Report of RIPE 64 Ljubljana

16 – 20 April, 2012

by **Monika Ermert**

for the CENTR secretariat

Table of Contents

Highlights

IPv4 Address Transfers - Brokers getting down to promote Inter-RIR address policies

Sandra Brown, an “address broker”, presented a policy proposal for Inter-RIR transfers at the RIPE 64 in Ljubljana, backed up by a second version by Remco Mook, RIPE Board member and author of the hotly debated original transfers policy in the RIPE region.

Brown, who as a Nortel employee was involved in the sale of a fat IPv4 block by her company (then in bankruptcy) to Microsoft last year, co-founded IPv4 Marketplace LLC, one of five address brokers registered at ARIN as “facilitators” for transfers. She had seen the business opportunity during the Nortel-Microsoft deal, Brown said, and she expected address transfers and sales would be a business at least for five years.

Her company decided to engage with the RIRs, and Brown and her co-founders have traveled the RIR meetings since in order to promote Inter-RIR transfers that would allow to satisfy demands from regions already scarce of IPv4 address space with addresses for example from the ARIN region. So far it is APNIC who has passed an Inter-RIR transfers policy, being the first RIR that has run out of IPv4 addresses already a year ago.

Paul Wilson, CEO of APNIC, announced at the RIPE meeting APNIC would not only offer address requesters pre-approval (of their documented need for address space) but also provide a list of all pre-approved requesters to smoothen transfers once blocks became available. APNIC also wanted to have a binding agreement with brokers in order to ensure they would follow APNIC policies. The APNIC announcement, according to Wilson, was a step to get away from the “brokers are bad”-situation, at least for those brokers playing according to RIR rules.

The proposal (2012-1) that would soon be succeeded by the new version (2012-2, co-authored by Brown, Mook and James Blessing), according to Mook, was trying to be rather simple. It was allowing Inter-RIR transfers with the needs-based policy by the receiving region. Waiting periods shall prevent speculation, but RIPE members criticized the notion that transfered IPv4 addresses could “not be **sold** within 15 month” (ARIN 12 month). There was not a lot of discussion about the pointer to the EU Anti-Spam EU provisions on Anti-Spam in EU Directive 2002/58.

As RIPE will be the second registry to run out of addresses (according to Geoff Huston's current projection on August, 13th 2012), RIPE members, too, could benefit from transfers from the ARIN region, once ARIN also has a transfer policy. Such a policy could be in place in six to nine weeks once the ARIN advisory council and board have taken up a positive vote from ARIN members, many of whom voted in favor of a transfers policy at the ARIN meeting in Vancouver on April 24-25.

APNIC has already passed a policy, LACNIC has not decided yet, and AFRINIC did not even start the discussion. AFRINIC is expected to run out of IPv4 addresses (see Geoff Huston's calculation) around November, 4th 2014 and LACNIC even earlier, around January 29th the same year.

While for address space assigned or allocated by the RIRs and cleanly registered in their databases broker facilitated transfers look rather straightforward, it gets interesting when transfers concern legacy space ¨C the bulk of address space especially in the ARIN region. ARIN -and also RIPE NCC- have been campaigning for legacy space holders to join the RIRs or to sign as ARIN proposes a “Legacy Registration Services Agreement (LRSA)”.

Yet brokers such as Addrex (the broker involved in the Nortel-Microsoft deal) have questioned ARIN's authority and gone as far as promoting a “post-distribution registrar service to entities that hold Internet Protocol version 4 (IPv4) number blocks that were granted to them, without a contract, by a United States Government authorized distribution authority” plus a market place for IPv4 address, Addrex.net itself.

US academic Milton Mueller recently wrote in a paper that brokers like Addrex have begun to question the “RIRs’ exclusive control of IP address allocation” and proposed “a structural separation between address registries (the RIRs) and address registrars (the postallocation services)”. Mueller compared this to the “separation ICANN created between domain name registries and registrars”.

With pressure on the RIR system ¨C Wilson reported about questions from Chinese Officials about how APNIC would try to recover the bulk of legacy addresses around in Western countries - the RIRs got started attempts to bring legacy space into their registry and the respective holders into the system. During the RIPE meeting in Ljubljana Niall O'Reilly (University College of Dublin) warned not to force legacy address holders ¨C in Europa many academic institutions - to submit to the body of RIPE policies which would stall their moving forward while their legal counsels would check on potential compliance issues. O'Reilly proposed to the Address Policy Working Group that legacy holders should be involved in creating a more light-weight policy that would allow them to join RIPE. O'Reilly will now prepare a document for consideration by legacy holders and the RIPE community.

Given the long-standing abstinence of the RIRs from IPv4 address transfers and “sales”, the issue of transfers has become a topic people in the RIPE region seem to accept as inevitable at least.

DNS-Changer - “We cannot spoof these addresses forever”

After July, 9th, every user who has not got rid of the DNS-Changer malware will get no responses to their DNS queries. The DNS-Changer malware reset the DNS settings of around 4 million machines worldwide to attract and benefit from the traffic. When the FBI in November took out a group of people allegedly responsible for the fraud, it wanted to prevent that victims would lose DNS connection out of the blue and therefore -under a court order- assigned to ISC the operation of substituting the servers and serving DNS answers to the infected machines.

Joao Damas from ISC gave an update on the operation in a RIPE panel on DNS-Changer and the FBI Operation “Ghostclick”. In March a federal judge has extended the deadline for the operation of the servers, obviously there are still many machines that need to be cleaned up. Damas also underlined: “This will be the last extension. We cannot spoof these addresses forever.” Damas himself with this statement points to the fact that the manipulation of DNS traffic deviates from the pure doctrine and, as panel moderator Peter Koch pointed out, would make a nice test scenario for DNSSEC. With DNSSEC deployed and validation widespread the manipulated servers would not allow the re-routing over the FBI/ISC servers.

An even more discussed point was the reaction of the RIPE NCC to the order to freeze the IP addresses used by the fraudsters. While NCC lawyers requested from the FBI that an order had to come from a Dutch Court, when the Dutch police after a Mutual Legal Assistance Treaty request from the FBI quickly produced and presented an order which RIPE NCC lawyers accepted and enforced by freezing the address blocks in question. But the order received was no court order, but an order by the police, based on article 2 of the Dutch Police law. Article 2 is a rather general provision describing the task of the police to uphold the rule of law and render assistance to those who need it.

After checking the police order the RIPE NCC decided it was not sufficient for freezing the address space (four blocks) in question because article 2 did not enable the police to oblige a party to actively do something and also there was a need for a legal basis for invoking article 2 in the first place. As the

prosecutor did not follow-up requests for a further legal basis RIPE NCC “unfroze” the addresses in January.

As the RIPE NCC concluded that there was no sufficient legal basis for such actions under Dutch law in general, the organisation finally decided to go to court and challenge the procedure, Counsel Jochem de Ruig reported. “With hindsight”, Jochem acknowledged, “maybe it would have been better if we would not have done that and not executed the order. Or think in the future when it's just a police order and hasn't been stamped by a court, we would not like to do that.” Daniel Karrenberg, Chief Scientist of RIPE NCC, added: “We will not cave again. We will insist on the judicial review. We will defend the rights of our members.” Certainly, with allegations of “imminent danger” by police, the managers would have to make a decision what to do. “You can always make mistakes”, he said.

Several participants had pointed to the “very bad precedent” the “caving in” had produced, especially given the earlier discussion in the RIPE community about potential “layer nine”-risks of the Routing PKI system. Once the latter is fully deployed, the de-validation of RPKI certificates at the whim of law enforcement would mean the respective party would drop from routing tables.

The ongoing court procedure demanded by the RIPE NCC, according to de Ruig, shall bring more legal clarity on future orders. While in a first Court hearing the State did not appear, the parties first met in Court on April, 11th. De Ruig expects a decision by the Court on how to proceed (either with a full hearing or further written statements) in June and a decision presumably in 2013.

In addition to questions on the “caving in” and the ongoing “spoofing” of addresses by ISC, RIPE NCC had also to answer questions, why members had not been informed about the DNS-Changer issue when receiving the first request by the FBI. As customers of RIPE members very well could have been (and were) affected by the scheme RIPE NCC could have helped its members to mitigate.

Outlook on the World Conference on International Telecommunication

The Cooperation Working Group, which again attracted merely half a dozen government representatives (compared to 70 participants in the last edition of the closed-session RIPE NCC roundtable events in Brussels in February), talked about the International Telecommunication Regulations (ITR).

The ITR, a treaty passed under the auspices of the International Telecommunication Union (ITU) in 1988 in Melbourne, will be reviewed by the ITU member states during the first World Conference of International Telecommunication (WCIT). The ITR, which according to the ITU is the only international treaty talking telecoms, has been focused on phone connections at a time when most operators were still state monopolies.

While an update looks over-due, there are a lot of ITU member states that are concerned with the potential ¨C and maybe even inevitable ¨C expanding of the ITR to Internet connections. Looking into the preparatory work for the treaty conference in Dubai in December 2012 it seems that countries like the US, but also European countries will block new articles on content issues, state intervention on routing or a reform to global IP address allocation, the latter still not fully explained by proponent Russia. A potential role of the ITU in IPv6 allocation has been an issue of contention for some time, but so far it failed to get consensus.

Phil Rushton, Number and Standard Strategist of British Telecom (a so-called sector member of the ITU, same as RIPE NCC and some ccTLDs) gave an overview over the controversial issues, see the following list:

• Transposition of ITRs into national law?
• All telecommunications (capabilities)? Only International Telecommunications?

• Recommendations to become mandatory
• Internet traffic termination? To be discussed
• Combatting SPAM?
• Provide Calling Line Identification (CLI)? Country of Origin? On SIP?
• States to dictate routing? On SIP?

The most relevant issues from the point of view of the Internet community - leaving aside the option that Internet issues should be kept out of the treaty completely ¨C are potential mandate for ITU standards, routing intervention and all network security related aspects for which even a new special article (8A) has been proposed.

ITU recommendations getting elevated to mandated standards?

Currently two options have made it to the draft ITR text: either ITU-T recommendations mentioned in the regulations (in various paragraphs) in general do not receive "the same legal status as the regulations" or they do not get regulatory status "unless otherwise specified in these regulations". There seemed to be near-consensus at the last prep-meeting that ITU-T recommendations could not be elevated by the text to mandatory automatically. Still both options of text still exist and there are many recommendations mentioned in the text, each with specifics as to their status. Additionally there are five different variants of member states' obligations with regard to implementation of the "relevant ITU-T recommendations", some even asking the member states that they have to honor (and make private companies in their countries honor) "any Instructions forming part of or derived from these recommendations". In most instances referrals to ITU-T recommendations do not give specific recommendation numbers, but simply point to the "relevant" ITU-T recommendations.

State intervention in Routing

With regard to routing the current draft new ITRs includes a proposal from Egypt asking at least for the possibility to intervene in routing decisions for security reasons.

> *"A Member State shall have the right to know through where its traffic has been routed, and should have the right to impose any routeing regulations in this regard, for purposes of security and countering fraud."*

There seem to have been more far-reaching routing intervention ideas, but they did not make it (at least not so far) to the draft new ITR text. It is unclear how a provision like the one proposed by Egypt should work in practice.

Another very interesting question is if the states will continue to include their "kill-switch"-provision in the ITR which allows countries to "suspend international telecommunication services partially or totally". There are additional proposals put into the draft new ITR with regard to such a kill switch, which reads:

> *"Member States also reserve the right to cut off, in accordance with their national law, any other private telecommunications which may appear dangerous to the security of the State or contrary to its laws, to public order or to decency."*

Given the recent debates on "no disconnect-strategies", the latter a poster-child of EU Digital Commissioner Neelie Kroes, it will be interesting to see, who will favor and who will reject such proposals.

The issue of security and cybercrime

There are several aspects discussed in relation to cybersecurity, one focuses on the transmission of calling party line (CLI) ¨C or at least the origin (geographical and provider identifier) of communication in order to prevent “naming and numbering misuse” or “fraud”.

Another “security” issue is the spam problem, which even the group of European countries represented by CEPT, think is worth mentioning by “promotion of anti-spam legislation” in the member states.

A big step would certainly be the inclusion of a whole new chapter on “Confidence and security in the provision of international telecommunications and services”. The proposed new article 8A (proposed for example by the Russian Federation and the Organization of former Soviet States for Telecom issues) includes provisions like

> *“Member states shall take measures to ensure Internet stability and security, to fight cybercrime and counter spam while protecting and respecting the provisions of privacy and freedom of expression as contained in the relevant parts of the Universal Declaration of Human Rights”*

The new article 8A has not yet been discussed in depth so far, so there are still half a dozen different proposals for it, with some leaning toward prompting private sector responsibility for network security, and others calling for cooperation of member states in developing technical standards and acceptable norms. Discussion will take place during the last preparatory meeting on June 20-22, as will on the equally sensible issue on accounting and/or “economic issues”. In the debate on how far traffic and transit prices should be framed or even set by governments, market and state regulated philosophies clash.

Outlook

BT-strategist Rushton confirmed that it is nearly impossible to predict the chances of the various proposals at the current stage. Governments, according to one official, are still in a somewhat tactical phase. Neither red lines were explicitly declared, nor have all final proposals been laid on the table yet (see for example the IPv6 allocation proposal to be further detailed by Russia). According to the procedure, proposals can very well only be put on the table during the last preparatory meeting on June, 20-22, or even at the negotiation plenary in December.

Statistic alone make clear how far away the community is from consensus: compared to the standing ITR text of 10 text pages the draft new ITRs are 67 pages at the moment. They include alternative proposals for the already discussed parts from Preamble to Article 5 and, starting from Article 6 to Article 10 not yet discussed alternatives.

French regulator (too) interested in the pricing of Peering

The French Regulator, Autorité de régulation des communications électroniques et des postes (ARCEP), wants to regularly monitor peering relations and prices to check on potential competition issues. Two times each year network operators and large content providers in France, but also non-French operators peering with French companies are required to fill in a form about peering and transit, about data traffic exchanged and the prices payed, Pasal Dagras from the ARCEP explained during a panel discussion in Ljubljana.
The relevant order, meanwhile published also in an English version, names the following entities as being subject to the ARCEP questionnaires:

> operators directly under ARCEPs oversight
>
> *“electronic communication operators that have “an interconnection relationship with at least one electronic communications operator” in France and providers of public communication services, “that have a direct relationship with at least one electronic communications operator (..) for the*

purposes of interconnection, and which have actively taken steps to have their services or content used or accessed by end users in France.

Criteria about what means actives steps to attract French users include having a top level domain in .fr (or under a French territory-ccTLD), “offering content in French”, “offering products and services that are shipped to or supplied in France, to a significant degree” or “being established on the French territory”.

Several participants at the RIPE meeting, including Malcolm Hutty from the London Internet Exchange (LINX), bluntly questioned ARCEP's competency to request answers from non-French operators. ARCEP, while having agreed to some limitations for non-French providers after a consultation (for example including the criterion of proportionality), still was sure, according to Dagras, that all operators including non-French operators had to file answers on every request they receive.

Hutty on the other hand warned that attempts to enforce national rules in an extraterritorial context would set a very bad precedent. The burdensome procedure to monitor peering and transit relations could also push non-French providers to avoid peering with the French companies altogether. Several participants noted that, as peering was a private party commercial relationship. How ARCEP would enforce the monitoring over non-French companies is open.

ARCEP, according to the order, hopes to coordinate with other regulatory authorities with regard to the monitoring, which -according to the ARCEP- is based on EU Telecom Package Directives a EU Council Decision (on the open Internet, December, 13 2011) and part of the activities of the agency to secure competition and net neutrality (see ARCEP's Internet neutrality recommendations published on September, 30, 2010). Starting point for the monitoring, according to Raphael Maunier from Backbone provider NeoTelecoms, was a complaint from Cogent against incumbent France Telecom. Maunier warned that there was a lack of dialogue between small/medium ISPs and the regulatory in France. ARCEP in May started open consultation about its net neutrality project. The consultation might allow opponents of the monitoring order to take a stance.

Plenaries and Working Groups

IPv4 - Address policy Working Group

There is not a lot left to do, it seems, for the Address Policy Working Group with regard to IPv4. Expecting to run-out mid-August of the last IPv4 addresses, there is no need for further address allocation or assignment policies for IPv4. Beside the now more interesting transfers policies and a way to deal with legacy holders in the future, not the least in connection with routing certification and, potentially later route filtering based on certificates, a maintenance policy was necessary, though. RIPE long-time Chair announced he was prepared to draft one IPv4 maintenance policy document that would draw together from existing documents what address holders needed to know. Blokzijl included contractual relationships in the RIPE region, IPv4 registration maintenance, transfer of allocations, allocations from the last /8, unforeseen consequences, legacy space and temporary assignments in a first version of a maintenance document. Daniel Karrenberg, Chief Scientist at the RIPE NCC, said he expected that after the run-out of IPv4 a complete new start was necessary and that the maintenance document was not sufficient to address the changed landscape. With regard to legacy space Neill O'Reilly underlined ongoing work to arrive at a legacy resource holder status (see highlights).

Open policy proposals on IPv4 include the nearly concluded reservation of IPv4 addresses (a /16 from the final /8) for Internet Exchanges and an IPv6 allocation modification that shall enable small LIRs to issue larger blocks (not /64) to their customers.

IPv6 - A call to go back to IPv6 preferential treatment in dual stack environment

Geoff Huston, Chief Scientist from APNIC, in his plenary presentation urgently called operators to go back to preferential dealing of IPv6 in dual stack environments. While this had been the original standard implementation, meanwhile there were all sorts of attempts to make a smart decision if going for IPv4 or IPv6, sometimes resulting in very long round trip times (300 ms for Windows 7 and Chrome, for example).

With IPv6 native often being faster, yet showing a 5 percent failure rate (with high geographic differences: 0,2 percent failure rate in Norway, 18 percent in Spain) Huston recommended parallel DNS queries and a v6 connection request when AAAA records are sent back. Firefox seemed to work well according to Huston's results as they send SYN requests in parallel, yet Huston said, it might not be on by default.

For those who will have dual-stack connectivity during World IPv6 Day, it might therefore be good to check their Firefox configuration. At the RIPE meeting there was yet another pitch for World IPv6 day on June, 6. Yet up to today the network operator (48) and more so the vendor (3) participation list looks rather slim. With regard to network operators, from Europe there are still mainly research networks participating (beside French pioneer Free and Dutch XS4All). For the US there are at least Comcast, Time Warner Cable and AT&T as large operators committing to the 1 percent IPv6 traffic mark.

Abuse WG

But Klaasen, Anti-Terror expert at the Dutch Ministry of the Interior, presented Clean IT, an EU project to develop guidelines and best practices fighting terrorism on the Internet. The Justice and Interior Ministries of the Netherlands, Germany, the UK, Belgium and Spain have partnered for the project and at their upcoming fourth session in June in Berlin beside discussing the draft document on principles and best practices also want to talk about the establishment of a standing platform for “private-public-partnership”, Klaasen said. Klaasen explained that the project did look at the Internet as a target for, but also as a weapon and a resource for terrorists.

The project obviously hopes to rally support from providers for “cleaning” the Internet, as, according to earlier versions of the document, “governments do not have the resources (and ambition) to control the internet traffic”. Providers may not really look forward to private cleansing, especially when reading article 11 of the 0.35 document:

> “Laws and regulations determine what is unlawful. Unequivocally unlawful use of the internet for terrorist purposes must be addressed by ISPs or their clients after being notified. What constitutes unacceptable use can only be determined by ISPs.”

Klaasen said during the RIPE Abuse WG session that the “process of radicalization itself” or “recruitment” or the “use of social media” was not illegal. “It's very difficult to define when the threshold of illegality has crossed. This is what we try to define and in this context we try to find best practices we could use.” How far providers should do the policing or even preventing of later illegal acts is not yet clear from the documents.

> An updated version of the document now has deleted the part on “unacceptable” content, yet in a new “best practice”-part added a provision that providers should:
>
> “Ban illegal terrorist use of the Internet in their terms of service/business conditions and acceptable use policies. This would allow providers to take action against clients using their platform for terrorist purposes and thereby limiting the scale of terrorist incitement, recruitment and training opportunities.”
>
> One has to wonder why there would be a need to exclude “illegal terrorist use” of one's service when it is illegal according to existing legislation? The other new best practice proposals include a

"flagging/reporting button systems", notice and take-down and one provision on awareness, education and information.

Reactions at the RIPE meeting were mixed, with Database WG Chair Wilfried Woeber warning that infrastructure, once established, often seemed to invite its use for a variety of reasons. Filtering originally developed for fighting child pornography being eyed by copyright enforcers was only one example. Klaasen acknowledged during the session that some of the proposals in the Clean IT project could conflict with privacy and data protection provisions as currently reviewed in the EU. Therefore the Clean IT project had included NGOs, Klaasen underlined. When asked which NGOs were part of the discussions he rejected to answer, getting back with an answer to this reporter three weeks later. According to the information given the NGOs participating were:

- LICRA (www.licra.org)
- INACH (www.inach.net)
- HCC (www.hcc.nl, this is in Dutch only, HCC is Europe's biggest computer end-users association)
- ISOC Belgium (www.isoc.be)

According to information from European Digital Rights (EDRI), who declined to participate in the project, ISOC Belgium was not officially participating (only an employee in a personal capacity); HCC was rather an industry association than an NGO; INACH was an anti-hate-speech organisation, similar to Licra, the International League against Racism and Anti-Semitism (motor of the well known French Yahoo case). EDRI underlined that there were no human rights, free speech or data protection organisations participating.

The discussion about a future Abuse Role record for RIPE resource holders is still ongoing.
We have two broad categories and that's abnormalities within Internet number resource registrations and violation of the copyright or intellectual right of the RIPE NCC.

ENUM - to close or not to close?

Can the ENUM working group be closed? Despite a full agenda there are those who think it is time to close the group, or at least move it to dormant.

Alexander Mayrhofer from nic.at gave a roundup presentation about success, failures and alternatives of the protocol. ENUM had in the first place succeeded not in user ENUM scenarios (too complex) or as infrastructure ENUM version (because network operators were not keen to openly share their data), but as Private ENUM. Private ENUM is used inside network operators networks, within a group of operators or for VoIP peering. Operators were using private ENUM for internal routing queries or to find out who is the carrier for a number, and if the number looked up is portable, or who a caller was (heavily used in the US, according to Mayrhofer).

One example for using the protocol as private ENUM was given by Wolfgang Tremmel from the German Internet Exchange DeCIX (jointly with Xconnect), which in addition to its data peering offer starting in July 2012 offers a "voice exchange" for customers. ENUM there is used for querying, while SIP is used for the processing of the calls. DeCIX was targeting between 50 and 100 customers for the voice exchange offer.

Questions raised on the new service were how many changes to the ENUM protocol made so far (including source and destination number in a query which is not compatible with standard ENUM implementations) and potential enhancements in the future would distinct the protocol used from standard ENUM.

DNS

The DNS working group talked about DNSSEC in the first place, with several presentations, including one made in plenary by Ed Lewis from NeuStar, suggesting that there was a need for additional guidelines for DNSSEC operation.

Lewis, who mainly pointed to a gap between operators and developers, asked for a much more definitive BCP document and better means (tools) to track the capabilities of clients and thus helping to decide "when a new parameter is understood by enough clients and how to trigger tech-refresh at the the client end". The most guidance needed, he said, was with regard to cryptography to assist determining when to switch algorithms and how parameters impact performance.

According to a NeuStar study, 82 TLDs currently are signed (27 percent of all) with 19 starting since June 2011 and one abandoning DNSSEC again. What Lewis found was that most of the DNSSEC operated zones (90 percent) used only one of two cryptographic algorithms and the same number did use the same set of sizes for their keys.

Lewis findings were supported by findings in Sweden. A health check of DNSSEC for Swedish zones (part of a larger Internet health check including net neutrality) by .se found many most domains use RSA 2048 bit keys for the key signing and 1024 bit for the zone signing keys. Often signatures were too short or unexpectedly long, Patrik Wallström from .se reported. He said that the publication of type 2 DS keys was sufficient and that there was no need of double publication. Also the DNSSEC health check showed that too often SOA Expire lacked a connection to RRSIG expiration time and this should be reviewed. .se had tried to support DNSSEC deployment by active checking of DNSSEC status of zones in .se and is providing a tool for checks for the providers. A DNSSEC error function allows to quickly detect problems when transferring signed domains. Wallström said that additional, light-weight guidelines for operators were necessary.
The code for the DNSSEC health check can be found here.

Yet another set of new guidelines were announced by Roland M. van Rijswijk, from SURFnet Middleware Services. Rijswijk, who faced unavailability of the surf.net zone after DNSSEC signing, found that there is a problem with "ancient firewalls" that blocked UDP fragments at the service networks edge. Firewall checks were necessary before one started DNSSEC validating.

It looks like there will be several best practices documents ¨C in addition to the operational IETF RFC for DNSSEC.

The next RIPE meeting will be in Amsterdam, September 24-28.