Report of the

RIPE 61

Rome, Italy,

November 15 - 19, 2010

Prepared by Monika Ermert
For the CENTR secretariat

Table of Contents

Highlights

End of Ipv4, future transfers and a registration policy?

Ipv4 is running out, really. It's generally expected by most that by March IANA will have no more Ipv4 blocks to assign to the RIRs, and some – in the RIPE's case two or three month later – there will be no blocks any more to be available for ISP and companies in the RIPE region. Alex Le Heux from the RIPE NCC said to this reporter that the end at IANA might come earlier, as he was expecting requests to IANA from APNIC and ARIN in only days, and with possibly four more /4 gone only two free blocks would be left before the pool comes down to the last five /8 from which each RIR then will receive one (according to the Global Policy for the Allocation of the Remaining Ipv4 Address Space (RIPE-436).

Running out in 2011

Depending on how fast especially APNIC which has the biggest burn rate at this time allocates its next Ipv4 blocks, APNIC might even put in another request before the end of the year which might leave RIPE without additional allocation. Despite such speculations Le Heux said to this reporter he expected to run out only in Q3 (or possibly even Q4) next year which seems to be relatively optimistic – and also is based on the expectation that there will be no stretch run for the last resources next year. So far there had been "no panic", requests had grown linear as before in the RIPE region, RIPE experts said. Le Heux said, with the expected depletion of IANA the situation could change, but predictions were impossible.

Transfers policy revisited

La Heux during the Address Policy Working Group also presented what he said were inconsistencies in the way transfers of Ipv4 addresses from one company or organisation to another was managed by the RIPE NCC. RIPE procedure 301, which describes mergers and acquisitions, allows transfers of resources in a straightforward way. On the other hand the transfers policy passed in 2008 by the RIPE members (now chapter 5.5 of the Ipv4 Address Allocation and Assignement Policy for the RIPE NCC Service Region) put several limitations.

- there should be no assignments to end users in the resources proposed for transfers
- the receiving site has to document their needs and the RIPE NCC has to approve (just as for regular allocation)
- the transferred blocks cannot be reassigned by the receiving party within two years

Le Heux pointed out that the two-year transfers moratorium for Ipv4 addresses might not serve the community well, because possibly Ipv4 address after depletion would be needed by some parties only for a short transition time and quicker transfers to other organisations in need could make sense to allow effective sharing of the scarce resources.

Additionally he was afraid that members desperate to find additional resources might decide to chose the "merger path" as the easier way to get Ipv4 addresses or even avoid both merger transfers procedure as well as the more restricted transfers policy. "They might decide that both of them are too much hassle and they will just transfer or move their address space around under the table and that would be worse because at that moment, we would have no idea any more with where the address space is and then we lose track of the main function of what the registry is about. It's knowing who is using which address space", said Le Heux.

A future registration policy?

A possible shift of the RIPE NCC's focus on registration instead of allocation policy for Ipv4 was supported by RIPE long-time Chair Rob Blokzijl who said he had his worries with the transfers policy, as to keep the RIPE data base clean was the first and foremost purpose. He was preparing a “technical document” for a “definition of the registry” together with the RIPE NCC. Based on the registry-definition a future registration policy could be developed or sifted out from existing policies and concentrated in one document. While there was no need for new registration policies now, there might be after depletion also be the right time to think about additional rules to register transfers. Blokzijl said: “I think what we are talking about is not so much regulating the transfers of address blocks. Our interest here is 'tell us where you transfer it'.” This would allow the RIPE NCC to keep the registry clean and up to date. Blokzijl said his initiative to define the registry was also triggered by the start of certification of address resources (see below).

RIRs as stewards or plain registries

It will be interesting to see if the RIPE will chose either the path of ARIN that promotes a stronger role of the registry in the transfers business (and wants to keep the need-based allocation also for transfers) or if RIPE chooses to follow APNIC APNIC CTO Geoff Huston supported Blokzijls view during the address policy WG session pointing to the APNIC decision to put “no particular restrictions in terms of moving addresses around between folk” after depletion. “The idea being that once we haven't got this allocation mechanism around, we truly revert to being a simple registry. And a simple registry needs to admit reality, and the fewer policies you have about what you would call reality tends to make the registry more useful for everybody else.”

ARIN CEO John Curran on the other hand described the ARIN transfers policy as clearly based on documentation of “need”. “A party that qualifies for address space and meets the definition of "Need" per today's definition just as we do with requests, can turn around and show up with another party and say I am getting it from this guy.” ARIN would not check if there was payment for the addresses or not, but would still adhere to RFC 2050 of the IETF.

The decision of other RIRs with regard to that question might in the future influence the possible development of a global policy on returning of Ipv4 address resources (handed back from LIRs) to IANA and possible inter-RIR allocation of these resources. Again ARIN at this moment seems to opt for a return of Ipv4 addresses only for those RIRs that still “exercise stewardship” (obviously this means allocating on a needs-based principle). ARIN might possibly be able to hand back more Ipv4 resources as the most legacy space sits in the ARIN region. And in the ARIN region there is a discussion to – much steward-like – to reclaim resources from legacy owners who do not bother to show up and register their resources in ARIN's ongoing data-base clean-up activity.

Official resource certification starts January, 1/ Policies incomplete

With the start of certification of for PA resources imminent, still a lot of policy documents are to be developed. On January, 1, RIPE starts to act as certification authority offering certificates for resources to interested LIRs. Alex Bland from RIPE NCC explained the system that will be further developed for other than PA resources and allow LIRs to act as certificates themselves for their customers in the future. Currently, Bland said: “These certificates contain a couple of things: A public key, since this entire system is based on public key infrastructure; it lists all of your resources; and a signature saying the RIPE NCC gives this a stamp of approval and certifies that you are the legitimate holder of the resources listed in this certificate.” LIRs can as a first step create the so called rout origin authorisation objects (roas) that can be validated by third parties to ensure correct route announcements. The standards for the Routing PKI system are still developed in the Secure Inter-domain Routing WG of the IETF.

With regard to the policies for certification at RIPE, Nigel Titley presented a slim policy proposal that mainly regulates that everybody who has a record for a resource in the RIPE database can get a certificate for that. Certificates will be valid for 18 month. Withdrawal of the record of the resource will automatically result in the   certificate being revoked. While Tiltley said the policy had been focused on a few very basic rules. There has been a concern that certificates once in place might be linked to a clear financial record of the respective resource holder. Also revocation of resources was seen as a possible handle third parties like law enforcement or copyright owners might view as a possible point of control.
Bland pointed in his presentation to work that intends to get checks on the certificates into routers. Cisco, he said, had already running code, and Juniper was working “on something similar”. In the long run the idea is that if certificates are invalid, for example revoked or expired, the respective routes would be dropped. Bland said this by no means would mean that the RIPE NCC would become a “routing police”. “Certificates don't create additional powers for the RIRs”, he said, because certificates would merely reflect the registration status. “It simply means if you don't have any registration, you don't get a certificate.” Still people were free to route prefixes without or with invalid certificates. Network operators would stay “in the driver's seat. We don't control that, we don't do that for you.”

It may take still some time before Certificates are taken up by the membership, yet two kinds of pressures are possible in the middle or long run. Once deployed by large backbone operators – and also once the system to use certificates for route filtering is well established, there might be a push in the sector to those who did not “opt in” in the first place. Another sector interested in pushing for adoption might be law enforcement and politicians. The possibility to make routing of prefixes more difficult – at least to some extent – might be tempting as law enforcement agencies have been interested in cooperation with the RIPE and RIPE NCC in an effort to somehow get bad routes blocked.

As the proposed certification policy is intended to “reflect registration status”, it might be also interesting to take a look at the proposals from the RIPE NCC about the closure of LIRs and the deregistration of resources, both presented in Rome.

Closure of a LIR and Deregistration of Resources by the RIPE NCC

The NCC proposed new procedure for LIR closure and resource deregistration was intended to have all aspects for the procedure in one document, Athina Fragkouli from the RIPE NCC explained. There had been procedural steps for both measures, but they were scattered in various places of RIPE NCC documents. Also there had be no complete list of reasons for closure and deregistration, she said. Closure of a LIR according to the new procedural document can be started by the RIPE NCC for non-compliance with RIPE policies including:

– unresponsiveness
– assignments that are against the RIPE policies
– incorrect registration in the RIPE DB
– no compliance with RIPE NCC audit
– no compliance with an arbiter's ruling

The respective LIR is given email notice and he will receive two reminders. Closure, if the LIR did not use the option to make changes to fix the situation, will be executed after 90 days. A new set of reasons for a closure of procedures targets “falsified or incorrect information” and “fraudulent behaviour”. Again the procedure gives the LIR 90 days to make adjustments before RIPE NCC closes the respective RIR.

Finally the RIPE NCC in its procedure also provides for “immediate closure” of a LIR in the following cases:

- contributor files for bankruptcy, etc
- contributor damages the name of the RIPE NCC
- contributor fails to submit registration papers
- contributor fails to submit any rule of applicable law
- non-payment
- termination of the RIPE NCC membership

For these reasons the RIPE NCC reserves the right to decide if they will give just an immediate closure notification or if there will be requests to change the situation and reminders before the closure. This looks pretty tough, yet there was no big discussion during the session. Ruediger Volk from Deutsche Telekom said, he did not see "really drastic things here", yet said the bankruptcy case might be viewed different in different legislations as to how much this meant for the future live of an entity. Volk also pointed out with regard to deregistration following LIR closure that users of the respective entity might be affected by deregistration of resources without being involved in the reason that led to closure and deregistration.

The consequences for the LIR termination are "end of service of the NCC", end of RIPE membership, but also "deregistration of resources" - so the respective LIRs is no longer holder of the resources he had been allocated by the RIR (certificates would also vanish with this).

Deregistration follows its own procedure (notification, four weeks response time, all in all 3 month to make adjustments before final deregistration). Reasons for deregistration beside the termination of the SSA (and LIR closure as explained above) are also:

- invalidity of original allocation/assignment criteria
- incorrect registration in the RIPE DB
- falsified/incorrect registration
- fraudulent request
- refusal to comply with RIPE NCC audit
- Dutch court order

Nearly the exact rules apply also for provider indirect end user resources and directly assigned resources to end users.

Cz.nic's experience with DNSSEC algorithm roll-over

Cz.nic decided to a roll-over from NSEC to NSEC3 to avoid zone walking for the future. NSEC 3 also made a change from RSASHA1 to a newer algorithm necessary as it is incompatible with the latter. As it is not possible to just change the ZSK algorithm a KSK roll-over was necessary. Cz.nic according to Jaromir Talir did use the opportunity to publicly promote a change from validation using the local trust anchor (Cz.nic trust anchor) to the now available root zone trust anchor.

The most important result of the effort Talir was that pre-publishing for the roll-over used for regular KSK roll-overs was not possible, due to the fact that the "simple publication of DNSKEY with different algorithms in the zonefile makes the zone bogus" In reality BIND and Unbound reacted somewhat differently, with Unbound staying close to the RFC (making the zone bogus) while BIND behaving outside of the standard by not treating the zone with the new algorithm as bogus.

The authoritative standard is RFC 3045, where section 2.2 reads:

“There must be an RRSIG for each RRset using at least one DNSKEY of each algorithm in the zone apex DNSKEY Rrset. The apex RRset itself must be signed by each algorithm in the DS Rrset located at the delegating parent (if any).” cz.nic therefore opted for a double signing.

According to Talir each RRset had to be signed with the new DNSKEY, signatures had to be put in the zonefile before DNSKEY and DS needed to be sent upstream.

The steps taken by Cz.nic according to Talirs report were:

3.8.2010

– We signed zonefile with new KSK/ZSK (+old KSK/ZSK), published this big double-signed zonefile and waited TTL for RRSIG

– We inserted new KSK/ZSK into zonefile and waited TTL of DNSKEY

– We sent exchange request to IANA to insert new DS and remove the old ones. (processed in two days!)

24.8.2010

– We removed old KSKs from zonefile and waited TTL of DNSKEY

– We signed zonefile just with new KSK/ZSK and waited TTL of RRSIG

– We signed zonefile once again using NSEC3 instead of NSEC

According to Talir there were no big issues for the roll-over. He also said that he expected for the future that every KSK roll-over would also be a algorithm roll-over, because the possible quick development of IT.

Steve Kent questioned the jump from RSA SHA 1 to RSA 512 (instead of using RSA 256 first), but Talir had explained that in order to avoid to have another algorithm roll-over too soon, the registry had gone for “the best available on the market”.

ATLAS – probes help to get a complete “weather report “ of the net

The RIPE NCC scientists have worked on their measurement projects for years, developing the “Test Traffic Network” that allowed measurements from various places all over the world and the DNSMON service. Now RIPE NCC is aiming to distribute 50.000 probes all over Europe and possibly half a million all over the world to allowing a very detailed monitoring of traffic on the net. The idea presented by Daniel Karrenberg is to organize this as a community project with possible sponsors investing in a number of probes(8 probes for 2K Euro, 16 probes for 4K Euro or 256 probes for 64K Euro, the latter equalling 65536 Euro) in exchange for credits that will allow them to initiate special monitoring requests.

While all data should become public – which Karrenberg said was necessary for a community and RIPE project – procedures about possible up-front information should be further discussed. Sponsors would still gain by participating because to build a network of their own of such a magnitude would be much more expensive, said Karrenberg. He said he expected that a large network of probes once established would allow to even zoom in to special geographic regions to analyse problems there.

For a start the probes do “pings” and “traceroutes” to a fixed number of sites are possible, DNS queries are expected to be possible later. Additional checks would also become available with further development of the mini-probes, that run on an Ethernet power connection and are attached per Ethernet to a home or larger network router. The probes while offering 8 MB RAM and 16 MB Flash, are dumb and will be managed through a hierarchical systems of controllers and higher brain servers via the RIPE Atlas portal. Probes hook up to the system via a dedicated registration server which has

the overall view of the status of the system.
A central database holds data gathered and manages user credits, over a special user interface probe owners can look-up the status of the probes and actual measurements. Firmware-updates will be automatic. All elements of the probe system were using secure channels, Karrenberg and Robert Kisteleki explained in several presentations. Security issues were partly a reason, according to Karrenberg, for not publishing the source code of the probes. Yet he also said, he did not want to see commercial competitors start similar projects. He was afraid that RIPE NCC would not invest in similar projects if Atlas failed because it was just taken up elsewhere.

For the time being RIPE NCC still offers to send single probes to volunteer participants, those who would be interested in more probes and in getting credits to initiate their own measurements are expected to become sponsors. The target, according to Karrenberg was to have around 10.000 probes distributed over Europe by the end of 2011.

Working Groups, Plenaries

DNS

The DNS WG heard reports about the decommissioning of the ITAR, a very short update from ICANN, and inter alia reports on the start of the Cyrillic version of the ru-TLD, preparations to use Ghost as an alternative algorithm in DNSSEC.

The Decommissioning of the IANA Internet Trust Anchor Registry (ITAR) was welcomed by the RIPE community. After an end of life notice for November 2010 IANA was removing the remaining trust anchors. The rootzone a month after signing had already surpassed the ITAR with regard to the number of trust anchors stored. Announcements about the decommissioning had sped up the migration process for most of the remaining TLDs. Currently 49 of 65 signed zones have DS records in the root.

Else Gerich, Vice president of IANA, did not touch on the problems regarding the still blocked .arpa-request to have the arpa-DS put in the root (and the resulting validation problems after the ITAR dropped the .arpa keys). In fact Dave Knight from ICANN spoke about the signing of .arpa as one project at ICANN.

Meanwhile this reporter has received an explanation from well-informed sources that the issue responsible for the blocking is a latent dispute about who is responsible for .arpa – obviously NTIA is of the opinion that itself is responsible and as it has not initiated signing the arpa-zone there is now a bureaucratic hang-up. The IANA data base clearly lists the IAB as the If this will be resolved soon, as this reporter was told by Joe Abley from ICANN, remains to be seen.

Vasily Dolmatov (Cryptocom,Hosting Community) explained preparations to use Gost as an alternative (obligatory for public services or personal data handling in Russia) to the RSA crcryptotandard family. Gost has been presented as IETF RFCs (5830, 5831, 5832, 5833) now and consequently has been integrated in Open SSL 1.0.0a and later, Unbound 1.4.6 (by default) and BIND 9.7.0-P2 (Cryptocom did implementation work on all three). Checks showed no problems with RSA-GOST-RSA chains. Only .ru is not yet signed.

The Cyrillic version of .ru that started normal registration on Nov, 11, after several stages of sunrise application periods (with the addition of two additional sunrise periods also for non-Cyrillic TM-owners starting May 12 and mass media, NGOs, companies that could not register their names as trademarks starting July 15). After sunrise there were 18000 registrations, after the first day of first-come-first-serve registration on November, 11, there were 250.000. TLD.ru expects 800.000 in one year. The TLD that is operated jointly be TLD ru and 19 registrars uses a modified version of EPP with a revised registrar change scheme. Two nodes are in place in Moscow and St. Petersburg for front end database operation. A decision if the registry will operator as thin was still open. The registry has 2 hidden primary DNS servers and 11 secondary DNS servers. Ipv6 is supported, DNSSEC is currently tested.

Cooperation

The Cooperation WG heard a report by Maria Hall, representative from the Swedish government and WG Co-Chair on the recent meetings of the International Telecommunication Union (ITU Plenipotentiary in Guadalajara, see earlier CENTR report) and about the next steps for the Internet Governance Forum (IGF 2010) for which a renewed mandate is currently under discussion at the United Nations Plenary Session in New York (find the current draft UN resolution here). Hall supported the continuation of the IGF as a useful forum to bring together governments, technical community and business. Sweden and the EU were favouring the continuation at the UN while acknowledging the need for improvements (more countries, especially more development countries, more technical community, “more of you guys” that would participate in the discussion on critical Internet resources[1]). Hall applauded the dialogue developed over the five IGF editions since 2006 and said the multi-stakeholder dialogue could be helpful in other sectors, too, but still the model was new and governments sometimes wanted just to speak among themselves.

Since the UN World Summit on the Information Society (WSIS) there has beside the IGF been an ongoing discussion about what the summit meant by initiating “enhanced cooperation”. Now a consultation organized by the UN secretary General is under way, see again the draft UN General Assembly resolution (statements can still be sent in until the end of December, said Hall). Following up to Hall's presentation the New York resolution looks nice for the IGF as it supports what Hall said will be a self-developing mode for the IGF mostly – improvements are discussed by a special WG under the auspices of the Committee on Science and Technology (chaired by Swiss BAKOM rep. Frederic Riehl).

Hall referred to the outcome of the Plenipotentiary in Guadalajara as pretty ok, with the ITU reference to the RIRs, ICANN, the IETF, ISOC and other Internet self regulatory bodies as one of the major successes after lengthy discussions (“it's really messy”, “a lot of work”, negotiations until two o'clock in the night”, Hall).

Paul Rendek, Head of External Relations and Communications of RIPE, gave an overview over the enormous amount of “multi-stakeholder dialogue” or “enhanced cooperation”-work RIPE NCC is doing, beside being active at all of the mentioned for a (plus OECD, Council of Europe, EU Commission) the RIPE NCC organizes special government round tables, with the first Middle East government round table planned for March 3, 2011 in Beirut, and the another edition of the regular Amsterdam government round table on Monday, February 28. Another line of discussion is pursued by RIPE with law enforcement.

It is interesting to note that the Cooperation Working Group, originally initiated as an open link between governments, law enforcement and the RIPE operator community is much less accepted by governments. Only a fraction of the governments attending the government round tables (38 reps from 12 countries on February, 22 2010) show up at the RIPE meetings. Law enforcement from the US (FBI) is a regular, silent participant, UK and Dutch Leas participated occasionally. A notable exception are the Swedish government sending Maria Hall as the Vice-Chair and the German Government, keeping the community up to date relatively regular on its Ipv6 activities.

Constanze Buerger from the German Ministry of the Interior which is has been allocated a /26 Ipv6 address block and starts to assign small blocks to German States (Laender) and cities next year. Last

[1] Critical Internet resources is a catchword for ICANN/IANA's root management role and the, according to some UN member states, unilateral oversight role of the US.

tests for firewalls, security hard- and software and services were at the moment ongoing but would be finalized for the official start of the v6 network for the public authorities in February 2011. Joerg Wellbrink from the German Army (Ministry of Defence) presented their ongoing Ipv6 preparations of the military. Pings over the satellites of the army down through the net to the end user signal equipment had already been done as a first step. Currently the army had commissioned research and development on IT security. There was a need to come up with "ideas how to connect ad hoc mobile networks" with international partners and to use German security systems was no option. "I don't think we can convince the Americans to buy our stuff so we have to come up with some other things." Wellbrink said to this reporter he would appreciate to meet colleges from other countries at the RIPE meeting much more.

Address Policy

Beside discussions over clarifications in several existing policies, notably a fight about the definition of "openness" (does it exclude IXP that allow votes of members to grant new members' access? Or is open only 'transparent'?) in the Ipv6 IXP policy (that resulted in a complaint from Sergi Polischuk over RIPE NCC objecting to allocate Ipv6 resources for an Ukrainian exchange point), there were three major policy proposals discussed

– ARIN Proposition 119 on Globally Coordinated Transfer Policy

The proposal wants to push for a global acknowledgement of a needs-based allocation also in transfers

– RIPE-2010-5 "rewrite" of 2009-1"

The proposal wants to create a global policy for Ipv4 allocation after IANA Ipv4 exhaustion
It foresees a IANA reclamation pool of Ipv4 addresses that would allow post-depletion allocations to "eligible RIRs" (split resources equally). Eligibility is given if addresses are allocated by RIRs to LIRS according to a global, coordinated policy (stewardship values to be uphold), no mandatory returns of address space.

– Certification Policy, 2008-08 (see above, Highlights)

Some more news from the RIPE 61 Plenaries

Complexity

Several interesting presentations were given in the various plenary sessions, to mention only a panel session on complexity featuring Michael Behringer (CISCO), Geoff Huston (APNIC), Gert Döring (Spacenet) and Nico Fischbach (). Geoff Huston in what he said was a personal view underlined the trend to base business on complexity (ask any telco!, he said), while it was in fact quite hard to bas a business on simplicity and minimalism (those companies did not survive). Possibly the post-IP era would get rid of all the complexity and close the cycle again to something simple and easy (just the way IP started its career).

RIPE meeting evolution

RIPE and RIPE NCC try to add several features to the RIPE meetings like a BoF session (that focussed on Ipv6 applications in Rome) and an Ipv6 security tutorial.

RIPE General Meeting

The GA approved the charging scheme for 2011 and the RIPE NCC Conflict Arbitration Procedure. It appointed Pierre Baume, Conor Dufficy, Ronald Duncan, Alireza Ghafarallahi, James Hickman Ondřej Surý and Nick Williams to the RIPE NCC Arbiters Panel.

The next RIPE meeting will take place in Amsterdam on May .