the root zone. They're responding to queries with responses. Currently, there are 13 different identities and over 800 instances at physical locations worldwide. So the 13 identities are [a-m].root-servers.net and the 800 instances, when we talk more about Anycast, you'll understand exactly what an instance is. The root server's role is purely technical. They just serve the root zone.

So into the Root Server Operators. There are 12 different professional engineering groups that are Root Server Operators and they're focused on reliability and stability of the service, accessibility for all Internet users, cooperating between one another technically, and maintaining professionalism. They're a diverse group of organizations and their diversity includes technical diversity, organizational diversity, as well as geographic diversity.

Operators are not involved in policymaking and they're not involved in data modification. So you remember two slides ago I was like, the difference between publishing and editing. So you

can think of the operators as really the publishers as opposed to the editors or the authors of the root zone.

Operators are involved in careful operational evolution of service, so changing the service to meet new needs; evaluating and deploying suggested technical modifications; and ensuring stability, robustness, and reachability.

So that was a brief overview of the DNS and how it interacts with the root servers, and now we're going to get into more kind of up-to-date Root Server System today and some of the modern features of the Root Server System.

Here's a bit of a history slide. We started out in 1983 with 4 addresses and you can see it growing to 7 and then 8 and then 9, and then 1998 with 13. But we don't have 13 anymore. This is prior to IPv6, so I don't think in 1998 there were any IPv6 addresses. So now you could say there are 26 addresses. But there are still, as we say here on the slide, 13 IPv4 and IPv6 address pairs.

And these changes over time have been responded to technical demands. The Internet has changed over time and the big change between then and now is, of course, Anycast. That's the huge change. And this allows us to have over 800 international instances.

These are some foundation principles of the Root Server System. Most importantly, provide a stable, reliable, and resilient platform for DNS. It operates for the common good for all of the Internet. And the IANA is the source of the DNS root data.

Architectural changes have been made based on the results of technical evaluation and demonstrated technical need. And technical operation and expectations of the DNS are defined by the IETF, so the standards, stuff like DNS, I mentioned QNAME Minimization, which doesn't really affect the root servers, but these kinds of standards are developed by the IETF and the Root Server Operators just adhere to those standards.

And if you're really interested in this stuff and you're really interested in the history of the Root Server System, check out RSSAC024 which is a pretty long and extensive document, which should give you a lot of information about the Root Server System.

Here are the addresses as they look today. These are the identifiers as of today. And you'll see, on the left column, we have A through M for the different identities. We have the IP addresses in the middle. To the left of the middle column, we have the IPv4 address and then to the right of the middle column, we have the IPv6 address. And you'll notice that every

identity has both an IPv4 and an IPv6 address. And on the right, we have a manager of each one of these identities.

Here is a little map that's taken from root-servers.org. It uses some software that doesn't really accurately reflect where these instances are, and if you add up all these numbers, you don't get 800. But that's kind of an artifact of the software that's used for the mapping. You can actually look at individual cities on root-servers.org so you can see, "I wonder if this city, how many instances they have."

We have a question. Can we wait until the end of this section? Is that okay? Awesome, thank you.

But in total, there are 800 around the world. Excuse me, there are more than 800 because it changes a bit faster than I could update the presentation so we just say there are more than 800. The last time we gave this presentation, there were more than 600, I think, so you get an idea of the rate of change.

Okay, now this is a complicated slide. There's a lot on here, so I'm going to spend some time here.

We talked about the publisher, the IANA function. So imagine, let's go through this like a flow. I'm standing in front of it. So a TLD operator – a .com, a .net or a .org – has a change that they need to make to the root zone. What they'll do is they'll contact

the IANA with an update. Maybe they need to change the address of their name server or something, so they'll contact the IANA and say, "Here's the new address of my name servers."

So then IANA prepares that, checks that, does whatever they do, sends that to the Root Zone Maintainer, and the Root Zone Maintainer prepares it, especially with the introduction of DNSSEC. The Root Zone Maintainer has to do some cryptographic function over this data. And then I don't know if it's exactly like a push or pull function, but let's say they push it to the various identities and all of the instances, so all of the 800 root server instances that we talked about, or over 800 instances.

And then over here, on the far right, we have the Recursive Resolvers who are sending queries to the instance located nearest to them and getting responses.

So that's kind of the flow of what's being explained here, and the interesting thing, there's this squiggly line here. You see on the top, there's the RZERC and the RSSAC. Again, this is showing the difference between the editors of the data over here and the publishers of the data. We're sticking with that analogy of editors and publishers. We see here the RSSAC and the RSOs, they're just distributing that data. They're just answering queries. Here we see that data being prepared in this half.

So some features of the Root Server Operators, we talked about diversity before, but a bit more on diversity, they have different types of organizational structure. They have different histories as organizations. They're using different hardware and software platforms. That kind of diversity really helps in case there's a bug in one of those, like a bug in a certain operating system if we have a diversity of operating systems and it won't affect everyone. And they have a diversity of funding models.

They do, however, have shared best practices of physical security, important to over-provision in case DDoS attack or there's some kind of spike in use. And they have a professional and trusted staff.

The Root Server Operators cooperate. Many of the Root Server Operators, of course, come to ICANN and other meetings as well, all the various kind of Internet institutions and they're meetings. They use Internet-based collaboration tools, especially in times of trouble or preparing for times of trouble. There's a lot of collaboration that happens to ensure continuation of service.

And there are certain measures of transparency as well, which we'll get to later. We'll go through all the different types of transparency. And there's a lot of coordination as well.

Yeah, I mentioned the possible emergencies and periodic activities to support emergency response capabilities, just

planning for worst-case scenarios, and then these established Internet bodies where they are involved.

And this is, again, talking about the evolution of the Internet. The Internet continues to evolve. Root Zone Operators analyze and adopt new uses and protocol extensions on the service. So IDN is relatively new. By Internet terms, I guess they're relatively new. DNSSEC, just a few years old. I guess the root zone was signed in 2010. Someone will probably correct me because I'm wrong with that, but I think it was 2010. IPv6, we got the first Root Server Operator with an IPv6 address in 2008. And increasing robustness, responsiveness and resilience. Wide deployment of distributed Anycast with over 800 instances worldwide.

This slide goes over some of the myths, the misconceptions that people have about Root Server Operators and hopefully, the right column collects them. Root Server Operators do not actually control where Internet traffic goes. Routers do that.

Most DNS queries are not handled by a root server. Remember I talked about caching. Caching is going to take care of, I don't know exact percentage, but the vast majority of queries are going to be handled by cached responses. So most queries don't go anywhere near a root server.

Administration of the root zone and service provision are the same thing. No. Remember I talked about the difference between editors and publishers, and that's kind of how there's a separation. Here it's called administration of the root zone is separate from service provision. Same thing.

The root server identities have no special meaning. [a-m].root-servers.org are all pretty much, they're just letters. There's no special meaning there whatsoever.

There are a lot more than 13 root servers. There are 13 technical identities, but there are over 800 servers right now and that number keeps going up.

The root server operators do conduct coordination activities, so they plan for service operation as a whole. They are talking to one another. And the root server operators only receive the TLD portion of the query.

Now it's interesting. We left this on here. See, this is actually changing because of that thing I talked about earlier with QNAME Minimization, but this is still a myth. The reality is still that the Root Server Operators receive the entire query, but as QNMAE Minimization gets deployed, maybe that'll change. I don't know. Maybe we'll have to remove that bottom one in the future, but for now, it's still there.

And now I'm going to turn it over to my colleague, Steve Sheng who is going to do the last two.

STEVE SHENG: Thank you, Andrew. My name is Steve. Together with Andrew, we support the Root Server System Advisory Committee. So let me do a first, quick dive on the explanation of Anycast. As Andrew just mentioned, there are over 800 Anycast instances of the global root service.

So there are two concepts here. There's the Unicast and there's the Anycast. So in Unicast, the packets from all the sources go into the same destinations. You have multiple sources, but a packet always goes to the same destination. And a single instance serves all the sources. So as a result of this, think in a scenario of distributed denial services attack all the attack traffic will go to that single instance, so that's what we traditionally called Unicast.

And then compared to that is the Anycast. The difference here is in Anycast, instead of a single instance serving all the sources, we have multiple instances serve the same data to all the sources. It's a very key difference. Let me repeat that again. We have multiple instances serve the same data to all sources, and then the sources use the destination based on the intermediate routing policies. The result of that, Andrew just mentioned, one,

you reduce the latency to get that data and, second, you improve the resiliency in the face of denial of service attacks.

So let me illustrate that with a couple figures. So first of all, Unicast, all the traffic from multiple sources goes to the same destination and the traffic by routing takes the shortest route to that destination. So that's Unicast.

Here with Anycast, you have these multiple instances where they were essentially advertising saying, "I'm serving this address. Send the traffic closest to me." As a result, from the routing perspective, the traffic from the source, for example here, takes the shortest route to the closest destination. And because of that, the path is shortened and data is delivered more quickly.

So let me illustrate that with the denial service attack scenario. So for example, in this scenario, you have an attacker that's sending a lot of attack traffic, 300-400 megabytes per second. And then because of the Anycast, that traffic is sent to the closest, the shortest route to the destination which is this. So these other will be unaffected, so the service continues for those.

So that's a quick explanation of Unicast and Anycast and why it's important technology, both for reducing the roundtrip time and also improving the resiliency.

Now the Root Server System and your networks, so we have these questions in some of the previous tutorials where people ask, as a network operator, what can we do to reduce the latency, to improve the resiliency of accessing to the root service?

So first of all, you probably want to have three to four nearby Anycast instances of the root service. And second, just as important as having instances nearby, it's also very important to have increasing peering connections. So sometimes although you have the root servers nearby, because of peering arrangements, those traffic may not be directed through to those root servers. And as a network operator, you might also consider hosting a root server instance. So that's the first thing you can do.

The second thing is to deploy RFC7706 technology. What this technology is, is to reduce the time to access the root servers by running one on a loopback. So sometimes you may have a root server far away or sometimes you do not want someone to snoop or scoop the traffic that you are sending to the root servers. What you can do, as this RFC describes, you can run kind of a copy of the root service on a loopback address, and therefore, decrease the time and increase its caching. So that's a technology that has been recently standardized.

If you can convince your resolver operator to turn on the DNSSEC validation, you can validate the root zone that comes from the IANA, that's served by the Root Server Operators. Those are not modified in transit.

And finally, the Root Server System Advisory Committee has established a caucus which I'll go into a bit detail. It's a broad body of technical experts where they come together to do technical studies, improving the service. And that's where technical advice is created. If you want to have input to that, that's another venue, to join the RSSAC caucus.

So we mentioned a lot about RSSAC and what exactly is RSSAC. So the RSSAC, the full name is the Root Server System Advisory Committee and it exists to advise the ICANN community and the Board on matters relating to the operation, administration, security, and integrity of the Internet's Root Server System. Now, this is a very narrow scope. It's only focused on the Root Server System and to provide advice to the community and to the Board on those matters.

So RSSAC, it produces advice, it's an advisory committee. It produces advice to the Board, but not only to the Board, but to the community as well. One very important distinction here is RSSAC does not involve itself in operational matters, on how a

particular root is to be run. RSSAC does not involve itself in those matters.

Here's a broad, overall of the ICANN organizational structure, the community and RSSAC sits here along with the four advisory committees. So the RSSAC is one of the four advisory committees along with the At-Large Advisory Committee which represents the Internet end users, the Governmental Advisory Committee represents governments and the public policy interests, and the Security and Stability Advisory Committee that focuses on those issues. So RSSAC is one of the four advisory committees.

RSSAC is composed of appointed representatives from each of the Root Server Operators and then each operator has the option to appoint an alternate to RSSAC and that also liaisons, from the key bodies of the Root Zone Management. And in addition to that, we have the RSSAC Caucus, which is a body of technical experts. It's volunteer technical experts and those are confirmed by RSSAC based on their Statement of Interest.

The current RSSAC Co-chair is Brad Verd from Verisign. Brad, are you here? That's Brad. And then Tripti Sinha from the University of Maryland. Tripti? That's Tripti. Okay.

As I mentioned earlier, there are RSSAC established liaison relationships with these bodies. So the first two, the IANA and

the Root Zone Maintainer which currently is Verisign, so those are the entities that are involved in editing and publishing the root zone. And then Internet Architecture Board is an important body because it has overall responsibility to look at architectural issues for the Internet and its protocols.

In addition to that, we have liaisons to the SSAC, the ICANN Board, the Nominating Committee, and the last two committees are the result of the IANA transition, a Customer Standing Committee which oversees the performance of PTI and also the Root Zone Evolution Review Committee which considers architectural changes to the root zone. So those are the various liaisons in the RSSAC.

Currently, the RSSAC Caucus, we have 87 technical experts. They have public Statements of Interest. Those are publicly available. And then one of the goals for the Caucus is transparency, so they are transparent on who is on the caucus. They are transparent on the deliberations within the caucus because the mailing list is open, and also transparent on the credit. So when a report is issued, the people that contributed to those reports are listed as contributors. So you can see that.

I think the caucus has produced three or four documents since its creation. Several of them are quite substantive. To apply, there is an e-mail here. It's rssac-membership@icann.org.

The recent publications, I just want to name a few, the RSSAC027 and RSSAC 029. These are the workshop reports. The RSSAC for two years has been doing two workshops a year to focus on matters on the evolution of the root servers. As a part of the transparency, every time they've done a workshop, they've published a report. RSSAC028 is a technical analysis of the naming schemes used for individual root servers and then the RSSAC000. That's the operational procedures. Now, there's the RSSAC public meeting. I think it's on Tuesday afternoon. That will talk about some of these publications.

Currently, the RSSAC Caucus is working on three topics. The first one is best practices for the distribution of Anycast instances for the root servers. The second one is harmonization of anonymization procedures for data collection. So sometimes the Root Server Operators, they provide some of this data to researchers, to various resources, and then by law, some operators, they have to anonymize some part of that data.

So this looks at whether it's good to harmonize the approach that the various Root Server Operators take on that. And there is also a packet size DNS work party. Again, those work will be discussed further in the public session tomorrow.

Transparency, both the RSSAC and the Root Server Operators have taken continuous efforts to improve the transparency. From the RSSAC perspective, they created a caucus, which is a

wider body of experts beyond just the DNS operators. That can take input when it produces a technical vice. So that's one important step for transparency.

The RSSAC, for a few years, has been publishing minutes, workshop reports. Those are on the RSSAC website. The Caucus and the RSSAC have a public calendar so one can view what the next upcoming RSSAC or RSSAC Caucus meeting or work party meeting is. They meet three times at ICANN meetings and, as a result, they engage with various supporting organizations and constituency groups.

For about two years now, the RSSAC has been giving these tutorials on the Root Server System informing the community how the Root Server System works. And it has been standardizing its operational procedures. Many of those, as a result of the RSSAC review, the transparency effort has been ongoing.

For the Root Server Operators, they publish agendas of their meetings. At IETF, the Root-Ops meet at IETF and they publish the agendas. They collaborate on reporting on major events. So there was a DDoS attack, I think in June, and they got together and published an analysis report.

One important website is the Root-Servers.org. I encourage you if you haven't, go to that website. There is a map there. It shows

currently the Anycast instances of the root servers around the world. It also has a link to individual Root Server Operator websites where you can find, for example, the statistics, every [Op that] published on RSSAC002, and information about their own service.

So those are the transparency efforts, both on the RSSAC and the Root Server Operator end.

If you have more questions on the RSSAC, you can direct your question by writing to this e-mail, Ask-RSSAC@icann.org. I think we receive some. There is a lot of spam in this, but we do receive, from time to time, legitimate questions. The caucus is open. The caucus webpage contains the mailing lists, the working groups, and also the main RSSAC website.

So with that, that's the last slide. We're open to questions and we will be moderating where the operators missed, we'll answer them. Steve?

STEVE CONTE: So, Steve, hold onto your mic. I think what we're going to do is I'll handle the query. You handle the response. So we have Root Server Operators throughout the room. Anyone who has a question – I know someone had a question when Andrew was speaking – raise your hand. I'll bring you the mic, and then Steve

will bring the mic to any Root Server Operator who wants to go. So I've got two questions lined up here.

UNIDENTIFIED MALE: Actually, I would like first to thank you for this useful information. I would like to know why in that gross number of the root servers, it stopped at number 13. Is this technical?

STEVE SHENG: Okay, so the question is why number 13? Any Root Server Operators?

UNIDENTIFIED MALE: So what I mean, if there's any technical obligations?

STEVE SHENG: Is there any technical limitations for that? Who would like to answer? Fred? Go ahead.

FRED BAKER: So there are two different answers, depending on timeframe. When the root system was first set up, we were only dealing with IPv4 and we had a limitation that we expected that UDP packets should not exceed 576 bytes in size, which when you take out the IP header and such, leaves 480 bytes for payload. Divide that

by the size of the different objects that are in that message and that left room for 13 addresses. So the initial limitation of 13 related to the size of what we call the priming packet, that first message.

Now since then, we've added IPv6 addresses, which are somewhat larger than IPv4 addresses. We've added keys. We've added other information. We've also extended the size of the UDP packet, so we're able to handle a larger amount of data in the UDP packet.

But even with that, during the key rollover – which we're actually in the process of right now, we have two active keys for the root rather than one – it turns out that that pretty much fills the UDP packet. So as long as we presume that the priming packet will be carried using UDP, we have a limitation on the number of services that we can run.

The way that would change would be for us to decide that we're going to use TCP for that instead of UDP. But that's not a decision that we've made at this point.

UNIDENTIFIED MALE: Thank you, Fred.

STEVE CONTE: Excellent. This was Fred Baker from F-Root Identifiers, right? Okay, and next question was here.

UNIDENTIFIED MALE: Not a question, but a comment about what Andrew said. I'm [inaudible] from NIC Chile. A number of years ago, we installed the first mirror of a Root Name Server in Chile. It was actually an F-Root. And we tried to get all the ISPs to connect directly to it and [telling] how much more efficient everything would be if that traffic remained in country and didn't have to go abroad.

But actually, what happened was that for most queries, there was no difference because of caching. The only case where you could tell a real difference was for queries for non-existent TLDs.

ANDREW MCCONACHIE: Thank you for that comment. Go ahead, Brad.

BRAD VERD: Hey. Brad Verd, Co-Chair, RSSAC and A-Root/J-Root Operator with Verisign.

Just a quick comment on your comment, RSSAC has published a lexicon which is some of the vocabulary terminology that we use. And in that, the term "mirror" has been deprecated. Thank you. And the reason being is it implies that it is a copy of

something, and these are instances. They're all the same. They all serve the same data, same responses. There is no difference. So I just wanted to point that out.

ANDREW MCCONACHIE: Thank you, Brad. Next question?

STEVE CONTE: Any other questions? We have one here.

BOB OCHIENG: Thanks, Steve. A quick question on normally when we get applications are those who are interested in hosting instances. The question is whether it should be at IXPs and I think it is not really recommended for IXPs. Maybe an explanation around an optimal host. Where should optimally the instance be?

ANDREW MCCONACHIE: Thank you for that question. Where should be the ultimate place? Anyone?

STEVE CONTE: Anyone want to take that? Brad.

BRAD VERD: Where instances go is up to the individual operators who offer hosting of their instances. Okay? So Verisign has a way of determining the best place for their servers, just like ICANN does, just like University of Maryland does, just like all of the different operations do. And we make judgments on where the best instances are.

I don't know your specific scenario or what happened around hosting an instance with you. I can speak for Verisign and Verisign alone because this is a root operator question versus an RSSAC question. Verisign, our goal is to get as many instances to as many people as possible, so while we take a number of things into account like the number of eyeballs that might be sitting behind you, the number of recursives that might be behind your network wherever it's going, that's not the only deciding factor.

The example I'll use is that we have a server that sits in Kenya, and the server in Kenya doesn't get a lot of queries. And a lot of people are like, "Why do you have a server in Kenya when it doesn't get a whole lot of queries?" It's like, "Well, those 60 queries a second are the most important queries to those people querying it. It's very important to them and it provides stability and resiliency for that region."

Really, the only answer I can give you for a Verisign perspective is it's situational. I'd be happy to talk to you later about your

situation and see if we can get one with you. I hope that answers your question.

ANDREW MCCONACHIE: A question up front. Steve, you want to grab that one?

UNIDENTIFIED MALE: I just want to know, is the internal architecture of all 13 root servers the same? What I mean is the way they handle the request and give the output, the designing of the system is done centrally for all the 13 root servers or individual operator designs the internal architecture of the server?

TERRY MANDERSON: Maybe I can respond. Hi, I'm Terry Manderson, responsible for the root server operated by ICANN. Every Root Server Operator has a different architectural model for their equipment. The answer that they deliver is precisely the same across all root server instances, and that's our mandate. We answer exactly the same way, so if you ask for the NSRR set for .net, every root server instance will provide the exact same answer and that's by design. The constructs about our internal architectures are about a diversity concern, so we do things differently and that's important. Does that help answer your question?

UNIDENTIFIED MALE: [inaudible]. The [Anycast] which is expanded, do they have the same architecture that the main root server or they also have separate architecture?

TERRY MANDERSON: It varies. Some have the same. And there's no such thing as a main root server. An Anycast instance is a root server. It's just placed in different locations. And different instances can be big, they can be small, or they can be scoped in size for the catchment area that they're being deployed into.

So perhaps in ICANN I have a root server deployed on one of the Pacific islands behind a satellite link. It's a small installation because it doesn't need to answer 60,000 queries per second. I also have other instances, say, in Prague where I fill up a couple of racks with equipment because it needs to answer 60,000 queries per second. So it varies on where the instance is being deployed, and each Root Server Operator does that differently. And they do that in such a fashion so it's more productive to the global system rather than just their own instance.

ANDREW MCCONACHIE: Thank you, Terry. Any more questions?

BOB OCHIENG: One last one. I think one other question that you get from many people is, are instances responsible or authoritative to specific TLDs or are they authoritative to all TLDs?

I mean, would F, for example, only give responses to particular TLDs, maybe .com, .net?

BRAD VERD: I think I can speak for the collective of root servers when I say this, that root server instances are only authoritative for two zones, potentially three zones, and those are root – so it's only authoritative for the root. None of the root instances are authoritative for com, for org, for any of the other TLDs. All the roots also serve root-servers.net, which is the delegation zone for all of the servers. And then as a legacy thing, ARPA resides on a number of the root servers also, and that's it.

ANDREW MCCONACHIE: Thank you, Brad. Terry, did you have something else or are you just standing? Okay. Any other questions? [Norel]?

UNIDENTIFIED FEMALE: So does it often go wrong because people misconfigure Anycast addressing or routing within the networks? What other sorts of things go wrong due to all sorts of reasons?

ANDREW MCCONACHIE: Terry will take that one.

TERRY MANDERSON: Hey, [Norel]. Long time no see. Things don't often actually go wrong with root servers. They're pretty simple. What you often see is routing effects on the Internet, which root servers actually don't have control of. So generally, if you're going to see any issues regarding the root server's service, it's more often related to routing behaviors within intermediate ISPs along the path.

I have no control over that. It's a fact of life. It's like a cable getting cut somewhere. It's a fact of life. Do we concern ourselves with that? Yes, we do. We watch that, we try and mitigate around that. I can speak for the root server at ICANN, yeah, we take a lot of care and make sure we understand what's happening there.

We're also very concerned about DDoS effects and attacks that either are directed at the Root Server System or are directed at other people that use the Root Server System and the collateral

damage related to that. So we're concerned about those things as well. And?

UNIDENTIFIED MALE: And do what?

TERRY MANDERSON: What do you mean, "and do what"?

UNIDENTIFIED FEMALE: More examples, please, or we can talk about that over the bar, I suppose.

TERRY MANDERSON: I'm not aware of too many more examples. It's pretty constrained as to the things we see in a security and stability sense.

BRAD VERD: It seems like you're implying something more goes wrong. Do you have some examples or specific questions?

UNIDENTIFIED FEMALE: I can just think of so many ways to misconfigure things in so many different places, so I was just sort of wondering more

about the sorts of steps you take in order to mitigate against that. I mean, that kind of sounded like you were saying, "Well, it's other people's problems," but part of what you do is to promote good practices and best practices in configuring networks so that people can reach servers appropriately.

TERRY MANDERSON: We don't actually promote good behaviors at ISPs. That's not our mandate. We don't walk into an ISP and say, "Hey, you must do this and you must configure your network like this because that's the right thing to do, these are the BCPs and so on and so forth." We're about making sure we get the last mile reduced as much as possible and increase the overall global stability of the Root Server System.

ANDREW MCCONACHIE: Any other questions?

UNIDENTIFIED FEMALE: I'm [inaudible] and I'm representing the Pacific Islands and you mentioned that you have a root server in the Pacific Islands. I know that you gave a link that we could go to, to check which cities you have these in, but just out of curiosity, do you have it in just one Pacific island or in a couple of Pacific islands, and which one in particular and operated by who?

ANDREW MCCONACHIE: Pacific island question.

TERRY MANDERSON: The best place is go onto the website. ICANN has a number of instances across a number of the islands in the Pacific islands. We have one in Fiji, Kiribati, and other places, in Guam, and so on and so forth. So we're there. If you'd like to talk to Save, he'll happily help you do more.

STEVE CONTE: Again, the website is Root-Servers.org and you can go there and see, every root lists exactly where they're located at. Don't trust the map. Like Andrew said, don't look at the map and say, "That's it." There are links below on a per letter basis that list the cities where they're located.

TERRY MANDERSON: And there will be more instances than just ICANN. Thank you.

UNIDENTIFIED FEMALE: I'm wondering about QNAME Minimization. What is QNAME Minimization? How will it impact a number of root servers or traffic on root servers? It will be in back of [this].

UNIDENTIFIED MALE: What is QNAME Minimization? How does it impact the traffic to root servers?

UNIDENTIFIED FEMALE: [Inaudible] and if it affects traffic, maybe we will not need so much root servers.

DUANE WESSELS: This is Duane Wessels from Verisign. I think part of the answer is we don't know yet. QNAME Minimization is sort of new. It is implemented in, I believe, two Recursive Name Servers at this point, one of them, I think by default and one not by default, so it's a little bit new. If we were sort of magically at the place where all Recursive Name Servers or all clients that query the root system were doing QNAME Minimization, then yes, it would be a very drastic change. Traffic would probably go down overall.

But I think the reality is that it's going to be a pretty slow deployment. It's not going to be something that leads to a reduction in need of root server capacity. It's not going to be something that we'll say, "Oh, we can turn off half of them now," or something like that.

Again, because of things like attacks, we'll always need the capacity that we have today. QNAME Minimization isn't really going to stop attacks or things like that.

TERRY MANDERSON: Thank you, Duane. Any more questions? Oh, there's one.

UNIDENTIFIED MALE: I have just a question to Verisign. Verisign is the only operator who operates two root servers. If they merge it to one, will the Internet traffic in some way be affected? If not, why are you maintaining two root servers while all other operators have one?

BRAD VERD: Yes, Verisign has two servers and if you read – is it RSSAC024, the history document?

UNIDENTIFIED MALE: Yeah, that's 024.

BRAD VERD: RSSAC024, the history documents will explain to you why we had two. Okay? So it is a legacy thing and we operate two. As far as the hypothetical of combining two, I'm not even sure how to

address that. It's a hypothetical, so I don't know what it would do. But I don't think traffic volumes would change.

If you go in and look at the RSSAC002 metrics, pretty much all the servers get the same amount of traffic, even kind of spread out regardless. Each identity as an aggregate gets the same amount of traffic, not each instance around the globe, much like Terry said. You have some instances that get very small amount of queries, just like the one I mentioned in Kenya and then you have others that are located in large peering centers, lots and lots of traffic. But the identity as a whole, across the board, they're pretty much even.

UNIDENTIFIED MALE: You have just said there are about 800 servers and all are equal in capacity as far as traffic handling is concerned. So 13 may be the legacy. Now if it becomes 12 or if that becomes part of 800 without a name, does it operationally affect in any way or [inaudible] legacy?

BRAD VERD: I'm sorry. I'm not understanding the question. I'm sorry.

UNIDENTIFIED MALE: Actually, you have mentioned there are about 800 servers in different parts.

UNIDENTIFIED MALE: Anycast.

UNIDENTIFIED MALE: Anycast, but all are almost operationally equal?

BRAD VERD: Yes.

UNIDENTIFIED MALE: So it's not actually….

BRAD VERD: Not operationally equal. They serve the same data, give the same exact answer. Operationally, they're different.

UNIDENTIFIED MALE: Okay. Operationally different, but they serve the same data and from the user side, it's [inaudible]. So legacy is one part I accept, but operationally, now if one server is merged with the other, so the name gets eliminated, the same server remains. Will it, in any way, change the scenario?

BRAD VERD: So right now in RSSAC, we are talking through the idea of how to add and remove servers, root server identities. And right now, we're still working through that. That's what the caucus is engaged in and those are a number of ideas and topics that are being talked about. So if you want to help answer those very specific questions, please join the caucus and help.

STEVE CONTE: Thank you. Any more questions?

UNIDENTIFIED MALE: If there are no more hands, I was actually asked a question not too long ago and I didn't have a good answer for it, so I'm going to ask it since we've got some Root Server Operators here and maybe it might be a Root Zone Maintainer question too. I'm not sure.

800+ Anycast instances of root servers out there, does each instance, does the synchronization get the root zone from the distribution master or is each Root Server Operator responsible for getting it once and then distributing it?

BRAD VERD: So this goes back to the diversity comment that was said all throughout the slides and Terry talked about it earlier. So each of the letters has their own distribution system to their Anycast cloud. So the Root Zone Maintainer has its own distribution cloud that it distributes to each of the letters or each of the organizations' distribution system, and then the Root Server Organization is responsible for distributing to their own cloud.

STEVE CONTE: Thank you. One question here.

UNIDENTIFIED MALE: I am [inaudible] from [inaudible]. Do you measure every root server load or something in this traffic in every country or just in the 13 root servers?

UNIDENTIFIED MALE: So how is the system being measured?

DUANE WESSELS: So RSSAC has a document called RSSAC002 which defines measurements that the root servers make. The way that document is written is each operator is responsible for measuring its own set of systems and reporting it as a whole. So the expectation is that an operator measures all of the servers

within their purview, all of them that they operate, and reports it as a whole. When the reporting happens, this data is public, you can go and look at it, but it doesn't show you the breakdown per instance. It just shows you the numbers for the server as a whole. Does that answer your question?

You should look at that document because it defines what metrics are measured. It's pretty basic. It's total query rate, number of IP address sources, and things like that.

STEVE CONTE: Wait for the mic, please.

UNIDENTIFIED MALE: You said the data is public for the others?

DUANE WESSELS: Yes.

UNIDENTIFIED MALE: Is it public on the Root Server Operator side?

DUANE WESSELS: If you go to the Root-Servers.org website, which was listed up on the slides before – or maybe it's still there – and if you scroll down to the bottom, you can click on the different identities.

And then there's a little button that says "RSSAC Metrics," I think is what it says, so yeah, and then it'll take you to each operator's page to see the data.

UNIDENTIFIED MALE: Thanks.

STEVE CONTE: No more questions? No more comments? We've got them for a little bit of time still. All right, well, Andrew, Steve, and the Root Server Operators, thank you very much for joining us today.

We will be here, for those who might have missed some of the earlier How It Works stuff that we've done throughout today, we're doing another session on all of the How It Works tutorials tomorrow as well. So even in relation to the RSSAC stuff, if you think of a question between now and this time tomorrow, or actually earlier tomorrow, feel free to come and join us again and come to the mic and give us your question or your comment.

Other than that, I'd like to say thanks to Steve and Andrew and the Root Server Operators. Thank you.

STEVE SHENG: Thank you for coming.

[END OF TRANSCRIPTION]