



# **Report of RIPE 63 Vienna**

**31 Oct – 4 Nov, 2011**

**by Monika Ermert**

---

**for the CENTR secretariat**

## Table of Contents

<b>Highlights .....</b>	<b>3</b>
RPKI.....	3
Main Concern: The potential abuses of certificate revocation.....	3
Ever closer to the core: Filtering and Blocking .....	4
Which jurisdiction? .....	5
Enduring Pain – a theory on effect of a prolonged delay of IPv6 deployment (including an update on IPv6) .....	6
RIPE Future .....	6
<b>News from the Plenaries, WGs and BoFs .....</b>	<b>7</b>
DNS WG .....	7
Knot DNS and Yadifa.....	7
More new Tools for the DNS .....	7
Address Policy .....	8
IPv6.....	9
Cooperation WG – Who to cooperate with? .....	9
<b>RIPE News .....</b>	<b>10</b>
Charging Scheme rejected for the first time in RIPE history .....	10

## Highlights

### RPKI

After a heated discussion the Board of the RIPE Network Coordination Center (RIPE NCC) cleared the way to continue with the implementation of PKI for the routing system ([RPKI](#)). The RIPE community is clearly split about how fast and how far they want to go with RPKI.

The nearly finished IETF standard is similar to DNSSEC in its attempt to allow cryptographical checks if a route announcement is made by an authoritative source. Route hijacking – or the much more prevalent mistakes in routing announcements – is expected to be tackled by this. The long-term goal is to develop the system further to not only secure route origins, but also complete routing paths. Experimental implementation of the latter was presented by Randy Bush arguing that the necessary capacity of routers would be available in a few years.

The RIPE NCC started to officially issue certificates for its members (via its registration portal) last January and there are close to 700 certificates in the database (IPv4-, IPv6- and autonomous system numbers). For around 400 there are Route Origin Authorizations (ROAs) stored in the system. For the time being, RIPE NCC offers the services as a hosted system for Provider Aggregatable (PA) space. According to an announcement on the RIPE NCC website, LIRs should also be free to set up their own Certification Authority underneath and sub-certify resources of their customers.

A very small majority (the motion passed with 120 to 116 votes) agreed at the Vienna AGM to allow the RIPE NCC to go ahead. The minority was in favour of slowing down the process at least somewhat, and for the time being only agreeing to issue certificates, but not to provide ROAs hosting. While some proponents like Rüdiger Volk (DTAG) said this did not make a difference for those who wanted to act as a CA of their own, obviously many members felt the compromise would at least send the signal that there were still open questions from the community that had to be dealt with.

#### *Main Concern: The potential abuses of certificate revocation*

Malcolm Hutty, Director of Public Affairs at the London Internet Exchange and President of the European provider association EuroISPA, had started to question the RPKI plans at RIPE 62 in Amsterdam and had clearly denied support to a policy proposal tabled at the RIPE Address Policy WG that would have approved the existing practices for RPKI without community discussion by the RIPE NCC. During a panel discussion Hutty reiterated concerns that a routing system that provides for effective de-validation by the top instance in the hierarchy would make the routing system an easy and attractive target for attacks, not the least for law enforcement agencies or even private parties bringing complaints against sites in a network.

So far, Hutty explained, when approached by law enforcement – something which happens on a regularly basis according to reports by the RIPE NCC staff –, the RIPE NCC could point to the lack of effectiveness to withdraw allocations because the revocation had not direct impact on how the respective address range was being routed by the many thousand partners in the routing system. Assuming that participants in the routing system integrate automatic validation in their routing filters, the de-validation by RIPE NCC – either ordered by a government agency or decided upon by RIPE because of non-payment of member fees – could result in routes being dropped by at least parts of routing partners.

The argument is accepted by many, including those who have taken part in the development of the RPKI protocols like Randy Bush. Bush said during the panel discussion that there was a chance that „people in funny clothes carrying guns“ would indeed try to use the system, on the other hand technology in no way could stop these efforts, but engineers still had to try to make the routing system more secure. „I want to

stop the idiots“, he said. But there is no agreement if RPKI is balanced with regard to the costs (mainly the social, political costs) and the benefits in security. Sascha Luck from the Cork Internet Exchange said that RPKI reminded him of tanks rolled in against what he said were minor problems of the routing system.

Hutty's opponents in the panel discussion were two US-based developers, Stephen Kent (BBN) and Sandy Murphy (Sparta), both of whom have pushed the finalization of the standard documents as part of ongoing projects of their companies undertaken with US government funding. Sandy rejected that there was a fundamental change because there was no new hierarchy put on top of the routing system (Sandy said it only mirrored the hierarchy of resource distribution). This was heavily challenged by several RIPE members including Wilfried Woeber (University of Vienna/ACOnet), who in fact warned to think about creating a single point of failure in the routing system.

In talks with concerned RIPE members Kent said that there was a possibility to put the RPKI trust anchors in various places to allow, for example, those afraid of Dutch Court orders to get an alternative route view. Kent named for example the Electronic Frontier Foundation. An N of M system that would put the trust anchor information in various sites and allow computing the validity based on a score system would overload the system, he said.

Beside these substantial points, Hutty declared unacceptable that the RIPE NCC had pushed forward RPKI deployment in the complete absence of a community policy. In fact, the policy tabled (to adopt the RIPE NCC best current practice) had not reached consensus and had been withdrawn by the author, IP Address Policy WG chair Sander Steffann. RIPE NCC CEO Axel Pawlik said after the voting that he saw it as a clear signal that the NCC had to be careful about the project.

Some RPKI issues were not tackled due to the fundamental debate about the technology. One of them is the question about a potential completely centralized trust anchor system at IANA: After having rejected IANA as a potential trust anchor in 2010, the Number Resource Organisation (NRO) sent a letter to ICANN in spring 2011 asking for a discussion about a centralized solution. At the meeting in Dakar, according to Pawlik, NRO/RIR representatives told ICANN that they were still discussing the issue in their home communities and there was not yet a need for ICANN to address the issue.

### **Ever closer to the core: Filtering and Blocking**

Following the new RIPE fashion to have not only „lightning talks“ but also more panel discussions, the DNS WG spent some time on challenging the discrepancy between the promotion of the “Response Policy Zones“-feature in BIND by the Internet Software Consortium (ISC) and its founder Paul Vixie on the one hand, and Vixie's activities as an outspoken opponent to DNS-blocking measures in current US draft law initiatives, namely the Protect IP Act

Vixie, together with other “Internet celebrities” like Steve Crocker, Dan Kaminski and VeriSign Chief Security Officer Danny McPherson sent an open letter to the politicians that tabled the Protect IP Act (earlier the draft law was called COICA) warning against the inefficiency of such blocking and against negative side-effects for example for DNSSEC-securing of the last mile. While blocked sites would remain inaccessible regardless of DNSSEC and the user's DNS client would just know that it is being lied to, “it won't know whether the lie is the result of court-ordered DNS filtering or criminal interference with the user's DNS lookup”. Vixie and the other signatories of the letter warned that “DNS filtering and Secure DNS are mutually incompatible”.

Against this background, said RPZ that actually rewrites answers is not accepted according to local policy, something that Patrik Fältström from CISCO rejected especially because of the negative effects on non-web applications. While blocking was a last-resort, rewriting was a complete no-go, said Fältström,

who is also responsible for ongoing work about the issue at the ICANN Security and Stability Advisory Committee. Participants at the DNS WG panel expressed considerable concerns about the RPZ-feature in BIND. “It sends a rather nasty message that it is ok to do this kind of thing”, Jim Reid said.

João Damas (ISC) had to defend RPZ and argued that a certain “manipulation” already existed in the DNS by catching. “The answer you get back is never or not necessarily the same thing that the authoritative server provided to begin with”, he said. But mainly he pointed to the pressure of customers, something confirmed by Olaf Kolkman of NLnetLabs. What has made ISC go this way was the long discussion about the fact that there were already people out there deploying software to do the rewrites. “There are companies out there that have their own software or hack BIND to provide this software to others and they’re selling it”, João said. Rather than driving people away from BIND the company did decide to offer the functionality themselves, which was turned off by default. Damas said that the goal was to give the good guys “another stick” against Spam and Malware. Damas also presented ISC’s Passive DNS System (DNSDB) and Security Information Exchange (SIE) Program that is targeted to use passive DNS (and other collected DNS data) to analyse malicious behavior and share it with partners and interested parties like law enforcement. Passive DNS data for the system are collected over a dedicated sensor network.

### *Which jurisdiction?*

Fältström said that the biggest problem with regard to filtering and blocking at the moment was that a lot of DNS blocking and filtering was lacking due process. Procedures and decision-making processes used for take-down at registries and registrars were “not based on any kind of legislation that had been scrutinized according to jurisdiction.” Getting clear laws and rules was a priority.

But Damas asked the question of which national legislation would apply and pointed to the take-down of the Spanish website [Rojadirecta.com](#), which had been judged within Spanish national law by two courts. [Rojadirecta](#) is still [redirected](#) to a US government site and subsequently [rojadirecta.es](#) has also been dropped by Google from the list of search results following a complaint by the Major Baseball League based on the Digital Millennium Copyright Act – which is a US, but no Spanish law. Cross-border implementation of national laws is one of the hot issues at the EU, too.

While Swedish government representative Maria Hall said at the RIPE DNS blocking panel that there were discussions of EU governments about the effect of blocking on the global Internet infrastructure, governments therefore had to understand the differences between blocking, rewriting and other alternatives. In the debates about the future EU Directive against Attacks on the Information Systems at the Committee level of the European Parliament, an amendment to the report of the Industry, Trade and Research Committee has been tabled that requests to make blocking an IP address or domain a criminal offence. The ITRE rapporteur decided to not table it now, but the lead Committee is the LIBE Committee.

Matt Pounsett, representing Afiliias, reminded spectators that in many cases of interventions triggered by malware the registries handled the issues as violations of the acceptable use policy. So contractual, instead of national law was governing many of the take-downs. While Afiliias certainly preferred that answers sent out by them on DNS requests were visible to people, Afiliias, too, did participate in take-downs on a case by case basis. DNS WG chair Peter Koch asked how the actions of private companies – be it malware take-downs or RPZ-filtering - were governed and what procedures were in place. Fältström underlined in his reaction to Pounsett that human rights including freedom of expression could not be negotiated away in a contract.

## Enduring Pain – a theory on effect of a prolonged delay of IPv6 deployment (including an update on IPv6)

APNIC Chief Scientist Geoff Huston in the closing plenary expressed his [concerns](#) about potential fatal effects that a prolonged transition could have to the deployment of IPv6. Huston, who said the community was doing bad with 0,3-0,4% IPv6 last-mile-traffic (compared to 39 percent dual-stack capability in the transit networks, and 50% IPv6 support in devices deployed), currently warned IPv6 could become “a distant dream” if network operators would use existing IPv4 resources and manage scarcity with technologies like Carrier Grade NATs, Content Delivery Networks or Application Layer Gateways.

The more expensive and “shiny” the transition mechanisms for sharing and rationing IPv4 addresses were, the longer network operators would expect to use them in order “to protect the value of the additional investment” made, thereby operators might lock themselves into the “transitional” service model for an extended or even indefinite period. Given that the various regions of the IP-address registries are expected to run out at different times, Huston said, the regions could go off in completely different directions with regard to IP connectivity – up to the point that universal connectivity would be lost due to the various scenarios the regions have transitioned to.

RIR	Predicted Exhaustion Date *	Remaining Address Pool (24 Oct 2011)
APNIC	19 April 2011 (actual)	1.20 /8s (0.3 /8s rsvd)
RIPE NCC	23 June 2012	3.91 /8s
ARIN	4 June 2013	5.91 /8s
LACNIC	25 February 2014	4.27 /8s
AFRINIC	23 June 2014	4.38 /8s

Exhaustion for the RIPE region according to Huston's calculations (see his table above) are expected for June 23<sup>rd</sup>, for example, while ARIN in North America will only run out a year later and AfriNIC would still have IPv4 addresses the year after. So is there really a risk for a breaking up of the universal net? Many observers said such a scenario was a little dramatic, yet all the additional boxes put into the network certainly would make interconnecting a little harder and “potentially a little less predictable and stable”, Alex Le Heux, from the Registration Service of the RIPE NCC, said. Le Heux also said with regard to RIPE run-out that it was impossible to predict because as soon as requests by big customers came in, depletion could be much closer. A RIPE NCC [statistics of current allocations](#) in all five RIRs was presented in the plenary.

Huston's recommendation to the RIPE community was not to wait with transition for IPv6 but to “bring it on” instead of making large investments in transition technologies to manage scarce IPv4 addresses. As in earlier talks, Huston pointed to the public interest angle of the transition and he asked that operators did look at the broader picture and not stick to the rule that the transition “is not happening until it happens to me”.

### RIPE Future

With the end of IPv4 allocation – and the change to allocation of much more spacious IPv6 blocks – the RIRs, too, have to consider their future path. While transition management – and the management of a final panic – after the last free /8 has been depleted, according to soft-landing policies in different RIRs, ISPs still can get a one-time (but more tiny than usual) last allocation – still needs some effort with transition to IPv6 allocations requests would become less frequent. For some more critical observers services like certification and also additional measurement projects like the developing [ATLAS probe](#)

[network](#) (the plan is to have 4000 deployed in 2012) are also an expression of the need to look for new tasks.

RIPE NCC's Chief Scientist Daniel Karrenberg, who also presented the Atlas project in a [keynote talk](#), said that more RIPE NCC instead of less was needed. "Today the facts are that the Internet business is not generally shrinking and that the RIPE NCC membership is still growing at an astonishing pace. So, do we really need less RIPE NCC? Or do we rather need more?", Karrenberg asked. He also touched on the so far agreed upon "fair enough"-consensus for the charging scheme. But later in the week the AGM meeting rejected the proposed new charging scheme for the first time in RIPE's history (see below).

## News from the Plenaries, WGs and BoFs

### DNS WG

Besides this highlighted discussion on Blocking and Filtering there were presentations on an new monitoring system, a DNSSEC trigger tool yet under development, new authoritative name server software and the recent DNS Easy and SSR meeting of „top security experts“ in Rome. Joe Abley from ICANN/IANA asked RIPE members to comment on the six IDN variant reports prepared by expert groups, which are open for public comment until November, 14<sup>th</sup>.

#### *Knot DNS and Yadifa*

Two new authoritative DNS name server software implementations were presented during the DNS WG: Knot DNS, which has been developed by engineers in the CZ.NIC Labs, and Yadifa (Yet Another DNS Implementation For All), which is the product of a small developer group of EURID, the .eu registry. Both registries said to this reporter that they were convinced that there was a need for additional diversity for authoritative DNS name servers and both in fact intend to rollout their respective servers alongside in addition to their BIND and NSD servers. "If either NSD or BIND fails for some reason, you lose 50 percent" today, explained Ondřej Surý of CZ.NIC.

Knot DNS is already available in Beta version for testing by everybody. Yadifa will be launched in February next year, according to Eurid's time table.

Another reason for the development, according to Peter Janssen, is also that the current BIND version is no "speed king" and still forces the registries to restart the server when updating the zones. Both servers offer dynamic updates and also additional speed, depending on the operating system up to 30 percent speed can be made (the biggest jump is seen on FreeBSD servers). Yadifa, in contrast to Knot DNS according to Janssen, attempts to offer "something for Windows", too. Both support also various Linux distributions and MacOS X.

More diversity in the name server gene pool was welcomed by many, including RIPE's Chief Scientist Daniel Karrenberg, who offered to use a tool for testing that he has developed for NSD before its launch. Several larger European registry operators said that for the time being they were prepared to test, but would not implement the two newcomers. DENIC and AFNIC (as well as CZ.NIC) are sponsoring the BIND 10 effort.

#### *More new Tools for the DNS*

As still a "tool for geeks" Olaf Kolkman from NLnet Labs presented the [DNSSEC trigger](#), which shall allow to bring DNSSEC to the last mile. The tool will reconfigure the setup of a laptop or PC so that the recursive name server lives on the local interface. For the moment the tool was only available for MacOS X, further releases were prepared. The DNS trigger would use the Unbound control mechanism for changes or reconfigurations on the fly and check if DNSSEC validation is working. For the probing the



local machine would ask the recursive names server via DHCP and would try to do DNSSEC via this channel, Kolkman explained. The tool and information about it can be found on a dedicated NLnet Labs [page](#).

A new tool for DNS configuration, control and monitoring ([DNSCCM](#)) was presented by Sara Dickinson from Sinodun Internet Technologies. DNSCCM is based on the Name Server Control Protocol that is under development at the Internet Engineering Task Force. It shall allow cross-platform managing of DNS servers. It is built on Yuma tools, open source (using the Yang/Netconf toolkit) and for authoritative name servers for now. The current version (with an alpha release expected in December or January) only supports NSD 3 and BIND 9 (BIND 10 was on the to-do-list). The project page is [here](#).

## Address Policy

There is a lot of IPv6 space, why not give out more? One current policy proposal asks to allow allocation of /29 also to smaller operators in order to enable them to do fast IPv6-allocations like in 6RD ([2011-04](#)). The so far allocated /32-blocks would then be upgraded to /29, according to the proposal. There is some reservation against pointing to specific transition technologies for address policy. Discussion therefore is ongoing, also on the question of how much space should then be reserved for future allocation.

Another IPv6 policy proposal still under discussion argues to abolish the multi-homing restriction for IPv6 provider independent (PI) resource allocations [2011-02](#). According to the proposal there were enough (strategic) reasons for companies not to make the step towards an LIR membership, but still running their own infrastructure. Alongside this proposal the discussion about the possibility to eliminate the difference between PI and PA space still exists. With regard to the argument that the routing tables might get too large, there was an interesting presentation by Geoff Huston who showed that, so far, despite growth of the Internet in general, and IPv4 and IPv6 allocations in particular, the expectations that routing tables would explode with IPv6 has not materialized. For 2016 Huston calculated 557.000 v4 entries and 65.000 v6 entries in the routing table (compared to 2012 385.000 v4 and 10.000 v6 entries).

The third active policy proposal is a special IPv4 reservation for Internet Exchanges ([2011-05](#)), which seems to get easy support.

An ongoing policy discussion beside the PI-PA development is transfers of resources across RIR boundaries. The way forward for Inter-RIR transfers seems to be cleared by a step of the APNIC community, which just changed their own transfer policy from non-needs-based to needs-based. ARIN, which had hesitated to allow Inter-RIR transfers to regions without needs-based allocation and transfers principles, now might be able to take the next step. With the change in the APNIC policy transfers might become possible, and also this might pave the way for an IANA global policy to hand out addresses it might receive from legacy sources after the run-out.

The post-run-out phase is still an issue of various debates. In Vienna there was again a short update by RIPE Chair Rob Blokzijl about how to address post-run out IPv4-governance. He wants to have the RIPE focussed on the clean database instead of a lot of rules and obligations. A liberal approach, he hopes, could also bring more legacy space into the RIPE regime. The RIPE NCC for the Vienna meeting had included letters to those RIPE members (or RIPE participants) that are responsible for legacy allocations asking them to update the database and to consider to "legalize" this space. The RIPE NCC's efforts to bring in legacy space are reaching out from RIPE NCC members to non RIPE members over the coming month.

With regard to the effects of smaller allocations due to the current run-out fairly policy (demand for 3 month), RIPE NCC reported that it was visible in the statistics of allocation. There were more, and more smaller allocations. The bulk of address space nevertheless did go to large allocations.



## IPv6

A panel discussion in the plenary brought together four CPE router vendors who all underlined that their routers supported IPv6 with some marketing numbers put forward, like 10 Million IPv6 capable D-Link devices sold or the pointer to a commercial roll-out of the AVM Fritz Box in Q2/2010 via Access4All in the Netherlands. Carl Wuyts, System Architect Networks, at Technicolor said for Carrier Grade NATS there might be some degradation and the need to split contracts with customers respectively in different services classes. Technicolor has upgraded the IP stack of its own DSL Ethernet gateway to IPv6 (roll-out 1/2012). The CPE vendors on the panel said they were waiting for the operators to move (see enduring pain, above). For the short presentations by the CPE-vendors see [Technicolor](#), [AVM](#), [D-LINK](#), [Cisco](#).

Constanze Bürger, Ministry of the Interior Germany, gave an update on preparations for transition to IPv6 in the German Public Authorities Network. The German Government received a /26 from RIPE and is sub-allocating /32 to the German Federal States, which currently are developing their respective address plans (either separate plans for State Government, Military and other SubLIRs or one common plan for the State). An IPv6 Working Group brings together the experts of the 16 Federal States for information sharing and planning, a RIPE training has been organized. A matrix comparing the various profiles for IPv6 deployment like the RIPE-501 recommendation (listing relevant RFCs), the NIST profile, IPv6Ready profile shall assist procurement of hardware, software and services and transition to dual stack in general. Bürger also pointed to a recently accepted 6 Million Euro EU project for the transition of public administrations to IPv6, GEN6 (no website yet), a presentation about the project listing the partners can be found [here](#).

Beside that early planning for another edition of the World IPv6 Day (presented by Google) an IPv6 Week in Latin America was announced.

## Cooperation WG – Who to cooperate with?

The main discussion in the Cooperation WG was triggered by a report from Nurani Nimpuno from Netnod about the ongoing consultation in the UN Committee on Science and Technology for Development's Working Group on improvements of the Internet Governance Forum (IGF). The CSTD started to work a year ago under Swiss Chair Frédéric Riehl only to fail to produce consensus and stop for some time. Nimpuno pointed to the different opinions governments bring to the table when it comes to the talk-only, open, multi-stakeholder forum. Nimpuno came back straight from the restarted WG under a new, Hungarian Chair, Peter Major, to the RIPE 63 meeting.

While she said there had been considerable progress, nothing was decided and two more meetings were planned before a final report would be sent to ECOSOC, if possible. Nimpuno said with regard to funding, a problem of the IGF, there was little hope that the IGF would be officially funded by the UN. The IGF in fact is an activity of the UN Secretary General, for the time being the position of the executive secretary is still vacant (since Markus Kummer left in January 2011), Also there is no IGF-Chair, a position held by Indian diplomat Nitin Desai for the first five IGF years (2006-2010). A report about the RIPE NCC [activities at the IGF Nairobi](#) was presented by Chris Buckridge from the NCC.

Nimpuno reported in Vienna that at the first meeting of the CSTD WG 50 percent of government members did not show up, a possible hint for lack of support. A positive effect was that civil society and the technical community<sup>1</sup> did take a bigger role in the discussions. Quite obviously several governments

---

1 Technical Community members of the WG are Constance Bommelaer (ISOC), Samantha Dickinson (APNIC), Baher Esmat (ICANN); Business Community: Oscar Robles- Garay (NIC México), Marilyn Cade (mCADE), Patrik Fältström (Cisco Systems), Jimson Olufuye (ITAN), Christoph Steck (Telefonica), Theresa Swinehart (Verizon); Civil Society, Izumi Aizu (Tama University), Anriette Esterhuysen (APC), Parminder Jeet Singh (IT for Change) Marília Maciel (Fundação Getulio Vargas) Wolfgang Kleinwächter (University of Aarhus)

are looking for the long-standing changes in the Internet Governance arena in other places (and not so much in the IGF, because of the IGF's talk-only mode).

Nimpuno pointed to several other processes going on in parallel, especially the India Brazil and South Africa Proposal (IBSA, see recent CENTR report on the IGF) for a new UN body for public policy issues in Internet Governance. The Indian government has tabled the request for the UN General Assembly in December. Another proposal put forward at the UN level is an code of conduct for information security (affirming national sovereignty over nation's networks, and promoting an international Internet management system) – this one initiated by China and Russia. And there are more places where governments are looking for “Principles for Internet governance” with the London Cyber Conference on Nov 1-2 (to be followed by conferences in Hungary and South Korea) only the latest one. Nimpuno recommended coordinating presence at the variety of different meetings if possible.

The Cooperation WG talked about how cooperation could go beyond just reporting back to each other, so far the Cooperation WG has not been attracted a lot of governments (see RIPE 62 CENTR Report) with Sweden, Germany and RIPE's host country Netherlands attending most sessions. [Andrea Glorioso](#) from the European Commission introduced himself via Skype to the Cooperation WG, but announced that the Commission could not speak about IP address issues exclusively to RIPE. This resulted in a lot of head shaking by participants in Vienna.

## RIPE News

### Charging Scheme rejected for the first time in RIPE history

For the first time in RIPE history the proposed charging scheme was clearly rejected by the community. With 148 against 110 votes the new scheme was voted down, as many ISPs were afraid of a rise in costs to them – occurring in terms of cutbacks in their own business. The new charging scheme wanted to differentiate members in 10 member classes (up from five) with fees according to their size. Secondly Ipv4 address allocations would have been charged extra with 50 Euro per allocation, IPv6 addresses and AS numbers would be free. To make the RIPE NCC attractive for new members the entrance fee would have been reduced (from 2000 to 1000) and also there was no fee for legacy addresses. What made some providers weary was that according to the new scheme private IP address blocks (used by a more or less distant customer) would be calculated as part of the overall number of allocations for a LIR. After the rejection of the new charging scheme, the RIPE NCC now has to calculate member fees for 2012 based on the existing scheme, and to use some of the reserves of the organisation to fill gaps between income and expenses. “Vagueness” in the projected 2012 budget for the organization has also been brought up as an argument for the no-votes on the membership fee proposal.

A quite interesting development is the more active role the RIPE NCC obviously wants to take in the Middle East and Eastern Europe. Paul Rendek who acts as Director of External Relations is now based in Dubai. The RIPE NCC regularly organizes regional meetings. The last meeting is in Moscow, 28-20 November, following meetings in [Dubrovnik 2011](#) 07 Sep 2011, [Moscow 2011](#) 08 Jun 2011, [Saudi Arabia 2011](#) 14 May 2011. The most recent Middle East Network Operator Group Meeting took place in [MENOG 9/RIPE NCC Regional Meeting](#) took place in Muscat, Oman from 25 September - 4 October 2011.

RIPE 64 will take place in Ljubljana Slovenia, in May 2012