A Happy Story of Inter-RIR Transfer of Legacy Blocks from ARIN to RIPE

2016.04.03

Randy Bush <randy@psg.com>

Legacy at ARIN

- A legal mess; no lawyer will let one sign the LRSA
- You are not a second class citizen; you are not a citizen; you have no rights
- The policy community was been captured by Trump's Tea Party over a decade ago
- But the HostFolk etc. are great; trying to keep the net running despite

RIPE is Legacy Friendly

- A few years back, Legacy and PI policies were rationalized
- One can be a Legacy Member and lose no rights in one's address space
- Or you can be sponsored by a friendly LIR and lose no rights
- In either case, you pay and you get all services, DNS, IRR, RPKI, ...

RGnet's Case

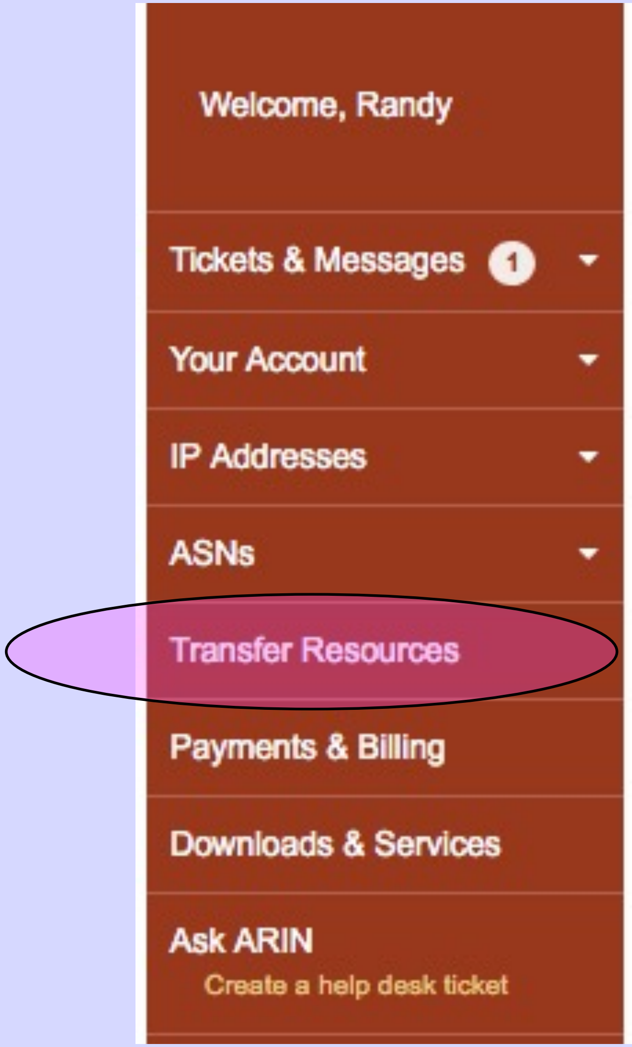
- RGnet had four legacy blocks in the ARIN region from before dirt was invented
- I have been working on RPKI for way too long and wanted RPKI service
- RGnet also does a bit of infrastructure in the RIPE region
- One of my $dayjobs is a RIPE member

What the Heck

- So it seemed to make sense for RGnet to have a go at transferring the four blocks from ARIN to RIPE
- The thought of the bureaucracies was daunting
- But their processes seemed documented
- And, as I was raised by five women, I can follow orders

January 26

- A kind and patient RIPE hostmaster explains I must first fill out the ARIN transfer request
- Log in and it's on the front page!



Welcome, Randy

Tickets & Messages 1

Your Account

IP Addresses

ASNs

Transfer Resources

Payments & Billing

Downloads & Services

Ask ARIN

Create a help desk ticket

ARIN loves online forms
I will not bore you with
the details

Policy Hole: You can not transfer ASNs!

ARIN Bureaucracy

- The web silliness eventually yielded a form letter I had to fill out, sign, etc. and 'Notarize,' a strange American custom certifying my signature
- We have no such thing in Japan
- So I agreed with ARIN to give them the properly done form at NANOG

February 10

- I paid ARIN US$500 for the process
- I give the form to ARIN HostFolk at NANOG in San Diego
- Their corporate jet was already in use for political junkets, so it would wait until the poor HostFolk flew home on a commercial carrier

February 19

- RIPE HostPerson tells me that "We have been notified by ARIN for the inter-RIR transfer request …"
- Asks me to
  - Confirm that I want to recive this transfer
  - Tell of infrastructure in RIPE region
  - Decide: Become a Member, use a Sponsoring LIR, …

Eurocracy, of Course

- I also had to send RGnet LLC's proof of existence
- The Legacy Agreement with a Sponsoring LIR
- Utilization plan for the address space
- I was teaching a security workshop in Auckland, so did not get this stuff done until February 26

Then the Sponsoring LIR went on a Ski Holiday

March 11

- Sponsoring LIR returns from skiing
- We sign the agreement
- And send it to RIPE
- Who notes I forgot to list the resources and offers to fix this
- We say “Yes, please.”
- And RIPE starts to process
- But it’s a weekend

March 15

- RIPE says I need to “Create an Organisation object for RGnet, LLC and let me know the Org-id.”

- And, for each net block, specify
  - netname:
  - admin-c:
  - tech-c:
  - Country:

March 16

- I had not used the RIPE database since 1948
- I had a maintainer ID and existing objects in the database
- So I played Adventure in

  `https://apps.db.ripe.net/`
- And cleaned most old objects up
- And created an Organisation: object

YAY!

```
organisation:   ORG-RG79-RIPE
org-name:       RGnet, LLC
org-type:       OTHER
descr:          RGnet Legacy Holder
address:        5147 Crystal Springs
address:        Bainbridge Island, WA 98110
address:        United States
e-mail:         randy@psg.com
admin-c:        RB366-ARIN
tech-c:         RB366-ARIN
abuse-mailbox:  blackhole@bogus.com
ref-nfy:        randy@psg.com
mnt-ref:        MAINT-RGNET
notify:         randy@psg.com
mnt-by:         MAINT-RGNET
created:        2016-03-15T13:41:51Z
last-modified:  2016-03-15T13:41:51Z
source:         RIPE
```

My Person: Object

```
person:         Randy Bush
address:        RGnet, LLC
address:        5147 Crystal Springs
address:        Bainbridge Island, WA 98110
address:        United States
phone:          +1 330 887 2874
fax-no:         +1 206 973 2762
e-mail:         randy@psg.com
nic-hdl:        RB366-ARIN
abuse-mailbox:  blackhole@bogus.com
notify:         rw@rg.net
mnt-by:         MAINT-RGNET
created:        1970-01-01T00:00:00Z
last-modified:  2016-03-17T09:55:18Z
source:         RIPE
```

See my 2000 rant at https://archive.psg.com/ 000914.ripe-whois.pdf

There was more RIPE DataBase Cruft, but You Don't Want to Know

March 16 Continued

- “We have scheduled with ARIN to process this Inter-RIR transfer and update our registries this afternoon (at approx. 17:00 CET or GMT+1).”
- So hack and go home, eh? At least it was not Friday. ☺
- But the reverse DNS was gonna be a problem, of course

DNS Transfer Gl!tch

- ARIN had to delete their reverse DNS delegations to me
- To get RIPE to delegate required me to create domain: objects
- Which I could not do until RIPE had received the transfer and created the inetnum: objects
- Then RIPE's system had to get ARIN's system to delegate to RIPE DNS

I got up in the middle of my night and created domain: objects

```
domain:    230.83.192.in-addr.arpa
descr:     RG79-192-83-230
admin-c:   RB366-ARIN
tech-c:    RB366-ARIN
zone-c:    RB366-ARIN
nserver:   rip.psg.com
nserver:   nlns.globnix.net
mnt-by:    MAINT-RGNET
source:    RIPE
```

The 18 Minute Gap ☺

- This is a complex process with step by step checks for safety
- So there was a gap of a few hours where reverse DNS did not work
- Luckily these are research networks with no paying customers
- I go back to sleep and wake in the morning to find everything is OK!

Of course Heas noticed the DNS gap and sent a surly email

☺

Six Weeks

Could'a Been Two/Three

No Real Pain

Lots'o Help

Fantastic HostFolk

With Thanks and Amazement

- ARIN HostFolk who patiently helped me through their bureaucracy
- An amazing RIPE HostPerson who not only helped me through the RIPE NCC bureaucracy, but gave me step by step instructions for dummies, which I needed
- And the RIPE and ARIN communities who made Inter-RIR transfer workable

No one will get annoyed with me for overly helping someone from our community (a legacy holder in this case). In fact we are encouraged to do so (as long as it's within the boundaries of our function). The mentality in Registration Services dept. is "if you can take an extra step to help someone then take it" ;)

And now on to the RPKI part of the project

Putting up a CA as a child of RIPE's CA

I Used Dragon Research Labs CA and Relying Party Software

https://trac.rpki.net/wiki/doc/RPKI/RRDPtestbed

XML Upgrade

- RIPE is running old XML and will move slowly to the new Internet-Draft so as not to break things
- Dragon Research software moved ahead
- So, when doing the identity set-up, one has to translate once, child to RIPE and once RIPE to child

First, you need xsltproc

```
    # apt-get install xsltproc
```

Then get the translator

```
    # wget http://subvert-rpki.hactrn.net/branches/
      tk705/potpourri/oob-translate.xsl
```

Then you can convert

```
    # xsltproc oob-translate.xsl RGnetCA.identity.xml
      > RGnetCA.identity-old.xml
```

and upload it to your parent's server.

In return, you should fetch your parent's identity. In RIPE's case, the gui has a link

```
    https://localcert.ripe.net/api/rpki/issuer-identity
```

As the xml crossed the ripe/local xml version boundary, you need to translate the ripe identity into the new xml format and feed this to your GUI or to rpkic

```
    # xsltproc -o ripe-identity-new.xml oob-translate.xsl
      issuer-identity-20160323.xml ca.rg.net:/root/foo
    # rpkic configure_parent ripe-identity-new.xml
    Parent calls itself 'e17841a7-8582-4832-ab81-8644b3d41dba',
       we call it 'e17841a7-8582-4832-ab81-8644b3d41dba'
    Parent calls us 'a5b39a7d-2629-496b-8806-86270050d53a'
    Wrote /root/foo/RGnetCA.e17841a7-8582-4832-ab81-
        8644b3d41dba.repository-request.xml
    This is the file to send to the repository operator
```

umask & uid Pain

- Dumped MYSQL, and Postgres uses uids
- CLI interface, rpkic, does not run as root
- The current directory might not be owned by rpki:rpki
- So it would create files it then could not read etc.
- Code was hacked to switch in and out of rpki:rpki when reading or creating files

TLS Problem

Old Debian and Ubuntu releases run versions of Python old enough that the Python "ssl" module in those versions doesn't support the TLS 1.2 cipher suites, resulting in a TLS negotiation failure trying to talk to RIPE NCC's RRDP server.

I gave up and went to Xenial, Ubuntu 16.04 Beta-2

TLS 1.2 Test

```
$ objdump -T `python -c 'import ssl;
 print ssl._ssl.__file__'` | fgrep _method

0000000000000000      DF *UND*  0000000000000000  OPENSSL_1.0.1 TLSv1_1_method
0000000000000000      DF *UND*  0000000000000000  OPENSSL_1.0.0 SSLv23_method
0000000000000000      DF *UND*  0000000000000000  OPENSSL_1.0.0 TLSv1_method
0000000000000000      DF *UND*  0000000000000000  OPENSSL_1.0.1 TLSv1_2_method
```

All the happy platforms run Python 2.7.11, while Debian Wheezy runs 2.7.3 and Ubuntu Trusty runs 2.7.6.

Xenial

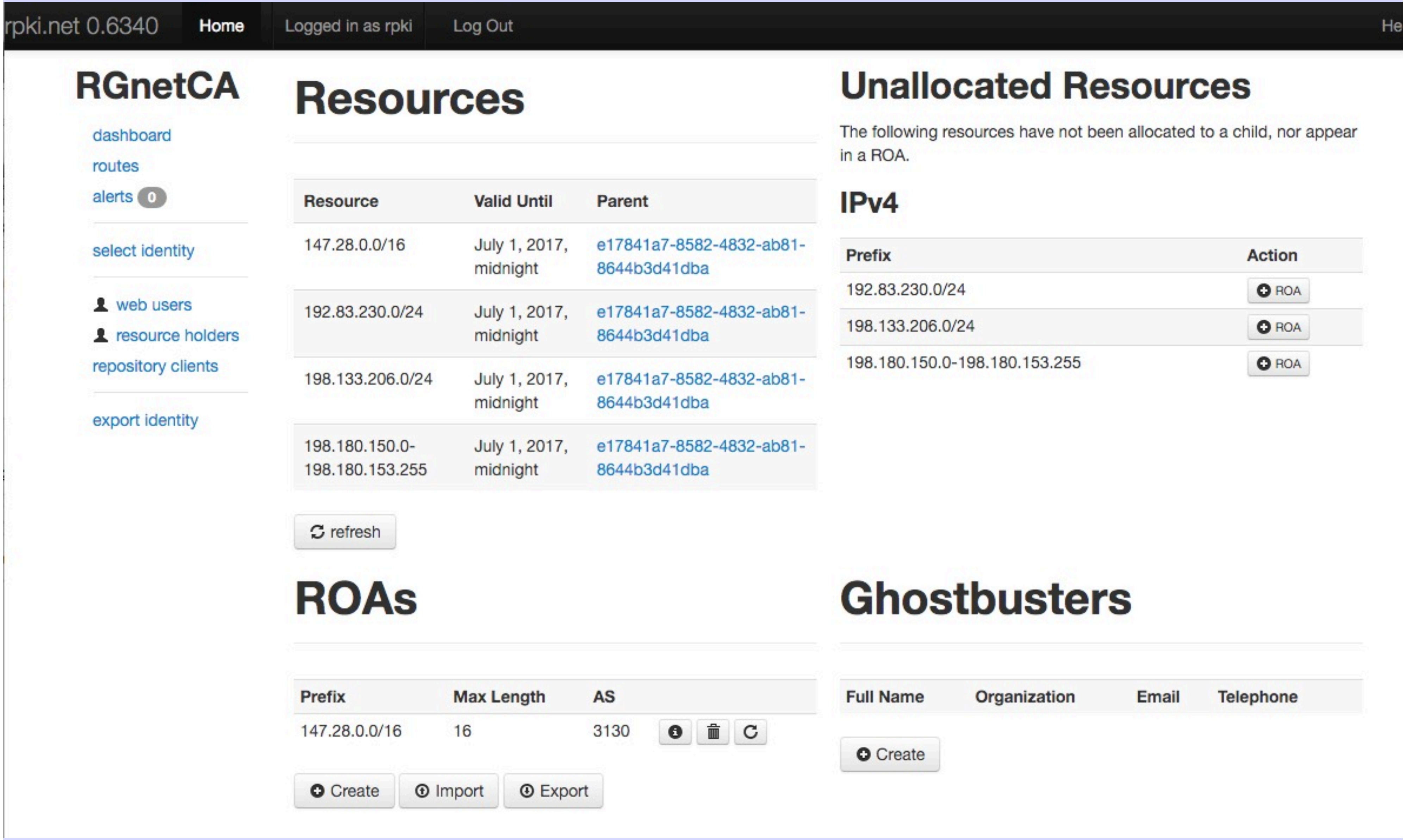
- It is pre-release
- So the daily dist-upgrade from hell
- And it has openssh 7, which has a bunch of changes
- Hash and key length upgrades may bite you

Lets Encrypt and Dane

- Let's Encrypt is a bit of a PITA
- https://wiki.rg.net/wiki/AcmeTinyUbuntu
- But heck, it is breaking the CA cartel

- DANE is another anti-cartel path
- I like to do both, and DANE is much easier
- Just a CNAME pointing to a TLSA RR for a LetsEncrypt certificate chain

And the Result



RGnetCA

- dashboard
- routes
- alerts 0

- select identity

- 👤 web users
- 👤 resource holders
- repository clients

- export identity

Resources

Resource	Valid Until	Parent
147.28.0.0/16	July 1, 2017, midnight	e17841a7-8582-4832-ab81-8644b3d41dba
192.83.230.0/24	July 1, 2017, midnight	e17841a7-8582-4832-ab81-8644b3d41dba
198.133.206.0/24	July 1, 2017, midnight	e17841a7-8582-4832-ab81-8644b3d41dba
198.180.150.0-198.180.153.255	July 1, 2017, midnight	e17841a7-8582-4832-ab81-8644b3d41dba

Unallocated Resources

The following resources have not been allocated to a child, nor appear in a ROA.

IPv4

Prefix	Action
192.83.230.0/24	⊕ ROA
198.133.206.0/24	⊕ ROA
198.180.150.0-198.180.153.255	⊕ ROA

ROAs

Prefix	Max Length	AS	
147.28.0.0/16	16	3130	ⓘ 🗑 ↻

Ghostbusters

Full Name	Organization	Email	Telephone

It's Documented

I try to wiki as much as possible

`https://trac.rpki.net/wiki/doc/RPKI/RRDPtestbed`

And these slides are online as

`https://archive.psg.com/160403.pdf`