DUBLIN – How It Works: Root Server Operations
Sunday, October 18, 2015 – 15:45 to 17:15 IST
ICANN54 | Dublin, Ireland

DAVID CONRAD: Hello, everyone. I'm David Conrad, ICANN CTO. This is the fourth session in the How It Work series. We started this series at Buenos Aires at the last ICANN meeting. This session is a new session. We didn't have this in Buenos Aires, and it is being provided by Duane Wessels of Verisign, who is one of the root server operators. Operates A and J. And is also a member of the Root Server System Advisory Committee. Duane will be presenting on the root server system. With no further ado, I will throw it over to Duane.

DUANE WESSELS: All right. Thanks, David. It's great to be able to be here today and present to all of you. I see some familiar faces out there, so I hope all of you are here to keep me honest, call me out on any mistakes or things that I say that may be not quite right.

As David said, these slides were written by RSSAC and they've asked me to sit up here and sort of read them to you, to present them to you, and I'm happy to do that. We have about only 40 slides and something like 90 minutes. I'm going to go kind of slow. Feel free to ask lots of questions during the slides if something doesn't make sense. And if we finish a little bit early, I guess that will be okay, too. But I hope you ask lots of questions.

DAVID CONRAD: If you have questions, please raise your hand. I've got a hand mic up here, wireless, that I'll bring over to you. Also, at the end of the session I'll be giving a URL for feedback. We have a lot of new faces on here, so I want to just prep you on this. It's a very short feedback form. If you wouldn't mind hanging out for two minutes at the end of the session, putting in the URL, and giving us some feedback so we know how these sessions are working for everybody in our community. Thanks.

DUANE WESSELS: Next slide. In this presentation, we have four main sections. We're going to spend just a little bit of time rehashing how DNS work, going over an overview of the domain name system. We'll talk about the history of the root server system. We'll talk about how things more or less work today, its features and how things are today. Then we'll talk about some things that RSSAC has been doing, some documents that have been published and other activities.

The fundamental identifiers on the Internet, as low as you can go, are the IP addresses. Every host that wants to speak the

Internet protocol that is connected to the Internet needs an address. For the most part, we like to say that IP addresses are unique. That is, you need a unique identifier to talk to another host. But as you probably also know, we have things called NATs which do translation and that allows us to sometimes use non-unique addresses.

But the things that we really care about, the servers that we talk to, those all have unique addresses. Those can either be IPv4 addresses or IPv6. We have some examples here of each of those types of addresses.

Addresses are essentially guaranteed to be unique because they are allocated through pools handed down from IANA and to the RIR system such that no two organizations are given the same address space to use, thus guaranteeing no collisions. Next, please. I think I just scrolled down a little bit instead of going to the next page. Ah, yeah.

Why DNS? The original problem dates back, oh gee, something like 30 or more years now, and it's because numbers, addresses are harder to remember than names. Even from the very, very early Internet ARPANET days, hosts had names as well as addresses. And we like to refer to them by their names.

More recently, we have other problems that DNS can solve for us, which is addresses might be shared or even names might be shared. A name might have multiple addresses, and an address might have multiple names. It also helps as a way to identify entry points into services. For example, www is a web server and so on. Next, please.

You've probably seen something like this diagram here on the right. This is a hierarchy which represents the hierarchal name space of the DNS. The top is what we call the root, and the next layer where here we have edu, mil, and uk, these are the top-level domains and so on down.

This diagram is of course relevant and important because it demonstrates that the DNS is a hierarchal system that helps it scale globally. Different organizations can manage their own part of this hierarchy, their own little space. It's what we call loosely coherent, which means that, for the most part, the answers are the same no matter when and where you ask. They may change a little bit on small-time scales, but generally they are coherent. The fact that it's distributed this way, again, allows these different parties to do their own coordination and autonomous management. Let's go to the next one.

This slide, I don't know if this had animations originally, but this shows what we call the resolution process. We sort of start with the end user sitting at a computer on the left which wants to visit a website. In this case, www.example.org.

That computer will send a DNS query to what we generally consider to be a caching DNS server there in the middle. You can see on that line there, it's saying www.example.org A? In the DNS lingo, A represents the address record. Particularly, the IP4 address record. A lot of times in examples and computer output, you'll see the question there to indicate that this is a query. This is the client querying for the A record of that name. The caching DNS server will then do the resolution by asking a number of authoritative name servers shown here on the right.

The root DNS server is where the caching server will start if it doesn't know where else to start. So it sends a query to the root and the root sends back a response which says, "Okay, go down to the next level," which in this case is the org, an org DNS server. And that will continue down as far as it needs to go. In this case, we only have these two or three levels, so when we get to the example.org DNS server, that one has the answer that we're looking for.

That answer goes back to the caching DNS server. On the picture here, it's saying that the A record, or the IP address for the name you wanted, is 198.51.100.52.

That's the kind of thing that happens hundreds of thousands or millions of times a second in the Internet, in the system. Fortunately, we have this thing called caching which allows that device in the middle, or maybe other devices, to remember the answer they got and reuse it for a certain amount of time, so that every time the user wants to go to the same site, this process doesn't have to happen entirely over and over and over again. Next, please.

As we sort of talked about in the last slide, all that the root servers know is where to go next. Generally, they don't have the data that the end user is really interested in. They only return what we call referrals. If you ask for something like example.org, a root server will give you a referral to the org name servers or the com name servers or the net name servers or whatever.

These referrals can be cached for pretty long amounts of time. It depends a little bit on how the particular TLD is operated, but in most cases, you can figure that these data should be cached for something like a day or two days, on the order of days. The design there is that that is supposed to lessen the load on the root servers. In practice it doesn't always work that way, but that's the idea. Next, please.

This slide talks about modern refinements to DNS. And we have DNSSEC here, which I guess it's modern. It's something that we've been talking about and working on for 10 or 15 years, depending on where you draw the line and go back.

We've been really pushing DNSSEC for about the last five years. It's been deployed in a number of zones, including the root zone and a number of top-level domains.

The reason that we are interested in DNSSEC is because it protects, especially these caches and users from spoofing or poisoning. It protects them from getting bad answers, and it allows them to verify that the data that they got is what the publisher of the data wanted them to get.

In order to do this, the caches and the devices or the clients, they have to validate these responses. That's not something that everybody does, but a lot of them do. That's a little bit of a big step to take if you're running a DNS cache or a recursive name server.

Something quite recent is privacy enhancements. This is work that's actually going on in the IETF right now. There's an IETF working group called DEPRIVE, which I believe stands for DNS Privacy Exchange, something like that. The idea is that there's efforts to prevent leakage of DNS queries. Also using cryptography to encrypt the transactions so that they are harder to, or can't be, eavesdropped on.

Anycast is also something that's… I guess it's modern. The idea behind IP Anycast is that you can operate a service from a single IP address from multiple locations, and you rely on the routing system to direct the traffic to the most appropriate or at least a not-terrible instance of a server to answer the request.

This is really great for DNS. It almost seems like DNS and Anycast were made for each other from the start. Anycast can help reduce latency by directing you to a server that's closer to you than other servers. It also helps in the case of attacks, because Anycast can sort of… If an attack is localized, then the attack only lands at one of the Anycast sites instead of, say, all of them. It's a great way to expand capacity without having to consume new addresses and new server names and things like that. I believe all the root servers at this point are using Anycast. Next, please.

One thing to be clear about is the difference between root servers and the root zone. Root servers are the things that provide the service. They have names like a.rootservers.net. There's 13 of these, A through M. The root servers play just a technical role. All they do is exist to serve the data from the root zone.

The root servers are the responsibility of the root server operators, which we're going to talk about it a little bit more in the next slide, I think. The root zone itself, you can think of it like a big data file. It contains a list of all the top-level domains, of which I think we're up to something like in the order 1,500 by now maybe. Not quite? 1,000.

DAVID CONRAD: I think 900-ish.

DUANE WESSELS: It contains that list of those top-level domains and where they can be found. Their name servers and their name server addresses. These are the delegations that the root servers return.

The root zone is created and managed by ICANN per the policies defined by the community, and it is compiled and distributed by Verisign to all of the root serve operators. Next, please. Sometimes the slides look too similar to each other. Okay.

There are 12 different root server operators. Professional engineering groups that are focused on reliability and stability of the service. One of the ways they do that, of course, is via the Anycast which we've talked about.

They make an important point of providing the service to all Internet users to making it available to everyone. The root server operators, as a group, focus pretty much exclusively on the technical operation and cooperation of the service. They place a lot of emphasis on professionalism.

The root server operators value their diversity. They are diverse in their organizations. There are a number of non-profit organizations running the root server operators. There are educational institutions. There are for-profit companies. There are government organizations and so on. Also, as you would expect, geographic diversity is very important, as we'll see in some upcoming slides. They are spread all over the place, and that is an important thing. Next, please.

The operators are not involved in the policy making, at least as the root server operator group. And they are not involved at all in modifying data. They have committed to publishing the data that they receive from the root zone, from ICANN root zone. That was more of an issue I think a few years ago, but they have all committed to that.

They are involved in careful organizational evolution of the service. For example, when new gTLDs were – and even before they were delegated a few years ago – this is something that the root server operators took very seriously to make sure that they were in a good state to handle these new TLDs. They spent time evaluating, deploying, suggesting technical modifications to the system. And of course, as we've already said, stability and robustness is a critical component of the root server system. Next, please.

We're going to talk a little bit about how we got here today. This table shows some of the root servers – or maybe all of them, I'm not sure – from the time of 1983-1986, a three-year timespan. At that time, there were four organizations running root servers. You can see them listed here.

SRI is the Software Research International Organization. They had a contract to run the Internet Network, or probably the ARPANET Information Center. At the time, they were running software which you probably haven't heard of called JEEVES.

One of my favorite things about this table is that you can see some of the root servers were listening on addresses that start with 10. So that's unthinkable today because the 10 network is RFC1918 private address space. But back then, that was certainly the case.

So three of these four were running JEEVES, and BIND was actually run by the Ballistic Research Laboratory, part of the US Army.

Let's go to the next slide, which I think is 1987. Around 1987 there were four new root servers added. One was added at

Rensselaer Polytechnic Institute, part of NYSERNet. University of Maryland. One for the US Air Force and one at NASA.

So some of these organizations still run root servers today and some do not. As we go on down to the next few slides, you'll be able to see further how they were evolved.

In the timeframe of about 1991, ISI is now running one root server. SRI is still running one. [ERL]. The Army has one. NYSERNet. UMD. Those are all the same. The addition here is the first root server located outside of the United States at NORDUnet. Let's back up just a second.

Also, I just wanted to make the point that now you can see BIND is starting to take a foothold here. A few running the JEEVES software, but more than not are running BIND. Alright, thanks. Next, please.

Around this timeframe, a little problem started to become apparent, which is that the list of root servers had grown to a point where if you asked one of them for the list of all the servers, you got a response that was starting to get a little bit on the large side.

There's an RFC called RFC1035 from I think 1987, which says that DNS responses can't be larger than 512 bytes and we started to run up to that size limit.

So Bill Manning, Mark Costa, and Paul Vixie came up with a plan to rename all the root servers to the names that we know today, which are in the rootservers.net zone. By doing that, it takes advantage of name compression in the DNS protocol, which means that name that's common to all of them doesn't have to be repeated throughout the message. It can only be listed once. That allows you to squeeze a few more names in there. That was done in 1997. Excuse me. Next, please.

This table shows how those nine were renamed into the rootservers.net zone. At that time, ns.internic.net was now a.rootservers.net, and ISI became B. PSI, which used to be NYSERNet, became C. Maryland became D. NASA became E. Internet System Consortium became F. DISA became G. The Army became H, and NORDUnet became I. That's the renumbering. At this point now, we have room for a few more, which I think we'll see on the next slide. So four more were added in the timeframe of 1996 to 1998.

Jon Postel, who was IANA back then, developed some criteria to decide where these four new root servers should go. There was clearly need outside of the United States, being only one outside until this time. Based on this plan, in Europe RIPE was chosen to run one and [WIDE] in Japan. Asia was chosen to run m.rootservers.net. Next, please.

Jon Postel unfortunately died around this time, and in the absence of his leadership, the root server operators decided to begin meeting regularly as a formal group and continue some of the traditions that he started, in particular operating the system for the good of the Internet and committing to maintaining a stable and reliant system.

They all recognize that IANA is the source of the root zone data and committed to making a sufficient investment to operate the system as needed. Next please.

Today, we have 13 root servers listed here. As you can see in the middle column there, all of them but two today have IPv6 addresses, which is quite good. I wouldn't be surprised if those other two acquire IPv6 in a short amount of time. Let's go to the next one.

This map comes from the rootservers.org website, which you all should go and visit in your free time. This is the kind of map where you can zoom in and out. It will show you the geographic locations of all the root servers. At this scale, you see a lot of dots with numbers in them. Those numbers indicate how many sites there are within that region. If you zoom in, they will expand and you can see where they're actually physically located.

We have a question or a comment from John?

[JOHN]: I noticed you missed J and L in the history of when they were assigned and stuff.

DUANE WESSELS: I noticed that, too. I don't know if that was a slide that got deleted. Or did I skip over it? Anyway… Without the slide to go off of, my recollection of J and L is that they were scheduled to be allocated to other [countries], but then Jon Postel unfortunately died. At that point, without his leadership, there was no one to make the decision about where to send them. At the time of his death, one of them was located at Verisign and one was located at ISI.

UNIDENTIFIED MALE: Yeah. And at that time, there was a CRADA, a cooperative research agreement that was between the US government NSF and SDSC [CIDA] – what is that? The Consortium of… Something having to do with Internet service providers.

The idea was that the CRADA was going to try to locate the best place network topologically to place the root servers. The end result of that report was that they couldn't figure out the right answer, so inertia just reigned and the J and L stayed where they were and history moved on.

DUANE WESSELS: Yeah, and also around that time I think we started to realize Anycast was a good thing, and with Anycast it sort of mattered a little bit less that a particular letter was located in a particular region or country or anything like that.

I thought you were going to say something about this map. Because [John] also works on this website that generates this map.

You should definitely spend some time on the rootservers.org website. From here, you can find out the locations not only on the map but you can get a list of all the sites for all the servers for a letter. You can get access to statistics and data and contact information and so on. Let's go to the next one.

This picture documents the root zone management and all the different parties and the flow of data. On the left is represented the TLD operators who may need to make additional changes to their entry in the root zone, and they would send a change request to IANA. IANA will receive that change request and notify both Verisign and NTIA that a change has been received. Then both Verisign and NTIA will do some technical checks on the change to make sure that it looks good and that procedures are being followed. And if the change is then approved, Verisign will add it or update its database of the root zone.

Verisign then publishes a root zone at least twice a day. Sometimes maybe a little bit more, but generally twice a day it gets published out to what we call the distribution masters shown here in the center of the diagram as the DM. The distribution masters are essentially just normal name servers that all the 13 root server letters are configured to get the zone from. They will receive a notification that there's a new version of the zone and then they will download it and publish it on their own systems, represented in the blue there, the A-M boxes.

In addition, as I said, I believe almost all of the operators are now using Anycast. So they have the task of distributing the zone to their many Anycast sites where those sites will receive queries from the DNS resolvers. Essentially, the consumers of the Internet.

This is a process that happens regularly and constantly. Numerous changes are received by IANA every day, and the zone itself is published twice daily. Next, please.

I said a little bit about this earlier, that one of the things the root server operators as a group really value is their diversity. They come from different organizations. There's a really nice mix of non-profits, for-profit, education, government, and so on. They also value diversity in their operations. They intentionally use different hardware and software and share with each other which versions they are using and which vendors they're using, specifically to make sure that there is no single point failure, if you will, or single vendor of failure, such that if a serious bug were uncovered that none of them would all be vulnerable to that same bug.

We also, as a group, talk about keeping the system secure, physical security. We talk about over-provisioning the system for attacks. Some of that has been documented in some documents that we'll talk about at the end of this presentation. Next, please.

In addition to meeting regularly on their own, the root servers are also very involved in a lot of these meetings that we're all aware of – this meeting, IETF, RIPE, NANOG, DNS OARC, APNIC, ARIN, AFNOG. All of these community meetings are places where you will find root server operator representatives to go and speak or listen.

We have infrastructure set up in case of emergencies or other needs where we can convene conference calls. Obviously, we have mailing lists and other online ways of communicating with each other in case something important or maybe even not so important comes up and we just want to talk about it.

I would also stress that if you're not familiar with DNS OARC, I encourage you to look that up. This is an organization which has members – not only root server operators, but other DNS operators or vendors or implementers. Through DNS OARC, we do a fair amount of data sharing, which is to say that the root server operators will provide – make data available for DNS OARC to collect and then disseminate to its members. It's a very great resource. Next, please.

As the Internet evolves, new requirements are put on the DNS system. I mentioned before the new gTLDs in particular. We meet to analyze impact and adapt new uses in protocol extensions. For example, internationalized domain names, DNSSEC, IPv6. We're constantly evaluating the system in terms of its robustness and security and stability and so on.

This slide here says that there's currently over 400 sites around the world. Again, if you go to that rootservers.org map, you'll be able to browse through some of them – or browse through all of them – and see where those locations are. Next, please.

This slide is supposed to address certain myths that seem to come up from time to time. One of them is that… I guess the myth is that root servers have some control over where Internet traffic goes to. I can't help but wonder a little bit if that's because sometimes… Myself I say route, but I hear other people say "root" when they're talking about when I would say routing, route and root – name collision there I guess. But it's certainly the case that the root name servers do not really have any control over where the traffic goes. That is a function of routing.

As we talked about in one of the slides about caching, in particular, and delegations, not every DNS query is handled by a root name server. Only in the case of cache misses or in the case of names that are… Well, either a cache miss or a name that doesn't really exist in the DNS would be handled by a root server. But the bulk of the queries are handled by the authoritative name servers. For example, a second-level domain or lower down in the hierarchy.

It's definitely the case that the administration of the zone is separate from the service provisioning. We had a slide that talked about that, where the root zone itself is different from the operation of the root servers.

There has been a myth that some root servers, or maybe one root server, is special in some way. That myth probably relates to a.rootservers.net because it's first in the list. If you're a DNS geek and you look in the zone file, you'll see it listed in what we call the SOA record, the Start of Authority record. That's just a historical artifact. None of the root servers are special. I wouldn't say they're all equivalent, but they're all equal in their specialness.

It’s absolutely the case that all of the root servers are operated by professional organizations who take it very seriously and are able to devote a lot of resources to the servers and the system that they operate.

Thanks to Anycast and load balancing and things like that, there are many, many more than 13 actual servers. There are 13 organizations or 13 technical entities. Well, there’s 13 letters. There’s 12 organizations. The number of servers is on the order of hundreds or thousands if you were to include all of those behind load balancers and things like that.

No single organization controls the system as a whole. There is a big emphasis on coordination rather than governance. Next, please.

RSSAC is the Root Server System Advisory Committee. Its role is to advise the community and the board on matters relating to the operation, administration, security, and integrity of the Internet’s root server system. We want to make the point that this is a very narrow scope. RSSAC exists to do only this.

RSSAC has been around for many years. Actually, longer than I’ve been involved in it. But in recent years, it has been revitalized. In those last couple of years, we’ve been pretty active and have a few documents to tell you about. Next slide.

Before that though, here's an org chart. If you go to the next slide, it will highlight where RSSAC fits within the ICANN community. It's this box down there. You probably have to load it on your laptop if you want to be able to read it. I can't read that from here. Next, please.

There's two parts to RSSAC. There's sometimes what we call the RSSAC Exec. This is composed of appointed representatives of the root server operators. Each operator can appoint one person and one alternate to this group. Then there's also a number of liaisons, which we'll list in a separate slide.

Separate from that is what we call the RSSAC Caucus. This is a rather large body of volunteers, subject matter experts, who have signed up to do work for us, work parties and document writing and that kind of thing. The caucus are appointed by the RSSAC. Next, please.

Here are your RSSAC co-chairs. Lars Lehman is not able to be here today, but Tripti is here in the back. Thank you, Tripti. She helps write a lot of these slides, so thank you very much. Tripti is from the University of Maryland representing D root, and Lars Lehman is from NetNode representing I root. Next, please.

Here's the list of the RSSAC liaisons. We have a liaison to the IANA Functions Operator. We have a liaison to the root zone maintainer, Verisign. That's actually myself. A liaison to IANA

Functions Administration, which is NTIA. We have a liaison to the IETF/IAB, which is the Internet Architecture Board. We have one to SSAC, one to the ICANN Board, and one to the ICANN Nominations Committee.

In some cases, these liaisons actually are… They have other roles, so it's not necessarily the case that each one of these is a separate person or separate from the RSSAC Exec. Next, please.

The caucus is, I think it says up to 67 technical experts. They are a pool of expertise that the RSSAC can rely on to do work, write documents, and other sorts of things.

If you wanted to join the RSSAC Caucus, you would need to submit a Statement of Interest and you would be reviewed by the RSSAC Membership Committee. If you're interested in applying, here's the e-mail address that you can send an inquiry to. Next, please.

Here's the number of publications that RSSAC has done within recent years. The first one here is RSSAC 001. This is Service Expectations of Root Servers. This document describes expectations – things like you must have a certain amount of capacity to handle attacks and flash crowds. You must be willing to describe your infrastructure. You must be willing to publish statistics and so on.

This document is actually currently held in publication so that it can be released at the same time as an RFC, which describes the same thing and updates an older RFC, which is woefully out of date.

Question in the back?

DAVID CONRAD: One second, please. We have remote participants.

UNIDENTIFIED MALE: Are the service level expectations different from mirrors and the main [inaudible] service? And if different, is there any document that talks about service level expectations for the mirrors?

DUANE WESSELS: I'm sorry. For the mirrors? So there is no differentiation. We don't treat the Anycast sites any differently. They're all treated equally. For example, Verisign, for A root, it has five sites. These are five Anycast sites. There are no other sites. There are no non-Anycast sites. They're all the same. Is that what you were asking? Sorry, Steve. Should've warned you.

DAVID CONRAD: This is how Steve gets his exercise during ICANN meetings.

UNIDENTIFIED MALE: Okay. There are [inaudible] instances of root server mirrors, Anycast sites. When you talk about service level expectations for the 13 root servers, are the same standards applicable to the mirrors?

DUANE WESSELS: If there are root servers that are being operated by organizations other than what we've talked about today – so if there was a party that decides to take the root zone and serve it on their own infrastructure – there is no document that I'm aware of that would describe those expectations. Those operations are not something that RSSAC generally considers or spends time thinking about. That is outside. We would consider that outside of the root server system.

UNIDENTIFIED MALE: Okay, in that case, I think there is a gap. There is a security gap. A certain local network might be relying on a mirror rather than looking up from the main root server. So if there are some compromises in service standards of the mirrors, then there is a gap.

DUANE WESSELS: Do you want to make a comment, David?

DAVID CONRAD: Each of the root server operators that provide Anycast instances do so under their own terms and conditions. The ones that I'm familiar with, the L root server (ICANN operates the L root server) in order to obtain an instance of the L root server, you have to agree to provide certain service levels associated with that root server.

I don't know what the agreements are for the other root server operators. But from the perspective of ICANN and the operation of the L root server, each of the instances are essentially identical, with the exception of the routing policy associated with that root server. Some of the root servers are built to address a local community as opposed to the global community, and as such do not need the same level bandwidth and capacity as the ones that are aimed at providing service to the global community.

The servers themselves, the data that the servers provide, are all identical and the requirements – the service requirements – for the individual instances are identical. It's just the network infrastructure requirements may differ depending on the institution that is hosting the L root instance. I don't know what Verisign does.

DUANE WESSELS: But also, all those L root instances are operated by ICANN.

DAVID CONRAD: Right. All of those servers are operated by ICANN. They're just hosted in facilities based on agreements, contractual relationships between ICANN and the administrators of those sites.

DUANE WESSELS: So any service operated by a root server operator is subject to those expectations. Sorry I wasn't clear before. If you were talking about a service operated by someone who's not a root server operator, then there is no document that describes how they should do that.

MOHIT BATRA: Hi. Mohit Batra from National Internet Exchange of India. There's and [RFC 2870] whose name is root name server operational requirements. So probably this document is the one which we are talking about.

DUANE WESSELS: That RFC 2870 is the one which I said is very old. It is to be updated by RSSAC 001 and some new [RFC]. RSSAC 001 is an update to 2870, and it will be published hopefully soon when the new RFC makes its way through the IETF.

MOHIT BATRA: Actually, I was not aware that RSSAC publications are also there. I was aware of the SSAC, the SSAC numbers, which are around 70 right now, 70 publications from the SSAC.

DUANE WESSELS: Yeah, it sounds about right.

MOHIT BATRA: I was not aware about [inaudible] RSSAC publications.

DUANE WESSELS: Well, we don't have quite as many yet. So maybe as we get more, you'll become more aware of them.

MOHIT BATRA: Yes. So are they subject to public comment periods or not?

DUANE WESSELS: Generally not. No. At least none of the documents published so far have had public comment periods.

So RSSAC 002 is sort of a companion document to RSSAC 001; 002 defines measurements that root server operators should make available about their service. So this includes things like you should publish how many counts of queries were received per day and how many queries came in over IPv4 versus IPv6 and how many came in over TCP versus UDP, and you should include measurements on how long it took you to load the root zone into your system and things like that. This one is published for almost a couple years now or almost a year now, so that's good.

RSSAC 003 is a document that I was involved in. This is a report on root zone TTLs. We did some research on whether or not the TTLs that are used in the root zone are relevant for today's Internet because those TTLs haven't changed for a long time. I guess if you want to know more about that, you can stop me afterwards or in the hall. Or you can come to a session which I think is on Wednesday which is going to talk about this.

RSSAC has also published, rather than reports, some things that we call statements. These are things like comments on ICG proposal, comment on CCWG Working Group. There's one that talks about the IAB liaison to RSSAC and another one here which is the statement on the increase of the DNSSEC signature validity period for the root zone. These are just smaller documents, but we've got a few of those. Next.

Is that the last one? We're close to the end, right?

UNIDENTIFIED MALE: Yeah, you got [inaudible].

DUANE WESSELS: Okay, almost to the end. Something currently going on within RSSAC is there is a Caucus Work Party on root server naming. Naming the root servers. This work party is studying whether or not the way that the root servers are named today is still a good idea and what the implication would be of changing their names. They're looking at the priming response. The priming response is the thing that gets you the list of the name servers and maybe whether or not that response needs to be signed with DNSSEC and so on. This work is pretty close to done, I believe. Maybe be another few weeks or a month and this will be published, I expect. That is probably the last slide.

Happy to take any more questions at this time. Let's see. We have a lot of time for questions.

DAVID CONRAD: We've got about 30 minutes. We have time for everyone to have a question, so start thinking about one.

UNIDENTIFIED MALE: Can this presentation be found shared because it's not on the meetings website?

DUANE WESSELS: It is on the meetings website. If you go and reload the agenda page, it's now posted. If you don't see it, please let me know because I do see it.

DAVID CONRAD: If I might ask, the individuals who are associated with running the root server, raise your hand. I see a few of you all here. A, J, L, D and I know F was here earlier. Oh, and B way up there. Wes just gets off an airplane. Thank you.

DUANE WESSELS: Any other myths that we can correct for anybody? We have a question from a non-technical person, I think.

[PAUL]: [inaudible] answer to the earlier question on RFC 2870, so that document will probably be published as an RFC before the end of the years. Since you were in my session this morning talking about the IETF process, that document has already gone all the way through the IETF process. It had community review. It was accepted by the IAB. It's an IAB stream document, if I remember correctly. And it has already been sent to the RFC editor. There is about a six or eight week time period between documents entering the RFC editor queue and coming out as RFCs if there's nothing else blocking, and there isn't anything else blocking this. So you should expect to see that one.

One thing that I didn't say this morning is if an RFC is revised, it gets a completely new number. The old RFC continues to exist, which is confusing to people, especially if they start looking from the lowest number to the highest. But this RFC will receive a new RFC number, and at that point, as Duane said, then they will publish the RSSAC one at the same time. But you should look for that.

If this was still in discussion in the IETF and you said, "How long will it take?" anyone here with IETF experience would all shrug in unison because we've all guessed wrong before. But since it's already in the RFC editor queue, we have a pretty good idea that it will be out within eight weeks.

UNIDENTIFIED MALE: Paul, this brings me to another question. Can I, after seeing an RFC, find out which working group it was made for?

[PAUL]: Yes, although in this case it wasn't a working group document. Is that right? I'm actually forgetting. Did that come through the [inaudible] or was that an IAB document?

UNIDENTIFIED MALE: I think it's just an IAB document, yeah.

[PAUL]: To answer your question of can you figure out which working group it is, if you go to the RFC editor's website and you look at not just the RFC itself, but there's a page with information about it, it will say which working group it came from, when it was sent to the RFC editor and such. Sometimes there's a multiyear gap between when a document is sent to the RFC editor and when it's published if it has dependencies on other ones. This one won't be that way.

So once this is published, let's say it came out as RFC 7999, if you go to the RFC editor's page for RFC 7999, it will say, "This was an IAB document," and it will have the history there. That's at rfc-editor.org.

UNIDENTIFIED MALE: No one is raising their hands. You're not off the hook yet. Like I said, we're actively seeking feedback on these sessions. Please take a moment and just head over to this link. There are maybe ten yes or no questions that we'd like to ask you and have a better understanding of how these session are in relation to the ICANN meeting and the relevance of them and all that. In the meantime, thank you very much, Duane, for coming in today and presenting.

DUANE WESSELS: Yeah, thank you.

UNIDENTIFIED MALE: David, I'm going to give you last words.

DAVID CONRAD: Thank you, everyone. If you find these valuable, please do indicate that in the surveys. We'll probably be having them again in Marrakech at the ICANN meeting there. If you think these are not valuable, then we won't. So please vote with your interest, and vote often. Thank you.

UNIDENTIFIED MALE: Also, if you missed any of them today, we're doing a repeat of all four sessions tomorrow, so please check the schedule. If you have any interest in coming to see any of the ones that you missed, we'd love to have you.

UNIDENTIFIED MALE: [inaudible]?

UNIDENTIFIED MALE: Yeah, probably not.

UNIDENTIFIED MALE: The room tomorrow is the L4 Foyer or something like that.

UNIDENTIFIED MALE: Yeah, check your schedules. Thank you very much.

[END OF TRANSCRIPTION]