Council of European National
Top Level Domain Registries

Report on

RIPE 69

London

3 - 7 November 2014

Table of Contents

Highlights 3

IANA transition: Must ICANN become a membership organization? 3

Differences in draft proposals by five RIRs 3

Ideas for the IANA-RIR service level contract 3

Does ICANN need membership 3

Oh my god, it's easy 3

RIRs, IETF running off 4

Funding free software 4

From foundation to self-funded open source software provider 4

ISC as a new sales/distribution platform for open source software 5

Plenipot results from the RIPE's point of view: „Engagement works“ 5

DNS Shadowing 6

All those address tricks 6

Gaming the last mile 6

Hijacking Address space during transfers 7

More hijacks using a technical/policy whole 7

Working Groups 8

DNS 8

DNSSEC Algorithm Roll-over to Sha2 8

More DNSSEC issues, validation failure for Elliptic Curve Keys 8

Additional DNS talks 1: More DNS talks: Anycast on a shoestring 9

IETF News 10

Formalizing the election of Chairs

IANA transition: Must ICANN become a membership organization?

The RIPE community in London had their final possibility to talk f2f about the submission the five RIRs will file to the IANA transition coordination committee (ICG) on January 15th. The joint RIR position will be develped by the CRISP group for which Nurani Nimpuno and Andrei Robachevsky were selected as RIPE, and Paul Rendek as RIPE NCC representative.

Differences in draft proposals by five RIRs

CRISP has a month to develop their joint proposal with drafts by the RIRs pretty convergent. Differences exist, though, with regard to the potential establishment of an new „multi-stakeholder Oversight Numbers Council“ which is thought to control the performance of the IANA operator. In a way this is the RIR version of what has been discussed to enhance ICANN oversight by the community in some way.

Both LACNIC and APNIC also favor to have a new memorandum of understanding (MoU) between the NRO (better the RIRs, as the NRO is not incorporated) that would, according to Paul Rendek supplace the current MoU between ICANN and the Address Supporting Organisation (ASO).

Ideas for the IANA-RIR service level contract

RIPE NCC on the other hand prepared a list of criteria for the Service Level Agreement they favor to enter with the IANA operator which includes:

- obligation for IANA operator to execute global policies according to the global PDP (according to MoU between ICANN and ASO)
- processes and time lines for communication
- specific obligations on the IANA operator in terms of performing the number related IANA functions
- review mechanism and sanctions
- duration and conditions for termination of contract by both parties
- dispute resolution and jurisdiction for it

The draft proposal presented to the RIPE Community on a mandate for the RIPE NCC to tackle the issues is here.

Does ICANN need membership

Hans Petter Holen, the new Chair of the RIPE, requested a watertight contract with ICANN, especially as long as accountability issues were still to be solved. Said Holen:

> *„If we enter into a contract with an organisation that's not transparent and open and so on, we need to make sure that our lawyers make that contract watertight for us so that we can change operators in case this doesn't work.“*

An issue raised by the new RIPE chair was that the ICANN Board contrary to the RIPE Board and bodies were not accountable to members, but to the corporation according to Californian law. ICANN in his opinion he said had to create such a membership structure. The members could be the self governance bodies, he said, and the global internet more generally.

Oh my god, it's easy

Despite these deliberations there was a clear recognition at the RIPE meeting that the numbers and protocol „customers“ of IANA have a much easier task in preparing for the transition as the names communities. This was also how European governments had seen it during a dedicated meeting with the technical community in Brussels, attached to a CENTR meeting. Paul Rendek described, government reacted surprised to the limited tasks IANA performed for the RIRs (a hand ful of transactions per year, and three global policies only).

> „They are all busy very much looking at the name space and they are looking at the name space and they come over and look at the RIR space and go, literally, oh my God and then go back to the name space.“

RIRs, IETF running off

Given the relatively straightforward task, the lack of NTIA operational role in the IANA functions performed for the RIRs and the, as the RIPE and RIPE NCC officials underlined, well established transparency and accountability processes in the RIRs they might consider to opt for a Plan B if it becomes clear in June next year that ICANNs name business needs more time. It is possible that ARIN, the North American RIR is less interested in such an option, and a quick transition in general. ARIN CEO John Curran said in London, all accountability issues of ICANN had to be solved before making the step – that much certainly is the killer for a quick transation.

Certainly there are many questions attached to a potential „RIRs and IETF go first“-model: would the NTIA agree to such a split in the first place by updating the extended IANA contract accordingly? How would this change the whole transition game, would it perhaps result in the root oversight transiation to be postponed for a long time? The last question so far has made the RIRs to play the complicated transition game. In fact, both avenues, making a cut comes September or staying in one boat with ICANN, would not bear a major risk for the number administrations.

Funding free software

Bind provider Internet Systems Consortium announced that it will take over distribution and secretariat functions for NLnet Labs in order to help the Dutch competing DNS server provider to manage the transition from foundation funded to self funded.

In a plenary Jeff Osborn, CEO of ISC, made an appeal to address the problem of underfunded open source software development in general. He argued that he disliked the premium model (paying customers will get good, those who cannot afford would get „shitty“ software). Subscription and support models obviously worked better for some. ISC had after some troubles now managed to turnaround and was sound which allowed him to offer the sales support from his 4 head sales team, and 2 people marketing team (total staff is 40) for the much smaller NLnet Labs (8 people) for free.

From foundation to self-funded open source software provider

NLnet Labs is a foundation that had operated on a 15 year grant from NLnet. By next year the NLnet Labs has to become self-funded. The foundation had started to look for alternative revenue streams for some time, said Benno Overeinder. SIDN was still supportive, but would not provide a regular source of income. For tax reasons, a commercial company, OpenNetLabs had been established this year and it would earn the money needed to maintain and further develop the flagship products NSD and Unbound.

The partnership with NLnet Labs was possible as both were open source and non-for-profit operations, said Osborn. He also argued that pooling might help to catch free riders who told his Sales team that while using Bind they would use NSD and Unbound more.

ISC as a new sales/distribution platform for open source software

Osborn announced ISC would first distribe the NLnet Labs security notices jointly with those for Bind, a next step would be that ISC would sell NLnet Labs support, too. A double service for those customers who use both systems could also be of interest, said Benno Overeinder from NL net Labs.

He adamantly said, while benefitting form the joint markting and sales, both partners would maintain their technical basis to ensure diversity. To create diversity was originally one of the main reasons for developing NSD and Unbound in the first place.

At the same time NLnet Labs is not the only DNS provider interested in the Open Source partnership. CZ.NIC would be interested in moving its Knot DNS work also to self-funded. In London nic.cz had therefore also talks with the potential future sales and marketing platform. Osborn said to this reporter, that NLnet Labs would first be supported by the sales team for free, with more distribution for more open source projects that might change.

CZ.NIC announced in London it was about to develop a resolver to complement the Knot Server family. The resolver would be ready in 2015

Plenipot results from the RIPE's point of view: „Engagement works“

The closure of the ITU Plenipotentiary coincided with the last day of the RIPE meeting, Chris Buckridge therefore could report „success“ from the Busan meeting. All resolutions that had concerned the Internet technical community, or more specifically the IP address registries as for example the retabled proposal to make the ITU itself an address registry, had been taken out of the final documents.

Buckridge said the main outcome from the RIPE NCC point of view was the success of the engagement strategy with CEPT (the Conferation Europeen des Post and Telecommunication), and to a lesser extent the RCC (the regional group around Russia) and Arab Group: „engagement works“. Governments had relied considerably on the experts of the technical organisations for technical background to support their arguments about a limited role of the ITU in internet governance in the discussion, Buckridge reported. Bridgebuilding was also obvious when the Iranian delegate appealed to member states after the approval of the limited Internet package to engage in the IANA transition debate at ICANN and elsewhere. Several joint projects of ITU and ISOC were announced in Busan (Using ICT to fight Ebola, together with the GSMA, and ?), yet it was noted by one expert that the ITU was running on a tight budget.

Delegates on the spot confirmed that consensus building had been much smoother. Obviously countries were eager to avoid another split situation experienced in the World Conference on International Telecommunication (WCIT) in 2012. US Ambassador Daniel Sepulveda welcomed the consensus and made clear that an attempt to expand the scope of the ITU work into areas from privacy („content“ according to the US diplomat), enforcement (counterfeit devices) or cybercrime would only „limit its (the ITU's) ability to do anything.“

Developing countries had signalled once more that they saw the ITU as an appropriate venue for certain aspects of the Internet governance debate. The Council Working Group Internet which has been opened slightly for broader discussion and will provide access to its documents will be the place to watch about next steps with regard to the public policies issues pertaining to the Internet.

DNS Shadowing

Analyzing DNS get requests from their notorious GoogleAds network researchers at APNIC Labs realized that a considerable number of get requests was repeated a few minutes after the original request. As normally these requests were unique Geoff Huston and George Michaelson looked into the pattern of what they described as „DNS shadowing“ or „DNS stalking“. Out of 431 million DNS requests, about 780.000 were represented twice, Huston said.

For their presentation at RIPE 69 the researchers did a more indepth analysis of the top issuer of the stalking get requests (about 200 000 during) which according to routing information came from a server in Guanghzhou, China. The requests shadowed this server were dispersed globally all over the world. In an effort to find the communality of the shadowed server Huston found that all had been using a special browser extension for Chinese (pinyin).

The Australian researchers from these observations drew the conclusion that a party in China was „stalking“ Chinese language speakers while abroad, possibly in an effort to check on what Chinese travellers were up to on the web while travelling.

The fact that the stalker in this case did not bother to hide the stalking could well be a sign that he did not bother the stalked to know that they were watched.

Huston told this reporter that a more conspicious stalker could after using such a sophisticated way to spy on the internet whereabouts of persons very well hide the shadowing behind multiple servers. In his data set Huston had only looked at the top spots in his first round of analysis. Inteligence services very well might use the stalking or shadowing to spy on their targets, Huston ackknowledged. In his initial data set he saw widely dispersed servers that only sent out a small numbers of requests. When analyzing these could be neglected as „noise“.

All those address thicks

The RIPE NCC reported about different new trends in gaming the last mile IPv4 policy, using transfer phases and a special feature in the RIPE NCC data base to hijack addresses. For the last mile gaming members agreed to quickly develop a policy proposal. The hijacking will be more difficult to mitigate.

Gaming the last mile

The RIPE NCC reported during the Address Policy Working Group that they had realized 70 cases (of 1000 total) of newly opened local internet registries (LIRs) that had been requesting the availabe /22 allocation from the last mile IPv4 address pool and closing shortly thereafter. Some organisations had opened up to 10 new organisations at the same time. The allocated /22 will then be sold off and transferred and more new organisations could be opened.

With the IPv4 address blocks from the last mile /8 pool of the RIPE being unused and therefore clean address space and IPv4 addresses now being in short supply, this is lucrative business. Paying only a one year membership fee and tiny buck for the opening and closing of the new organisation (around 2000+ Euro) and prices for the /22 blocks up to 8000 Euro, it allows for a nice return of investement, especially when done at a bigger scale.

There is a concern that the modus operandi could become more „industrialized“ and a lot of address space set aside to allow allocations to new companies for years to come (to allow for dual stack for example) could be hampered.

In reaction to this trend the Address Policy Working Group agreed to push for an update to the last mile policy. During the session in London a ban to transfer the allocated /22 for the span of two years was favored. While it would not disallow to come back with new companies time and again, it would slow down the operation and make it much less attractive financially. Address Policy Co-Chair Gert Doering said to this reporter, the respective parties would have to paying four or five thousand Euro over two years and could not be sure the prices for the IPv4 addresses would be the same after that time. The respective policy update would take at least 3 and a half months from mailing list debate, to review and RIPE NCC impact assessment to last call and passing. He said he did not expect a problem from having a gaming panic before the policy kicks in. Currently there are still around 17.000 /8 available, he said, with the RIPE NCC having recovered some additional address space from IANA. IANA official Kim Davies said after a /12, all of the RIRs could expect another /13 in the coming months.

Hijacking Address space during transfers

Another trend that concerns the Address managers are the rising number of attempts to hijack address space while transfers are ongoing. Information about the to be transfered blocks are available on the RIPE website and the blocks make for an easy prey in time spans between the seller not announcing the space anymore and the buyer picking it up and annoucning it for himself. Adhoc recommendations to fix this problem are to only draw back annoucnments when the deal is complete and the buyer will announce the block himself.

More hijacks using a technical/policy whole

More fake routes have been observed by the experts, according to Doering, by exploiting a hole in the RIPE NCC data base. The data base allows RIPE members to create route objects for space that they don't maintain.

> *„I can go tomorrow, or in five minutes, in the RIPE database create a script and basically says I own all the space.“*

The issue became obvious after a Bulgarian provider had pirated address space earlier this year and RIPE customers who were about to transfer that space nad to realize that the addreses were taken. While there might be a small flaw in transfers policy, the big bug was „trust in the InternationaRouting Registry (IRR). The respective pirates are still active and had taken one prefix after another all the time. All in all 20-50 prefixes were hijacked. The hole in the IRR had to be fixed Adress policy WG Chair Gerd Doering said.

Working Groups

DNS

DNSSEC Algorithm Roll-over to Sha2

The DNW working group briefly discussed how to deal with algorithm roll-over for the DNS zones of RIPE. For the time being the RIPE DNS zones are signed with Sha1 that could however be deprecated soon due to known collission attacks. Given that the signing equipement used by the RIPE NCC (Secure64) was unable to sign with differnet algorithm keys at the same time, a normal key-roll over was impossible.

RIPE NCC DNS Operations Head Anand Buddhdev asked if members would favor a two step roll-over, with rolling over to insecure for a period of time (twice the TTL) after which the zones would be freshly signed with Sha2. Other options were to ask the vendor to support the two key-signing or change to a new vendor.

In any case the RIPE NCC would not make its regular November key roll-over, Buddhdev said, or it could just do the normal roll-over and tackle the algorithm roll-over next year. Discussion shall be continuing on the list to decide about this item. For reference he pointed to an upcoming report about the cz-nic experience on algorithm roll-over on the RIPE Labs site.

With 20 percent of DNS resolvers were validationg, serving keys with a algorithm not longer in use would be felt widely on the net, said Geoff Huston.

Key-rollover is also an item on the agenda of IANA, Kim Davies from ICANN/IANA said during the closing plenary. After many years beside the regular zone singing key roll-over, the key-signing key roll-over for the rootzone is considered. It has not been done before.

Other items still to be decided by the RIPE membership are the formalizaton of DNS secondary services to ccTLDs, the potential expansion of DNSMON to new zones and the possibility to open its results without delay to everybody.

More DNSSEC issues, validation failure for Elliptic Curve Keys

George Michaelson, APNIC, promoted Eleptic Curve crypto algorithms as a more effective alternative to RSA crypto algorithms for DNSSEC signatures. ECC signatures would be smaller, faster and cheaper, according to Michaelson. Despite that advantages, measurements showed that ECC validation resulted in much higher validation failure rates. Michaelson and Geoff Huston using their Google ads network showed that 23,6 percent validation failures for ECDSA signatures. From 3 773 420 experiments, 937,166 experiments queried for the DNSKEY RR of a validly signed (RSA) domain (24.8%) , 629,726 experiments queried for the DNSKEY RR of a validly signed (ECDSA) domain (16.6%).

Validation failure was 8.2 percent higher for ECDSA. Michaelson also noted that only 1,6 percent of the ECDSA clients did not fetch data despite the DNSSEC validation could not successfully be performed. IPR issues certainly had resulted in a lack of deployment of ECDSA. Google apparently does't support the ECDSA-Checks either.

The biggest problem that became obvious during the measurments, according to Michaelson, were deviations from the standard that were similar to a downgrade attack. Google while fetching both records flagged there were no signatures and still fetched the urls which practically equalled a downgrade attack. „The end user is not given any information that would allow them to infer they are potentially no longer protected by DNSSEC and we are proposing all behaviours but we are not signalling that you stop doing it. That doesn't feel good“, said Michaelson.

Two additional presentations in the DNS WG which this time had an unusual single slot in London covered measures to secure the DNS, including stealth DNS (to hide the architecture), diversity of software (as a countermeasure to zero-day exploits,) stealth DNS, anti-DdoS strategies (absorb or filter) and Response policy zone, a mechanism in BIND to give alternate answers to queries.

Additional DNS talks 1: More DNS talks: Anycast on a shoestring

Linux-expert and consultant Nat Morris about an experiment to install a low cost anycast system. With a combination of completly open source software (see githup), low cost vpn providers (the cheapest a VPN in India for 48 Dollar per year) and, in one extra step, the set up of a Rasberry Pi as a server, Morris succeded in keeping the costs under 1000 British Pound per year. Starting out with 4 anycast servrers in London (2), Detroit and india, Norris meanwhile has grown his 12 in in different parts of the world and 8 lined up to be deployed. Opinions about the project vary considerably. Some ccTLD experts asked if the concept might inform deployment in developping countries. Morris acknowleged that he not thought on ccTLDs in fact. Other experts questioned that the level of resiliency, a ccTLD could not risk.

In the Open Source Working Group which regularly has a full agenda (London was no exception here) Ondrej Sury presented cz.nics use of open source tools to further develop open source tools, maintains and tests them. A main principle of cz.nic Labs according to Sury is: no use of cloud. Instead using github cz.nic uses gitlabs for code development , code review and measurements.

The list of tools used is quite imporesive.

gitLab – https://about.gitlab.com/
CZ.NIC GitLab – https://gitlab.labs.nic.cz/
Jenkins – https://jenkins-ci.org/
CZ.NIC Jenkins – https://jenkins.labs.nic.cz/
GitLab2Jenkins – https://gitlab.labs.nic.cz/labs/gitlab2jenkins
clang-analyser – http://clang-analyzer.llvm.org/
cppcheck – http://cppcheck.sourceforge.net/
OCLint – http://oclint.org/
Lizard – https://github.com/terryyin/lizard

The Czech registry announced in London, that they that Knot DNS (which is also maintained and developed via GitHub) will develop a recursive resolver.

IETF News

Formalizing the election of Chairs.

All working groups independantly talked about the future election/selection of their CoChairs. As the WG Chairs had been unable to agree on a common proposal, every WG discussed a model with regard to how to select/elect their CoChairs. They differ slightly with regard to number of Chairs, trigger and style of election. Work on this is ongoing in all working groups.

Andrew Robachevski (ISOC) presented during the opening plenary presented the „Mutually Agreed Norms for Routing Security (MARNS)“. The document provides guidelines for opertors to make BGP routing more secure. The recommendations in the document are are:

- Prevent propagation of incorrect routing information.
- Network operator is able to communicate to their adjacent networks which announcements are correct
- Prevent traffic with spoofed source IP addresses.

The document can still be signed by interested parties. It was not a document alone, Robachevski said, it was a committment.

According to the report of the Numbers Ressource Organisation (NRO) the RIRs jointly pay over 800.000 Euro to ICANN, 100.000 for the IGF.

Wielfried Woeber has been selected for another three year term on the ASO Council.

Next meeting will take place in Amsterdam, May 2015