Council of European National Top Level Domain Registries

Report on RIPE 68 Warsaw

12 - 14 May 2014

Table of Contents

RIPE turns 25

A handful of network operators met May, 19th 1989 for the first RIPE meeting. During RIPE 68 at Warsaw the IP Address Registry for Europe and the Middle East, which is the oldest of the five IP registries, celebrated its 25th birthday.

In a dedicated session outgoing RIPE Chair Rob Blokzijl, Internet "father" Vint Cerf and APNIC Chief Scientist Geoff Huston congratulated the community for what many see as a success model of self-governance. Huston recollected that listening to Blokzijl and Karrenberg requesting that Europe should manage its own IP address space in the late 80s, he thought that "this was cool".

Both Huston and Blokzijl reminded the record number of participants (568) and the so called protocol wars that were still ongoing during the time of RIPE 1 – RIPE's first members were called "Amsterdam Bandits". Meanwhile, the Amsterdam bandits had won against the telco model, even telephony was just another IP service by now. But now the winners themselves had become the problem, Huston said in his speech.

"Is this a fight with the ITU-T anymore? Is this a fight about Internet governance anymore? Or is it us? Because I strongly think that even then, when we were fighting the OSI wars, it was over. It was us. (….) We are the problem. And the issue is, the dream is not always that good. Because what we are doing to ourselves is bizarre. We are the problem. Examining every little thing we do is now what we do out there on the Internet, and that is something that we really need to worry about."

To continue the success story according to Huston responsible technology was needed, a cautious call to re-consider pervasive monitoring which has paved the way for pervasive surveillance. Huston in a later talk (in the DNS WG) clearly pointed out how an offer like Google's public DNS helped one big player like Google to accumulate knowledge about the whereabouts and whatabouts of individuals on the Internet.

Since last December, according to Huston's statistics, DNS queries made via Google public DNS servers grew from 10 to 16 percent globally. If every sixth DNS query was going to Google, the company was able to know everything everybody did on the Internet, as these queries were preceding and initiating any conversations and actions of users. Warren Kumari from Google underlined, Google had committed itself in its privacy policy to not analyze this traffic.

"Google might collect all sorts of information from users. The one place where I would encourage people to go and read the Google public DNS privacy stuff. The one place where we don't or one of the places where we don't, is from this. I realize that proving that is improbable but I just wanted to mention it again."(...)We do many creepy things, just not there."

Changes to RIPE

Blokzijl who has officially stepped down in Warsaw from his position as RIPE Chair after 25 years in his birthday speech explained the changes experienced since 1989. From the tiny beginnings, a handful of academic operators, a routing table that fit on one page for all Europe, with no BGP at hand and a still hostile OSI/telco world around RIPE now has grown to over 10.000 members, mostly companies.

RIPE is still growing thanks to the fact that new members can get their /22 of IPv4 addresses from the running out /8 pool. In 1992 the RIPE NCC was established to carry on the operational day-to-day work. IP has, as Huston put it, won the war and is the protocol, the migration to IPv6 was said by Vint Cerf in his birthday speech to be one of two major challenges lying ahead of the organization.

The migration from scarce IPv4 to abundant IPv4 at the same time is triggering changes of RIPE and the work of RIPE NCC in particular. Instead of developing policies for fair distribution of the scarce addresses and establishing the processes for it, with IPv6, the first allocation for most RIPE members will also be their last, Blokzijl said, just because the amount of addresses handed out was so enormous.

Instead education and the exchange of information would become more important. RIPE meetings now try to attract interesting speakers and topics for its multi-day plenaries, feedback by the audience is encouraged by offering prices. A related initiative, which intends mainly to bring more academics to RIPE meetings is RACI, RIPE Academic Cooperation Initiative. Seven academics from all over the RIPE region were awarded tickets to come and present their research in Warsaw

Operators and politics

Outreach and representation of the community in Internet governance also has become more and more important, even if this activities seem to receive a split reception by RIPE members attending the meetings. While expert panels and NCC official reports about the developments do take more time (in Warsaw there were a panel on Internet Governance, reports on Internet Governance activities in the Cooperation WG and NCC services, and an IANA discussion in the DNS WG).

During the IG panel Shane Kerr expressed some of the qualms in the operational and technical community over the "governance" topic, saying that traditionally the community wanted to stay as far as possible away from governance and governments. Leaving RIPE Chair Rob Blokzijl, who has been skeptical of linking IP address management to politics, once more joked that Multi-Stakeholderism surely was the "right word for this internet governance discussion", because of the richness of its meanings – as 4736 correct English words could be made out of its letters.

While there still are those, hoping RIPE would focus on IP-address management and on some tasks with regard to the DNS, certainly RIPE NCC has dived into the governance space, together with the Number Resource Organization (NRO) and as part of the much more "governance"-active technical community. Having a Director External Relations in Paul Rendek, who is residing in Dubai, and linking RIPE to the Arabic countries, perhaps best illustrates RIPE's (or the RIPE NCC's) strategy to play in the IG arena.

New Faces, Female Board Members

There has also been quite some change in the RIPE leadership at this meeting. Not only is Rob Blokzijl stepping down handing over to Hans Petter Holen, who joined RIPE 20 years ago from Nordunet and has been representing RIPE in the ICANN Address Council since its establishment in 1999. Holen is a Board member of a number of Norwegian Companies (Visma Personnel AS, Bøndenes Hus AS).

Also, for the first time two women have been elected to the RIPE NCC Executive Board, former Swedish GAC member Maria Hall, now SUNET, and Salam Yamout, National ICT Strategy Coordinator at the Lebanese Presidency of the Council of Ministers.

Also elected was Christian Kaufmann, Akamai for a second term. Together with the EC-members Nigel Titley (May 2016), Remco van Mook (May 2016) and Dmitry Burkov (May 2015) the Board now has six instead of five members, following a decision by the GM to add one seat.

A change for RIPE's future certainly will be the creation of processes to elect/select future WG chairs and also a future sucessor for Hans Petter Holen. Holen himself had just been named by Blokzijl in a rather "shirtsleeve way". Holen had been chairing the address policy WG between 1998 and 2007.

Governance Issues

A panel discussion on Internet Governance Panel tried the impossible: to give an overview not only over recent and upcoming conferences (starting way back from WCIT up to NetMundial), but also about venues like one.net and the IANA transition discussion as well.

Reception of NetMundial by panelists was positive in general. The panel welcomed the support for multistakeholder and equal footing in the NetMundial final document. Arkko pointed to some desiderata: net neutrality, protection from liability for intermediaries. Former IAB Chair Olaf Kolkman described Netmundial's commitment to multi-stakeholder model for internet governance as the one alternative to a multi-lateral governance, and certainly the one preferred by the technical community.

NetMundial did not however seal the success of multi-stakeholder, instead, Phil Rushton (British Telecom) said that governments who met in the CSTD Working Group on Enhanced Cooperation (WGEC) after NetMundial refered to it as "yesterday's meeting" while at the same time putting their foot down on the role of governments (see the editorial post by Avri Doria on this here). Victor Milashevsky, Advisor to the Russian Minister of Communications underlined during the RIPE meeting that, the role of governments as the defender of citizens' rights had to be recognized in Internet Governance (see below, Cooperation).
). Victor Milashevsky, Advisor to the Russian Minister of Communications underlined during the RIPE meeting that, the role of governments as the defender of citizens' rights had to be recognized in Internet Governance (see below, Cooperation).

Netnod's Outreach and Communication Manager, Nurani Nimpuno, said organizing representation of the technical and operational community in the IG landscape, especially in UN events, was still a challenge. Patrik Fältström reacted to the question of how to deal with anti-multi-stakeholder government moves (like in Russia by

Post-Snowden Call by IETF Chair to RIPE community

Jari Arkko gave an update one the ongoing work on better security and privacy considerations in IETF standards, including new versions of HTML and TLS, HTML 2.0 and TLS 1.3. Arkko pointed to the just published Best Current Practice RFC 7258, published just ahead of the RIPE meeting which is summarized:

> *"Pervasive monitoring is a technical attack that should be mitigated in the design of IETF protocols, where possible."*

Discussion had taken longer than expected, Arkko reported. Obviously there were concerns about the RFC getting to much into the "politics" space, despite it not touching on any "motivations" for monitoring. Other arguments against the document were privacy cost and complexity privacy could add.

Measures envisaged in 7258 are:

1. revisiting of the security of existing protocols, (page see here)
2. an obligation to consider how a protocol enables or disables pervasive monitoring

While Arkko said, in his opinion the NSA program Bullrun – intentional weakening of the security of standards – had not been effective, the IETF should see itself as part of the problem and part of the solution. The IETF chair listed ongoing work on

1. HTML 2 – no mandatory encryption, but trend by big browser vendors to turn it on
2. TLS 1.3
3. New WG: Using TLS in applications (UTA) – BCPs for TLS in applications
4. DNS privacy work – Snowden's revelations triggered also a data minimization debate
5. BoF on TCPcrypt

Given the developments and the "inflection point" for some of the technology and the whole net moving toward the web model now was a good time for change, Arkko summarized. Arkko and Chris Grundemann both appealed to operators to participate in IETF or at least review drafts to integrate operative concerns (ISOC is doing a survey on operator participation in the IETF, see here).

IANA transition or NTIA transition?

Being served with IP address blocks from the global pool of IP addresses and AS numbers by IANA the IP address community, including RIPE, is directly affected by the envisaged change of oversight over the IANA function. Given that for the RIRs the question of who will take over the oversight rule from the NTIA is vital, the time allocated to discuss the issue during RIPE 68 seemed rather limited. During the Internet Governance Panel it was not the main topic, and the focus was much more on the governance landscape in particular. A dedicated slot in the Coordination WG – one might wonder why it had been put there instead of the plenary – did not offer a lot of discussion time.

The RIRs certainly have considered transition of the IP-address function years before (request have been made as far back as the ICANN meeting in Shanghai 2002) and Paul Rendek reiterated the line of thought: "We already thought that the oversight function of the US Government could have walked away. We actually wanted to remove that." The important question for the RIRs was "what will this oversight look like if the US Government is to walk away from this?" Accountability of the IP address distribution process, according to Rendek was very much in place with the policy processes. Still the community had to be ready to make their case in the transition debate, Patrik Fältström warned.

In one first step the NRO in a statement on ICANN's draft proposal of the principles and the process to develop a proposal to transition NTIA's stewardship of the IANA function sided with the Internet Architecture Board (IAB) requesting that each of the three communities (numbers, names, protocols) "be offered the primary responsibility to produce respective transition plans, in accordance both with their own established processes, and with the defined scope, principles and mechanisms". The open questions for RIPE according to Chris Buckridge, RIPE NCC, were, how multi-stakeholder oversight would be, how the RIR communities would fit in future oversight model and what the new model would mean for community processes.

One major issue discussed during the short debate in the Cooperation WG was related to the relevance of future IANA oversight for the RIRs. As the oversight function on the numbers part had been "empty" and RIPE/RIPE NCC had "never met NTIA" there was no need to consider any new structure, outgoing Chair Rob Blokzijl said. Daniel Karrenberg, RIPE NCC Scientist specified, processes as requested in the NTIA announcement, were in place at the RIPE and only a minor global registry was necessary, which could, if a plan b would be necessary, organized by the RIRs themselves. Documentation of the RIPE processes to illustrate their openness, accessibility and transparency might be needed, alongside the statement of the RIRs. Malcolm Hutty, LINX and also EuroISPA, on the other hand warned that oversight while not needed to oversee RIR self-governing number policy processes and operations was necessary to protect the latter against outside interference.

> *On the DNS side of the house, policy is determined within the ICANN community and imposed through registry agreements and registrar agreements on the registries and registrars and then through them, out to the end users (…).*
> *Now we don't work that way. We determine our own policies here, but it may not continue that way, it's not guaranteed, it's possible that ICANN might decide it wants to start developing policies for the conditions for getting address space, for the requirements that LIRs should have, to impose upon people that get address space.(...)*
> *This function, this oversight function, is an external check on ICANN that prevents ICANN from changing its mind about whether we get to set our policies or not. I would argue that it is very much in our interest to say that there needs to be a credible and effective external mechanism that continues to protect our right to set our own policies.*

Another issue brought up was how far the RIPE NCC should go in consulting a broader (than RIPE) community. Paul Rendek had proposed to consult at regional RIPE meetings, events like MENOG or ENOG. Daniel Karrenberg, also RIPE NCC, recommended to keep the consultation focused and located at the RIPE Cooperation WG.

According to Paul Rendek, a draft statement prepared by the RIPE NCC should be

prepared for RIPE 69 in London, to allow further consultation and finalize the RIR input into a joint proposal by spring 2015.

Open Hardware, open crypto

"If you can't hack it, you don't control it" - several projects were presented during the RIPE meeting that try to hack hardware and, to a lesser extent, crypto, to allow for taking back control over devices and settings.
Randy Bush, Internet Initiative Japan, promoted Cryptech, a project Bush described as initiated by IETF and IAB leaders, together with TOR developers. The IETF/IAB push according to Bush results from a declared need to give people better security for creating DNSSEC, RPKI or other key material, the TOR crowd is looking for open hardware end user devices like the open laptop (Novena "Bunnie" laptop). Said Bush:

> *"All of the stuff for key storage is relying on hardware security modules that are designed and made by people who work indirectly or directly for the United States governments, the Israelis or Chinese. Do you want to trust those? I don't."*

The declared goal is to produce

> *"an Open Source reference design".*

Funding for the development of SUNET, SURFNET, NORDUNET and the ISOC so far. Bush talked to several NICs at Warsaw searching for additional sponsors. He gave brief review of the first running code, versions of Sha1, Sha256, Sha512, during the Cooperation WG and the closing plenary. Works on a "true random number generator" also is underway. All work was presented at the Cryptech site, reviews are encouraged. Transparency and openness in funding ("no hidden funding") and diversity (core group of six includes a Russian crypto expert to provide Gost encryption variant) would be key, Bush promised. Problems to be tackled by the group were preventing the tampering via side channels as well as ensuring that those who use the design and cryptech-chip label ensure no manipulation takes place during shipment. Openly available tests for the users would be a good thing, said Aaron Kaplan, from Nic.at.

Better Crypto

Kaplan presented the "Better Crypto" initiative, which he described as an open review process for crypto settings addressing operators in the first place. In the BetterCrypto draft white paper the initiative, which has been prepared mainly by Austrian experts so far, put together recommendations on what ciphers and what key-length could be considered as reasonably secure for various web servers (Apache, ngix and others), mail servers (Postfix, Exim, Dovecut), data bases (like Mysql,Oracle etc) ,virtual private networks (Open VPN, IPSec, etc). The basic idea was, Kaplan described, to provide "easy to copy and past"-setting for administrators. What was critical was review by as many people as possible, and, as Kaplan noted, also some level of agility to react to new developments and revelations. Standardization of crypto agility is being proposed at the Internet Engineering Task Force currently.

Own your hardware - Turris router

Another project of open hardware presented during RIPE 68 was Turris, an open source hardware router (attached to a central Turris server) designed and built by the Czech registry cz.nic. As part of the initiative to share responsibility for security between operators and users, the researchers at the cz.nic labs found that no commercially available home routers was supporting IPv6, DNSSEC well and was also capable to support the planned monitoring functions.

The Turris router, based on openWRT has been built in Austria and the Czech republic (PCB prototype is from Cube, final batch AT&S (Leoben) PCB assembly and testing Certuma, metal cases from Emko. It allows users (a representative sample of Czech Internet users is chosen by the CZ.nic) to also route devices or smart objects in their homes.

A Turris central server collects data on anomalies, vulnerabilities or attacks, filtering lists and updates provided via the central server are optional to users). Trust in the monitoring provider is an issue of the concept, as it stores data from the Turris home routers.

The registry does not plan to make this a commercial project, and will not sell the router to interested parties outside of the Czech republic, as the device has been heavily subsidized to allow handing it out for a symbolic 1 Krona (production cost are around 300 Euro because of the limited number). Commercial providers could use the design, as it was open. One network provider supporting the Turris project is Comcast.

DNS - DDOS Mitigation

DdoS and amplification attacks were once more the topic of DNS related talks, in the plenary and the DNS WG sessions. An interesting overview over protocols vulnerable to amplification was presented by researcher Christian Rossow, Amsterdam University. Rossow listed 14 UDP based protocols, allowing for in some cases considerable amplification factors. For NTP for example he stated a potential factor of 4000 for bandwidth amplification (BAF, compared to a factor of 10 for packet amplification, PAF). NTP, he said, was the worst protocol tested with regard to amplification. At the same time, mitigation seems considerably easy. Within seven weeks after publication of the recommendation to disable or filter monlist (an NTP optional feature) the number of vulnerable servers came down to 8 percent.

For a full list of network, legacy, p2p and gaming protocols see Rossow's statistics below:

	BAF			PAF	
Protocol	*all*	50%	10%	*all*	Scenario
SNMP v2	6.3	8.6	11.3	1.00	*GetBulk* request
NTP	556.9	1083.2	4670.0	10.61	Request "monlist" statistics
DNS_{NS}	54.6	76.7	98.3	2.08	ANY lookup at author. NS
DNS_{OR}	28.7	41.2	64.1	1.32	ANY lookup at open resolv.
NetBios	3.8	4.5	4.9	1.00	Name resolution
SSDP	30.8	40.4	75.9	9.92	*SEARCH* request
CharGen	358.8	n/a	n/a	1.00	Character generation request
QOTD	140.3	n/a	n/a	1.00	Quote request
BitTorrent	3.8	5.3	10.3	1.58	File search
Kad	16.3	21.5	22.7	1.00	Peer list exchange
Quake 3	63.9	74.9	82.8	1.01	Server info exchange
Steam	5.5	6.9	14.7	1.12	Server info exchange
ZAv2	36.0	36.6	41.1	1.02	Peer list and cmd exchange
Sality	37.3	37.9	38.4	1.00	URL list exchange
Gameover	45.4	45.9	46.2	5.39	Peer and proxy exchange

With regard to the defense, Rossow re-iterated to implementation of BCP 38 and closing open resolvers. Rate limiting according to him was less effective, because it only made a change for a fraction of servers, he said. More measures included the NTP monlist filtering and implementing proper handshakes (fall back to TCP).

Standardizing monitoring

As the demand for DNS monitoring data increases, several DNS companies have started to consider how to "standardize" the efforts. Lars Johan Liman, Netnod, reported about ongoing talks at his company and Bind operator ISC alike. Currently there was no common agreement about what statistics should be collected and in what form they could be exchanged. An exchange of ideas took place at the OARC meeting preceding RIPE 68, and a Wiki page has been formed to help ongoing discussions. A document currently prepared by the route server advisory committee could become another base-line for discussion, Liman said during the DNS WG session (wiki-page announced here).

Liman did not touch the issue of an advisory body for the RSSAC during the DNS session, which he had said he intended to do.

A working party of the DNS WG has prepared a mechanism to formalize the provision of secondary DNS services for ccTLD operators on the table. RIPE will continue to provide secondaries for smaller (poor) ccTLDs, but listed some limitations and conditions for such services:

- it will only be available for smaller ccTLDs or their IDN-versions (around 10.000 registrations)
- some things have been made triggers of an exclusion of service (for example if the ccTLD already uses a commercial provider for secondaries)

In a letter exchange a deadline will be set for the service, with extensions possible after review.
There were no changes to the proposal by the WG.

Anand Buddhdev, RIPE NCC, reported about the introduction of diversity in the name server software for RIPE's authoritative name server services (currently only the BIND 9 is used). After considering Bind 10, Yadifa, Nominum, Knot DNS and NSD the latter two were chosen as a first addition.

A talk on censorship in Turkey by Stephan Bortzmeyer is covered together with the a filtering and blocking special presented in the Cooperation WG (see below).

The Cooperation WG gets their hands „dirty" with politics

For the first time the Cooperation WG had two sessions and an agenda packed with the rather policy-oriented topics: censorship, walled internet, and a rather diplomacy-like exchange with the advisor of the Russian Minister of Communications and Mass Media, Igor Milashevsky. The Cooperation WG now is chaired by Alain van Gaever, Principle Advisor Ofcom, (former Google employee and European Commission official) , by Maria Hall, SUNET, (former Swedish Government) and Meredith Whittaker, Google Program Manager Research. The Cooperation WG once more attracted only about half a dozen government/administration representatives (namely from Poland, the Czech Republic, Russia, Finland, Germany and Oman).

Content filtering - from blocking to hijacking the routes

The Cooperation WG dedicated its first slot completely to content blocking and the circumventing of such blocking. Quite a lot of analysis has gone into various attempts by governments to filter and block content, Olaf Kolkman presented a short version of a nice overview prepared by Italian SysAdmin and network expert Pier Carlo Chiodi also pointing to an draft informational RFC on blocking emanating from work done at the IAB. The latter classifies network-based, rendevous-based and endpoint-based blocking. Endpoint-based blocking (at the source), often not chosen by administrations/prosecutors because of limitations of control by the entity that wants to block access, is described as the most targeted and least harmful with regard to overblocking and security risks like for example the breakage of DNSSEC or attempts to route around blocks via open resolvers.
While the presentation and papers clearly make the case about the cost of filtering one might have wished more attendance from the target audience, namely public authorities, than it had at the Warsaw meeting.

An in-depth analysis of escalated filtering/blocking measures ordered by the Turkish government in March and April was presented during the DNS WG by Stephane Bortzmeyer (AFNIC). Bortzmeyer reconstructed the cat-and-mouse like battle between the Turkish authorities blocking Twitter by obliging Internet Access providers to hand out false answers to DNS-queries for Twitter.com.

When users switched to Google's public DNS resolvers (8.8.8.8) Turkish authorities compelled providers first to block access to 8.8.8.8 and, according to Bortzmeyer on March 29, to inject false routes for the Google resolvers. Users were redirected to the DNS services of incumbent Turkish Telecom, more specifically to 195.175.254.2. Bortzmeyer concluded that this was a new step. The Turkish authorities have gone from simple censorship to the hijacking of IP routes.

In the remaining two talks of the Blocking/Filtering slot of the DNS WG, Walid Al-Saqaf, a media researcher from Yemen, and Eric Wustrow, researcher at the University of Michigan, explained anti-censorship methods. Al-Saqaf after having his news site (yemenportal.net) blocked by the government in Yemen started to offer Alkasir. Alkasir, the arabic word for circumvention, allows users sending in reports about filtered sites to access these sites via SSH tunnels over a number of proxy servers.

A basic idea of Alkasir was to use information gathered via the users reports to analyse at which level (local ISP, national) blocking measures are taken. Users are encouraged to use the Alkasir server only for access to the blocked sites – Al-Saqaf had offered the service over his private server for some time, meanwhile he is working at a university As it was his private server, users had to commit to only use Alkasir for blocked content. Al-Saqaf meanwhile is doing research at Örebro University in Sweden and has just finalized his PHD about filtering in Arab countries. The thesis also correlated filtering events to political developments in various countries.

Wustrow presented the "Telex" concept as an alternative to the use of proxies. Proxying around censorship often resulted in a cat-and-mouse game with the censors. Telex instead, according to Wustrow, is based on Telex stations installed by ISP to redirect queries from their declared unblocked destinations to sites that are blocked. The real queries have to be reconstructed by the Telex stations using tags in the sent queries. In principle Telex stations do deep packet inspection to sent the queries off to the blocked

content, the Telex concept reads. Main problem of the service, which is now available in beta version form, is that ISPs have to be won as partners, and they must be trusted.

Russia@RIPE: Importance of government role

The VIP guest of the Cooperation Working Group, Igor Milashevsky, talked only in the second slot of the Cooperation WG. Expecting a panel discussion, Milashevsky obviously did not feel at ease while giving a short speech of rather general nature. The Russian politician while politely calling RIPE "a reference organization in the Internet governance system", underlined the need to restore confidence and trust by developing "international instruments and mechanisms to prohibit total surveillance".

Sticking to the recent Russian push for more government influence in Internet governance via some sort of international structure (ITU?), Milashevsky said, "state and governments are the main defender of freedom and security of the citizens." The role of governments therefore should be recognized. At the same time he declared limitations of freedom of expression as legitimate, as there was "no freedom without responsibility".

While Milashevsky clearly was a little nervous speaking at the operators' venue, the Russian politician was handled with RIPE unusual diplomatic care – either to not drive him away or because critics from Milashevsky's own region were concerned to put themselves on the radar of a Russian official.

Oh those politicians: Merkel's „Splinternet"

Milashevsky had not even to answer on the drive to "national Internets", that were described by Peter Koch (DENIC, but speaking personally for that talk) in a talk on "Walled Internets" or "Splinternets". Koch reported about an additional wave of walled gardens, this time not triggered by commercial operators closing in their customers, but triggered by knee-jerk post-Snowden reactions. The calls by high level politicians (German Chancellor Angela Merkel) to keep traffic local or at least inside Schengen (Schengen net) resulted, for example, in local email offers.

Koch here described two versions: the a little older DE-Mail, that worked with an overlay network for email using vetted entry points, but only hop-by-hop encryption, to allow malware detection. DE-Mail was not very successful so far. A Post-Snowden marketing product is Email made in Germany, that again offered what it called "secure" email, again using hop-by-hop encryption (using STARTTLS), but once more being dependent on vetted entry points, this time a "club" of major German email providers, namely Deutsche Telekom, 1&1 and FreeNet.

Koch appealed to operators and developers to much better explain the shortcomings and vulnerabilities of such club- or national models: cross-border traffic insecure, no end-to-end encryption, but trust placed on incumbent providers, lock-in of customers, and, worst of all, according to the expert a potential inertia to introduce standard solutions that make email end-to-end secure even where it crosses the club- or national borders.

Address Policy: Transfers/Validation and Privacy

Inter-RIR transfers are still under discussion in most of the RIRs (exception is APNIC which had been the first to run out). In RIPE Sandra Brown, IPv4 Market Group (an IPv4 address traders) re-tabled a policy for Inter-RIR transfers of IPv4 addresses.
With the debate on needs-based allocation resolved (according to 2013-3 the requirement for ex-ante documentation of need has been removed) a new attempt to create a RIPE policy for the Inter-RIR transfers of IPv4 addresses could be made, Brown said. It should allow the transfer of IPv4 addresses to and from other RIRs. It would be going to increase or supplement the pool of IPv4 addresses in the RIPE region and allow access to IPv4 resources from the other region.
Currently according to Brown only ARIN and APNIC have allowed transfers, and 34 transfers had been taken place between the two. The total number of transfers in the RIPE region was 342, the number within APNIC was 542, and the number within the ARIN region is 144. Lacnic and Afrinic still did have neither actual transfers, nor the policies, Brown reported.

Proof of identification and the necessary due diligence work requested of the RIPE NCC, potentially a hot topic, was discussed during Address Policy. A few resources holders have questioned the practice of RIPE NCC to ask for copies and potential storage of passports or national IDs. Athina Fragkouli, RIPE NCC, said RIPE NCC was looking into what has been stored. At the same time discussion about potential alternatives (PostIdent or other identification) was not conclusive.

During the NCC session RIPE NCC bolstered the need for identification and due diligence with a presentation on grown levels of hijacking of resources after the run out of regular IPv4 addresses.

Abuse WG - What if abuse is abused?

Bengt Gördén from Swedish ISP Resilans reported about considerable problems with anti-abuse activities that while fighting spam or alleged copyright infringement do not respond to complaints about mistakes, collateral damage by blacklisting or other issues. Gördén reported about the automatic sending of messages to anti-abuse messages, and the difficulties to get questions answered by the abuse-fighters. As an example, the city government of Gothenburg (194.71.226.0/24) was put on the blacklist by Spamhouse, yet the IP address block in question was not even routed. Gördén said the abuse work had become a problem in itself as it hurt customers, legal certainty about how to oblige the anti-abuse fighters to correct errors or mistakes was needed.

RIPE/RIR News

The RIPE General Meeting accepted, after some discussion the new charging scheme of 1600 Euro per member, plus 50 for each assignment. Legacy holders can either use the service of a LIR (which is cheaper, 50 Euro per assignment) or have a direct contract with RIPE NCC on their legacy resources. There was some dissatisfaction among participants that the legacy IP address charging would be relatively high (1600 per year, 2000 one time sign up, making it the same as members pay, yet the latter enjoy membership and voting rights). All votes see here.

RIPE 69 will take place in London, United Kingdom from 3 – 7 November, 2014