Council of European National Top-Level Domain Registries

Report on RIPE72

Copenhagen
23-27 May 2016

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org

Contents

Highlights

Concerns about ICANN's Public Safety Working Group

RIPE leadership expressed some concerns over the new ICANN Public Safety Working Group, a WG established by the ICANN Government Advisory Committee (GAC). The WG, which was set up to talk about law enforcement and consumer protection issues at ICANN, was not limited to Whois domain issues, but also had started to look into IP address issues, RIPE Chair Hans-Petter Holen reported during the RIPE database WG. Holen asked for attention and comments from the community. ICANN has been discussing policy development on Whois and a change from Whois to the Whois follow-up protocol "next generation registry directory services (RDS)" (IETF RDAP standard) for some time – it is on the Helsinki meeting agenda again.

IP address database to be discussed at RIR fora

A dedicated RIR workshop with the new PSWG during the most recent ICANN meeting in Marrakesh had been used to present governments and law enforcement gathered at ICANN with information on IP address policy development. Hot topics according to Holen had been data access and accuracy of the RIR databases. Governments and law enforcement officials had been invited to join the RIR meetings to further discuss these issues, said Holen.

During the Anti-Abuse WG at RIPE72, Europol presented challenges in finding the users of IP-address space allocated by RIPE. The main challenge remains the difficulty to trace users of certain IP-addresses due to the cross-border nature of IP address management – with an IP-address user being "hidden" behind several layers of service providers. Cross-border requests according to MLAT procedures were too slow and too time-consuming.

Holen called for attempts to educate law enforcement agencies (LEA) and other users of the RIPE database on how the database that included objects from over 13,000 Local IP Registries (LIRs) managing their IP address allocations to customers in different ways.

Cooperation with government agencies and law enforcement at RIPE is done preferably in the regular RIPE Regulatory Roundtable meetings, which remain closed meetings. The Cooperation WG, originally considered for discussions between operators and representatives from regulators and legislators, has developed more into a platform for presentations of academic work on Internet policy and Internet governance issues.

From "get over concerns" to "be careful when re-purposing data collected"

Opinions on how the RIPE community should address the issues vary considerably. Anti-Abuse WG Co-Chair Brian Nisbet said that the requirements on Whois (from law enforcement and legislators) would only get "more relevant" and the community had to "get over" some of the reservations it harboured for years. The RIR community could not exclude themselves from obligations to provide data to law enforcement. "Whenever we think about the reasons why we don't want to push the data we need to ask ourselves why do we want to do that and what good comes out of it."

On the other side of the spectrum there were calls for caution about a potential re-purposing of data processed for the RIPE databases. "The use of databases in the age of surveillance are nothing to be taken lightly", said US academic Milton Mueller (Georgia Tech), member of the Arin AC. According to data protection legislation (in Europe) data were collected for a purpose. Would RIPE decide to use this data beyond the original purpose – facilitating address management – it would have to ask for consent, said Mueller. Holen said he wanted to see an analysis of what the new EU Data Protection Regulation meant for RIPE's data processing. Peter Koch (Denic) said currently no special purpose for serving law enforcement purposes was mentioned in the relevant RIPE documents.

Bulk access to IP address data

One interesting question in that regard could be the provision of bulk data access (also for law

enforcement) for the RIPE database (which is provided similarly as bulk access to domain registry data). This issue came up during a debate over a new agreement signed by RIPE NCC with the Russian Government. While being said to be in line with the standards of cooperation with governments in general (according to RIPE NCC and the RIPE Executive Board Member Dimitry Burkov), some questions were raised over the bulk access routines by at least one senior expert, Daniel Karrenberg (who underlined his comment was made in a personal capacity).

Geolocation for IP-addresses not pursued

Possibly a reaction to related concerns – beside the obvious financial reasons – have resulted in the RIPE Executive Council to stop further work on geolocation data provision by RIPE. The RIPE database offers the "geoloc:" attribute on ORGANISATION and INET(6) NUM objects that may or may not be used as an additional source of information by these providers.

RIPE was not a geolocation provider, the decision states. Existing geolocations providers were free to use the geoloc attribute of the **inet(6)num** object (longitude and latitude numbers), but are advised that (as with other data base entrances) "geolocation information is added by the resource holders in the RIPE Database and RIPE NCC does not verify this information".

DNS Privacy@RIPE

A proposal to establish one or several public DNS servers that will allow to resolve DNS queries using DNS over TLS was received favourably by the RIPE DNS WG. The proposal presented by Sarah Dickinson of Sinodun (sara@sinodun.com) is intended to put into practice the standards developed by the IETF DNS Privacy WG (DPrive), namely RFC 7858 "Specification for DNS over Transport Layer Security (TLS)".

Action Item: Privacy enhanced DNS

While work on reference implementations of RFC 7858 and additional supporting features in RFC 7766 was underway, deployment of a few public DNS privacy servers for experimentation, research, (and also bug fixing) would be a first good step, said Dickinson. The goal for the future is that everybody is able to use DNS over TLS from his and her laptop by connecting to a TLS enabled server. Dickenson posed the question to the RIPE DNS WG members if they would support to have the RIPE NCC set up such a DNS over TLS server.

While there were some concerns over adding additional items to RIPE NCC's work tab, WG Co-Chair Jim Reid asked the RIPE NCC DNS Operations Team to consider the request and come back with feedback on a possible limited-term engagement of RIPE NCC. At the same time there were several participants offering to host servers in their networks:

1. Thomas Rasmussen, (UncensoredDNS), offered to set up an open resolver to test DNS over TLS. Upfront some issues on amplification attacks had to be addressed for Unbound, for BIND some fixes for that were at hand, he said. DNS Knot according to Marek Vavrusek "has out-of-order replies, query deduplication + pipelining, and TCP fastopen" and was engaged in a DNS/TLS project at the OARC hackathon (https://gitlab.labs.nic.cz/knot/resolver/merge_requests/18).

2. Ondrej Sury of cz.nic said that instead of tasking RIPE NCC, the community could ask for a /24 at RIPE (IPv4, or some space at IPv6) and all interested members could host DNS over TLS enhanced servers there. cz.nic was prepared to host such a service over shared PI space.

3. Over the mailing list DNS-OARC offered to host a server, depending on members' feedback. DNS-OARC would be able "to set up this on our Open DNSSEC-validating Resolvers (or in some other way) along with some graphs showing the utilization" (https://www.dns-oarc.net/oarc/services/odvr)", said Jerry Lundström.

Allison Mankin, one of the authors of the IETF specifications and former researcher at the recently discontinued Verisign labs, pointed out the OARC's ODVR might need to be adapted, as for now there would be a "contrast between end-users purposefully using the server for privacy and the provision of their DNS query data to the OARC membership". The services might be good to experiment with anonymizing/de-identifying the data.

4. Another written offer was sent over the mailing list from Roland van Rijswijk, SURFnet. SURFnet would be "willing to host one or two public resolvers at SURFnet that are TLS-enabled" and would reserve a "nice IP address" for it (145.0.0.145).

Qname Minimization

Additional steps to make the DNS a little more privacy friendly were presented with an implementation of Qname for Unbound. While DNS over TLS will allow to encrypt DNS queries and answers, Qname minimization allows to strip DNS queries of unnecessary parts of information when going up the DNS tree.

Users would not expose more data than necessary for a server in the tree to execute its task. The full name if not cached by the recursive resolver of a provider will not go up to the root zone (instead of asking for my.example.nl, the recursive sends .nl to the root, example.nl to the nl- and my.example.nl to the provider of example.nl-Domain). Minimization made all the more sense the more information (for example PGP keys) were stored in the DNS.

For Unbound 1.5.7 DNS minimization is implemented and can be turned on in the configuration by choosing "QNAME minimisation yes".

As the minimization results in multiplication of the DNS requests (for IPv4, Wildcards, DNSBL) the approach could result in abuse for DDoS attacks, which would need to be mitigated beforehand. Limitation of Qname iteration to 10 queries has been chose as a mitigation measure for Unbound 1.5.9.

A privacy problem can result from the fall-back to the full query for NXDomains – which will make the query visible. For Unbound 1.5.9 the solution is a more specific NXDomain cache, to be chosen by harden-below-nxdomain: yes. This in turn also results in a decrease of queries.

Mere baby steps to DNS privacy?

Geoff Huston called DNS over TLS a potential distraction from going for better privacy approaches for the DNS. Huston during the plenary had presented a statistical view on DNS query multiplication by either misconfigured servers, or by number crunchers that "stalk", profile or monitor DNS users.

DNS over TLS on public DNS servers might be in the way of projects like getDNS for example, "where you are dragging back towards the users and eliminating the recursive from the entire picture". According to Dickinson, getDNS was already supportive of strict (instead of opportunistic) encryption.

Going to DNS over TLS meant that people still had to decide who they chose to share their secrets with. "I can use DNS.google.com and it's a secret between me and Google, which I am sure they appreciate and so do I", he said. So the community had to consider if they wanted to rely on the intermediary or drive DNS resolution towards a secured edge.

Going directly to getDNS and encrypted DNS queries up to the authoritative resolvers would result in CPU denial of service attacks for authoritative and/or route servers. Baby steps were therefore recommended instead of a big leap forward. Another problem for the big leap was potential intermediaries (like hotel Wifis) would break the user's secure DNS services.

IANA transition – We got what we wanted

RIPE representatives in the various IANA transition consultation bodies (CRISP, CCWG, CWG, ICG) expressed satisfaction over the outcome of the IANA transition package, expressing that "we got what we wanted".

With another iteration with regard to the Service Level Agreement between ICANN (in the role as Post Transition IANA) and the NRO underway, Nurani Nimpuno (NetNod) and Athina Fragkouli (RIPE NCC) applauded the community for their efforts. The RIR community over the two-year process had earned much respect for their policy development processes.

On May 31, another version of the SLA (version 5.2) was published. Meanwhile, the ICANN Board has tasked ICANN management to finalize and implement the agreement. RIPE is expecting the SLA implementation along the overall implementation of steps agreed upon with regard to the IANA transition and ICANN accountability policies.

Nimpuno said the transition package was now processed by NTIA, but there was no way to know how Congress would deal with it. While the NTIA has declared the IANA transition package (including the Post-transition IANA proposals and the ICANN accountability measures including Bylaw changes) did fulfil the conditions set out, conservative Republicans seem to push against a transition in September. During the RIPE week there was another Hearing in the Senate Commerce Committee in Washington, during which Senator Marco Rubio strongly supported

a delay of the transition. Andrew Sullivan (Dyn DNS) during that hearing pointed out that the checks of DNS root zone changes (for example the addition of new Top Level Domains) by NTIA officials in fact had caused delays in emergency updates and therefore should be eliminated. Rubio's colleague (and former competitor in the US presidential elections) Ted Cruz had protested earlier against the transition in a letter to the NTIA.

A potential delay or deferral of the transition was not discussed by RIPE members. Concerns expressed over a potential change of governments' influence were addressed by US academic Milton Mueller, Arin AC member. He considered that in the new structure, governments had a role pretty much equal to other stakeholders. Yet the "beware of governments"-argument was used by some of the Republicans as an argument for delay.

Next steps for the RIPE community members involved in IANA transition and ICANN would be working on accountability work stream 2 issues, according to Fragkouli.

Address Policy – Not so good Internet citizens?

RIPE72 ended with contradictory results with regard to RIPE's policy for the distribution of the remaining IPv4 addresses. The reserves for which RIPE started a "last mile"-policy in 2012 have melted to 0,97 of a /8 which is just under 16 million single IPv4 addresses.

Stretch run

More specifically from the original last /8 – by the number of 185/8 – about a half is still in stock. The remaining reserves are recovered addresses, either those being distributed by the central IP address registry at IANA, or taken back by the RIPE NCC from within unused space within the RIPE region. With the recovery efforts having been mainly completed for the moment and unused larger IPv4 addresses reserves out in the market being seen and sold as assets more often, RIPE has arrived in the stretch run for the last addresses.

With the end of IPv4 in sight, there are members requesting more than the originally agreed upon /22 last package the RIPE NCC so far has handed over to all members on application. Hence a considerable controversy has developed.

IPv6 does not sell

Basically there are two camps when it comes to a possible loosening of the last mile policy. A number of smaller (younger) companies have argued that they are at a disadvantage compared to larger big corporations who were able to secure large chunks of IPv4 address space, in some cases before regular policies about the documentation of needs for address space have been established by the RIPE community.

Three co-authors (Elvis Velea, who since has dropped out as an author, Ricardo Gori) have prepared a proposal (2015-5) that asked for continuous allocation of /22 packages for those who could demonstrate an urgent need. To make the proposal more amenable to the opposing camp for the version presented in Copenhagen, they did introduce additional conditions including a high level of "RIPEness" (a kind of a certification for observance of RIPE standards). They also proposed that every additional /22 should come from recovered space only.

A core question in the controversy between the give it out-camp and the preserve it-camp is this: is IPv4 still the standard protocol to set up a network – or should this now be IPv6? One co-author of 2015-5 during the debate in Copenhagen defended the position for a more flexible last mile policy:

"There is business to be done with IPv4, not IPv6. IPv6 does not sell."

Remaining IPv4 reserves for transition only

The opposing camp does not agree with that presumption. On the contrary, the last /22 blocks, according to several participants during the plenary debate, need to be preserved for those late-comers ("future Twitter" founders, "our children", "our grand-children", depending on speakers age and experience) that will still need to translate to the large IPv4 world for many years to come. Some speakers even considered that the remaining /22 blocks might be handed out to newcomers only in the future.

A highly conservative change for the last mile was proposed by re-elected RIPE executive Board member Remco van Mook. He proposed to close down the last /8 effectively by allowing each RIPE member to hold one last /22, and nothing more. Included is an obligation to hand back a possible /22 after a merger,

acquisition or any other reception of such a last mile block – the blocks should eventually be marked, so that everybody who is about to buy a company would be well informed he could not keep that one in case he already possessed another last mile /22.

While such a policy might limit some circumvention of the current last-mile policy – for example the fast opening and closing of new memberships or even new companies to receive more of the scarce address space, even RIPE Chair Hans Petter Holen had some concerns because his own software company, he said, was acquiring companies from time to time. Handing back in use address space obviously would result in the need for renumbering. Van Mook did answer by pointing out that companies needed to keep open the exiting, payed LIR status – which in turn just re-introduces the problem of several memberships/ multiple company ownerships.

Contradictory decision on the administrative side

While for the policy side, the RIPE community had no agreement to go for either of the policies – closing down or opening up the last /8 – with a majority of speakers favouring a conservative preservation strategy, on the administrative side the RIPE membership went in the opposite direction.

After considerable debate during the General Meeting in Copenhagen, RIPE members decided to lift the ban for multiple memberships by individual RIPE members – thereby allowing a renewal of the trend of an explosive growth of membership numbers. Those numbers have gone up to around 14,000 by now – with 2,000 new members between May 2015 and May 2016 alone. In December the Executive Board of the RIPE NCC had put a preliminary stop to the possibility to hold multiple memberships. With the current lift, members can again go ahead and create new memberships and fetch additional /22 last mile allocations.

Reactions after the decision of the RIPE members were mixed. RIPE Chair Hans Petter Holen called it plainly “wrong”. “It is certainly not in the sense of the wider community”, said Holen. RIPE NCC CEO Axel Pawlik said that efforts to preserve the last IPv4 space were thwarted anyway. During the brief phase of banned multiple memberships members had gone over to open new companies instead. Those interested in fetching more of the last IPv4 resources would react with creative ways to go around new policies, he predicted.

On the other hand, once the last IPv4 addresses of RIPE were allocated, people would just have to turn to the market if they needed the old addresses and calculated the IP addresses into their business plans in the same way as routers or other hard- and software. Currently an IPv4 address costs around $10 USD per address – a /22 therefore would be $1,000 USD.

The question of when RIPE NCC will be allocating the last IPv4 depends highly on how liberal the addresses will be handed out – with the possibility of multiple memberships re-established, the burning rate might go up again. While most recent calculations were up to 6 to 7 years, with the ever fastening run for new memberships, the stretch run would be shorter, said Address Policy WG Chair Doering (SpaceNet) after the meeting. To compare: ARIN has already run out of IPv4 addresses last August and APNIC is getting close.

Working Groups and Plenary Bits

DNS WG

DNSSEC – Change of ZSK and KSK, and algorithm flexibilities

Both the algorithm change for the DNSSEC Zone Signing Key and the DNSSEC Key Signing Key for the root zone were discussed during the DNS WG. The ZSK algorithm change is already underway with Verisign as ZSK operator having decided on the change based, according to Wessels, on a recommendation from NIST. Contrary to the KSK change which has been discussed several times and been developed by a design team, there has not been prior public consultation on the ZSK change.

Wessels detailed the scheduling on of the ZSK change, pointing out that ICANN and Verisign had been working closely together to avoid interference between the two rolls. Testing between root maintainer and the Post IANA Transition operator-hopeful has already been done. The timetable looks like this:

- 2016-04-15 Testing between ICANN and Verisign (completed)
- 2016-05-12 KSK ceremony #25; sign 2016Q3 ZSKs (completed)
- 2016-08-11 KSK ceremony #26; sign 2016Q4 ZSKs
- 2016-09-20 First 2048-bit ZSK pre-published in root zone
- 2016-10-01 Root zone signed with 2048-bit ZSK

During the 25th KSK ceremony (that produced the 2016 Q3 keys ZSKs) the 2048 key was already signed, it will first go to the root on September 20 for prepublication (about 10 days). On 1 October, a root zone which has been signed by the larger key will be available. The post-publication of the older (shorter) ZSK key will be longer than usual (in case a fall-back becomes necessary).

While the change to the larger key is expected by the experts to go unnoticed, there are some concerns about the growing length of DNS responses, especially during the 10 days of pre-publishing and post-publishing, during which new and old ZSK are both live.

According to Wessels, size will go up from 736 octets (single 1024 bit key, ZSK) and 883 (normal 1024 to 1024 ZSK roll-over) to 1011 octets (1024 to 2048 transition) and 1139 (two keys 2048 ZSK). A similar effect would be reached, if there was a KSK roll-over with 2048 bit KSK and 2048 bit ZSK reaching the size of 1139 octets.

Tests undertaken by Verisign during February 24 (22:00 Uhr UTC – 22:10, 40,993,338 IP packets captured, 37,494,153 DNS UDP queries captured) resulted in no fragmentation (only for any queries). Truncation on the other hand rose, for DNSKey responses from 2,5 to 5.5 (single 1024 bit key to up to 5 .5% for 1024-1024 as well as 1024-2048 and 2048-2048). Truncation for all responses depends on the size of the key that used for signing. The normal level is about half a percent of all responses, after signing with larger key it goes up to about 1.4%. Also there the need for bandwidth for the root servers would rise according from 250 mbit/s to 350 mbit/s.

In case problems would arise during the introduction of the larger keys, Verisign was prepared to fall-back to the older 1024-bit key in October. Wessels recommended to operators to test their servers to be prepared for the change.

KSK roll after ZSK roll is done

As the larger KSK will add size, ICANN intends to wait with the change from the 1024-2048 roll until the ZSK change to the larger algorithm has been completed. Paul Hofmann, ICANN, said: “We want to make sure that the 2048 bit ZSK has worked just fine”. More details on the KSK algorithm change would be made available for public review soon (in addition to the document from the design team), he said. ICANN would also provide for a “fall-back”, “roll back” or “back-out”. Hofmann said that looking through

the process, “we have found some interesting stuff already and so we are hoping to flush that out soon.”

Answering questions for the need to change to the larger algorithms, Hofmann pointed out that to push DANE was one reason to go ahead, as there was no possibility to use DANE in browsers because browser vendors argued that given the update to 2048 bit for CA signatures they would not consider DANE until both the keys were upgraded to 2048 bit as well.

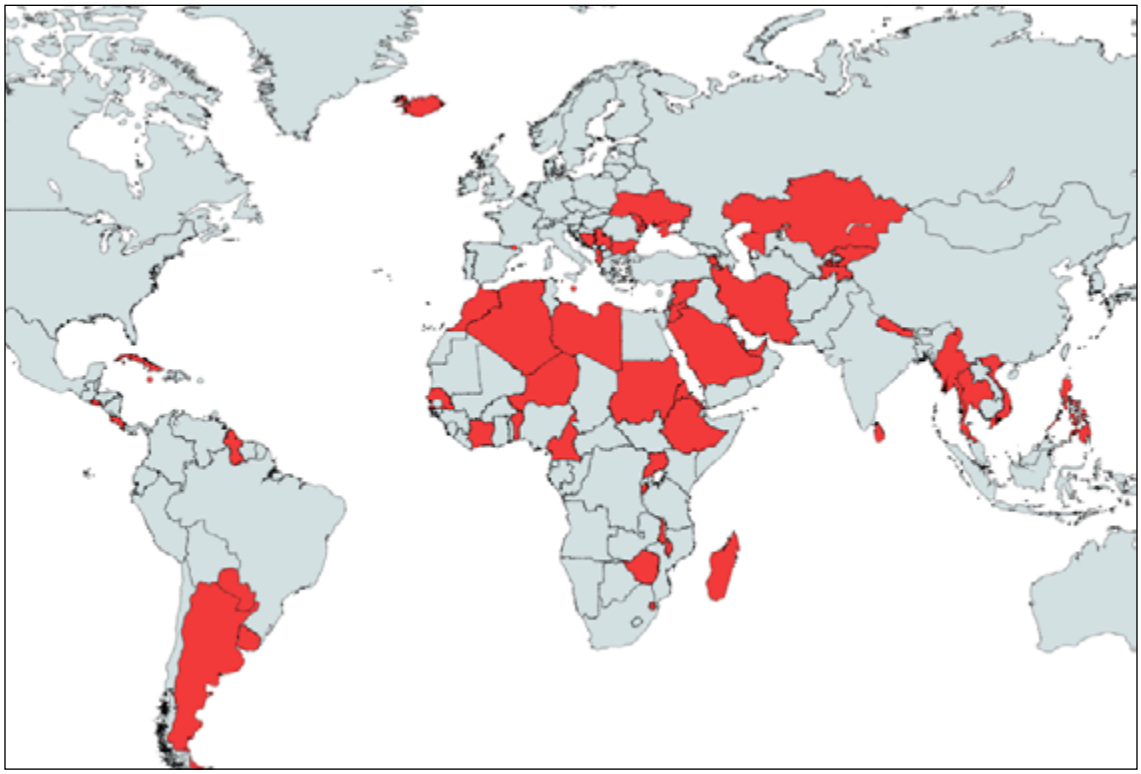
Anand Buddhdev reported about an algorithm change for ripe.net RIPE’s reverse zones from SHA-1 to SHA-2, SHA-2-56. The roll was performed in November 2015, with no validation failures. During the algorithm roll-over the RIPE NCC team had discovered several issues, though, for example older unbound versions had not been able to validate.

On general problems when introducing DNSSEC Paul Ebersman (Comcast) gave an in-depth presentation from introducing DNSSEC validating and signing, drawing the conclusions that:

- automation for signing was no option, but indispensable
- starting with validation made sense (easy to implement, even one paid a little for others’ failures)
- failure rates were getting better (2 dozen failures/month were a bad, even .gov was getting better)
- one step when preparing to validate was to get contacts at .mil, .gov
- it helped preventing cache poisoning
- DANE was already used for email at Comcast
- mistrust toward a single root for key made no sense as “we are already trust root servers/ICANN”)
- Customers were starting to expect security of DNSSEC

Implementing policy on DNS secondary services

In its regular DNS update Anand Buddhdev reported about the start of withdrawal of RIPE NCC service to provide DNS secondary servers to smaller TLDs. RIPE NCC is implementing the new policy (RIPE-663), that sets certain conditions for eligibility to receive the services. RIPE NCC currently checks all ccTLDs that receive the service. One candidate pre-empted the RIPE NCC check and migrated their servers away. 77 ccTLDs currently have RIPE NCC hosted secondaries, but according to Buddhdev, some will lose the service over the coming months.



BIND 9.11

After stopping the development of BIND 10 ISC is now offering BIND 9.11 which will be supported alongside BIND 9.10. Earlier versions would not be supported anymore, said Victoria Risk from ISC who presented a release update for 9.11 which was announced to be available in a third alpha version with all features completed starting 1 June. The requirements for 9.11 were:

- a standardised provisioning mechanism that didn't require users to maintain scripts
- faster zone deletion from the new zone file
- faster updates in general
- limit the number of notifies, or at least a configurable option to do that
- database option: catalogue zones (only implemented back end at the moment Red Hat), for catalogue zones there an IETF draft is in the making

The long list of features (see here) includes DNSSEC automation using a DNSSEC key manager utility (Python script) and a positive IPv6 bias (with addition of 50 millisecond advantage or head start for the IPv6 address assuming that both are available).

Major work of the somewhat reshuffled ISC team at the same time had gone to regular maintenance, in 2015 four regular maintenance releases were published, 12 security patches, two experimental releases for the resolver DDoS mitigation feature. According to Risk, a total of 486 issues had been resolved.

BIND Yeti Server?

There was also a request for RIPE NCC to run a Yeti server. Yeti is an alternative DNS service that sees itself as a testing ground for new developments (DNSSEC, Key roll-over, etc.). It is based on the legacy DNS root service (contrary to various alternative DNS services like open root or the like) and is up and running (see here).

Cooperation WG

The Cooperation WG had a highly interesting discussion with Jan Scholte, Professor at the University of Gothenburg on the much belaboured concepts of multistakeholderism and bottom-up governance. While Scholte in his research found that the IANA transition consultation processes had displayed an unprecedented richness in developing joint standards for the future IANA (and had done so in a short time), he questioned the religion-like status of multistakeholderism and bottom-up approach. There was "promise and worry" in the new concepts, he said, regarding the lack of geopolitical bottom-up, lack of bottom-up in social terms in terms of class, race, gender, age and so on, and lack of cultural diversity.

Challenges he observed during the IANA transition debates included:

- need for incredible investment of time and energy to figure out constant changes
- navigating the labyrinth, lack of resources to go to the different relevant fora
  dominance of a main culture at the expense of cultural diversity
  duplication and inefficiency (with many more fora dealing with the same issues)
- difficulty to enforce compliance (dependence on legitimacy)
- special interest capture is a problem (who represents whom?)
- accountability of the stakeholder unresolved (only to be addressed in work stream 2)

Scholte recommended in the end to resist the ideology of bottom-up and view multistakeholderism as "a political space" and a "place of power hierarchies like anywhere else". A possibly unintended illustration of Scholte's point on the difficulty of stakeholder representation was made by Chris Buckridge, RIPE NCC. With more and more seats to be filled at the tables of various UN (or other intergovernmental) ventures there was a need to tap on a larger pool of technical experts and also to make selection processes more transparent, he said.

The new platform http://www.internetcollaboration.org/ shall allow for transparency and also nomination/self-nomination on specific calls going forward. If there was funding for volunteers from the operators' community to take-on future roles had to be checked on case-by-case, said Buckridge.

The contrast of multi-stakeholder acknowledgment by many governments and the reality of legislation was illustrated by the presentation of Jesper Lund,

from EDRI member IT-Political Association of Denmark. The 250 member civil rights organization campaigns for Internet privacy and civil liberties online in general. As an example for controversial regulation/legislation Lund pointed to mandatory data retention which despite being declared unconstitutional by the European Court of Justice has been reintroduced in many EU member states and is also still pushed by the Ministry of the Interior in Denmark (despite an acknowledged lack of efficiency between 2007 and 2014).

The Cooperation WG has developed into a platform to discuss studies on Internet politics and governance, the bridging function between RIPE community and governments/regulators has become less important. Currently there is a discussion on the mailing list about the purpose of the WG. Some participants expect a push for the WG from the selection of two additional new Co-Chairs. Candidates to join Co-Chair Meredith Witthaker, Google, are:

- Achilleas Kemos – European Commission's DG CONNECT
- Collin Anderson – Network Researcher and Internet Policy enthusiast
- Analina Aspis – Lawyer and Researcher at the Law Research Institute Ambrosio Gioja
- Johan Helsingius – Co-founder of Bits of Freedom, Member of the Board, BaseN Networks Oy, Helsinki, Finland, Member of ICANN GNSO Council (Nominating Committee appointee to Non-Contracted Parties House)

Anti-Abuse WG

The Anti-Abuse WG had a fierce debate about an extension of the Abuse-C Policy – introduced for RIPE resource holders in 2012 (https://www.ripe.net/publications/docs/ripe-563) – to legacy resource holders. Despite the attempt by the proponent Piotr Strzyżewski to address concerns raised after the publication of the policy in January by making abuse-c entrances in the database mandatory only when data on legacy resources is changed in the database, the policy is broadly rejected (https://www.ripe.net/participate/policies/proposals/2016-01).

Most opponents question the effectiveness of the measure. Lack of documentation about the functioning was said to be a problem for the original policy in the first place. Some argue that the policy could even be harmful because data put into the database to "tick the box" could be misleading. From a legal standpoint, many opponents also point out that legacy holders are not governed by RIPE policies in the same way as RIPE resource holders. With objections clearly in the majority, the policy could not be advanced just as is.

RIPE NCC interactions with law enforcement agencies (LEA)

Former Serious Organized Crime Agency/Europol "Cop" Richard Leaning has joined RIPE NCC as a consultant on LEA and Government Internet Governance issues. Leaning presented the report on RIPE's interactions with LEAs, especially Interpol's Global Cybercrime Expert Group (IGCEG),

Spanish Guardia Civil, Europol EC3, (Joint Cyber Action Taskforce (J-CAT) and DG Home, and DG CONNECT. RIPE NCC staff is engaged in trainings on the functioning of the RIPE Database or has advisory roles (J-CAT, EU Commission). In 2015 there were a total of eight LEA requests: three for publicly available information, two for non-public data and three for information RIPE NCC did not have. Four of the eight 2015 requests were from the US.

Gregory Mounier (E3C) presented the problems LEA officers faced when trying to locate users of IP addresses, due to cross-border nature of the IP address use. As Mlat requests were too slow when tracking an address from a Romanian ISP to a France company and finally to a German user, Mounier asked, "how can we ensure that IP addresses are announced in the country where they are actually registered, and can the RIPE database reflect the location of an ISP handling an IP address?"

RIPE Administrativa

Major decisions of the General Meeting include the retaining of the current fee structure for RIPE members. Nigel Titley and Remco van Mook were re-elected for the RIPE NCC Executive Board.

RIPE CTO Daniel Karrenberg called on members to dig for the "gold" in RIPE Atlas. The project which is coming close to having its 10,000th probe connected, is currently being used for 290,000 measurement projects.

The next RIPE meeting will take place in Madrid on 24-28 October 2016.

CENTR is the association of European country code top-level domain (ccTLD) registries, such as .de for Germany or .si for Slovenia. CENTR currently counts 53 full and 9 associate members – together, they are responsible for over 80% of all registered domain names worldwide. The objectives of CENTR are to promote and participate in the development of high standards and best practices among ccTLD registries.

CENTR vzw/asbl
Belliardstraat 20 (6th floor)
1040 Brussels, Belgium
Tel: +32 2 627 5550
Fax: +32 2 627 5559
secretariat@centr.org
www.centr.org

To keep up-to-date with CENTR activities and reports, follow us on Twitter, Facebook or LinkedIn