Prop 132 (AS0)

Implementation plan, testbed report.

George Michaelson

MELBOURNE, AUSTRALIA 12 – 21 February 2020
APRICOT 2020
APNIC 49
25 YEARS

Prop-132 (AS0) implementation plan

- ***Late 2019**: Explore technology, develop model (done)*
- **Early 2020**: Expose model to community at APNIC 49/APRICOT 2020 Melbourne and discuss open issues
- **Early-mid 2020**: Initial deployment
- **Mid-late 2020**: Report back to APNIC 50 with statistics and status

Prop-132 (AS0) implementation plan

- ***Late 2019**: Explore technology, develop model (done)*
- **Early 2020**: Expose model to community at APNIC 49/APRICOT 2020 Melbourne and discuss open issues
- **Early-mid 2020**: Initial deployment
- **Mid-late 2020**: Report back to APNIC 50 with statistics and status

Implementation stages

- We propose to publish AS0 ROAs in stages to minimize risk:
  1. Testbed with example state. Daily cycle
  2. Launch production service
     - with experimental and documentation address space
  3. Add un-delegated address space
  4. Add returned/reclaimed address space

Why stages?

- Minimise risk:
  - Do the least likely to impact delegated spaces first
    - Then add the things we will delegate, but never delegated yet.
      - Then add the things which have been delegated but were reclaimed and returned.
  - What do people think about this?

Aligned to delegated statistics

- We propose to publish AS0 in a way which permits direct comparison to the visible state of registry as represented by the delegated-extended file:
  - **`ftp://ftp.apnic.net/public/apnic/stats/apnic/`**

delegated-extended stats file

```
2.3|apnic|20200107|129302||20200106|+1000
apnic|*|asn|*|10266|summary
apnic|*|ipv4|*|45341|summary
apnic|*|ipv6|*|73695|summary
apnic|AU|ipv4|1.0.0.0|256|20110811|assigned|A91872ED
apnic|CN|ipv4|1.0.1.0|256|20110414|allocated|A92E1062
apnic|CN|ipv4|1.0.2.0|512|20110414|allocated|A92E1062
apnic|AU|ipv4|1.0.4.0|1024|20110412|allocated|A9192210
apnic|CN|ipv4|1.0.8.0|2048|20110412|allocated|A92319D5
apnic|JP|ipv4|1.0.16.0|4096|20110412|allocated|A92D9378
apnic|CN|ipv4|1.0.32.0|8192|20110412|allocated|A92319D5
apnic|JP|ipv4|1.0.64.0|16384|20110412|allocated|A9252414
apnic|TH|ipv4|1.0.128.0|32768|20110408|allocated|A91CF4FE
apnic|CN|ipv4|1.1.0.0|256|20110414|allocated|A92E1062
apnic|AU|ipv4|1.1.1.0|256|20110811|assigned|A91872ED
apnic|CN|ipv4|1.1.2.0|512|20110414|allocated|A92E1062
apnic|CN|ipv4|1.1.4.0|1024|20110414|allocated|A92E1062
apnic|CN|ipv4|1.1.8.0|256|20110412|allocated|A91E9A58
apnic|CN|ipv4|1.1.9.0|256|20110412|allocated|A92319D5
apnic|CN|ipv4|1.1.10.0|512|20110412|allocated|A92319D5
apnic|CN|ipv4|1.1.12.0|1024|20110412|allocated|A92319D5
apnic|CN|ipv4|1.1.16.0|4096|20110412|allocated|A92319D5
apnic|CN|ipv4|1.1.32.0|8192|20110412|allocated|A92319D5
apnic|JP|ipv4|1.1.64.0|16384|20110412|allocated|A92D9378
apnic|TH|ipv4|1.1.128.0|32768|20110408|allocated|A91CF4FE
```

http://ftp.apnic.net/stats/apnic/delegated-apnic-latest

Motivations for delegated alignment

1. Publicly visible data which will permit anyone to compare AS0 ROA state with registry state
2. Unambiguously defined, regarding ‘available’ and ‘reserved’ status records
3. A simple mechanism to understand and implement.

- What do people think about this? Does this align with your expectations?

Separate Trust Anchor Locator (TAL)

- We propose to deploy the AS0 ROA outcome under a distinct Trust Anchor Locator (TAL). This is for a number of reasons:
  1. Reduces risk, since it moves the process from opt-out to opt-in, to be affected by AS 0 ROA
  2. Permits us to measure uptake and understand it distinctly from other RPKI activity
  3. Separates the AS 0 process out from under our main activity, permitting it to be seen as distinct from normal RPKI processing
  4. Based on experience, we can discuss moving to integration of AS 0 ROA under the main TAL as a second phase.
- Is a separate trust anchor an acceptable initial deployment model?

Other Considerations

- Impact on delegation process.
  - There may be a period of 24-48 hours between the revocation of the ROA and the resources being delegated.
- Understand how the other RIRs will engage in this process, if proposals reach consensus
  - Should this be a global policy so that all RIRs perform the same actions?
- Engagement with wider operations community and IETF

Prop132 testbed

- Up and running: TAL is available at
  - **`https://registry-testbed.apnic.net/as0-test-ta.tal`**
- Equivalent SLURM file available at
  - **`https://registry-testbed.apnic.net/as0-test-slurm.json`**
- Modified NLNet Labs “Krill” system (added ability to have more than one prefix/ROA)
  - Krill (**`https://github.com/NLnetLabs/krill`**) very easy to work with
  - Modified to combine all IPv6 prefixes to a common /24 in one ROA
- Tested with the RIPE validator, and Routinator
  - Adds 3Mb to the RIPE validator’s export state in .csv
  - ~2500 .roa objects, ~250 for IPv4, the rest for IPv6

Prop132 testbed (2)

- Mirrors standard APNIC RPKI CA structure:

  TA (0/0), (will be offline/HSM backed in production)

  Delegates to intermediate CA (also 0/0),

  Delegates to production CA (APNIC resources only),

  which issues ROAs

- Only one production CA
- Testbed TA not HSM-backed
  - Service deployment will require re-configuration of validator to include HSM-backed TAL

Prop132 testbed (3)

- State based on:
  - extended-delegated stats file (public)
  - changes per-day since publication of stats file (private)
    - …which become visible in next days file (public)
- Regenerated every ten minutes
- Production will work similarly

Prop132 testbed (4): Why not 1 ROA?

- Single ROA was a large object
  - 65,000 IPv4 and IPv6 elements
  - Sparse IPv6 delegation model made many holes.
- Probably the most complex object in the global RPKI data
  - Imposes higher ASN.1 parsing burden
  - Creates many distinct output states, one per prefix
  - Fate sharing: bad ROA? All data invalid
- Code (Krill) designed to issue one ROA per prefix
  - Low cost of initial pilot, small changes to make small aggregates

It’s live

RPKI Validator | Trust Anchors | ROAs | Ignore Filters | Whitelist | BGP Preview | Announcement Preview

Configured Trust Anchors

Trust Anchors	Processed Items	Last Updated (UTC)
AfriNIC RPKI Root	1281 0 0	2020-02-14 05:09:21
APNIC AS0 Root	2379 0 0	2020-02-14 05:05:24
APNIC RPKI Root	13859 0 146	2020-02-14 05:11:22
ARIN	8864 0 3	2020-02-14 05:09:25
LACNIC RPKI Root	7911 10 2	2020-02-14 05:09:24
RIPE NCC RPKI Root	45913 0 0	2020-02-14 05:01:43

It’s live

RPKI Validator Trust Anchors ROAs Ignore Filters Whitelist BGP Preview Announcement Preview

Configured Trust Anchors

Trust Anchors	Processed Items			Last Updated (UTC)
AfriNIC RPKI Root	1281	0	0	2020-02-14 05:09:21
APNIC AS0 Root	2379	0	0	2020-02-14 05:05:24
APNIC RPKI Root	13859	0	146	2020-02-14 05:11:22
ARIN	8864	0	3	2020-02-14 05:09:25
LACNIC RPKI Root	7911	10	2	2020-02-14 05:09:24
RIPE NCC RPKI Root	45913	0	0	2020-02-14 05:01:43

It’s live

```
"ASN","IP Prefix","Max Length","Trust Anchor"
"0","27.100.4.0/22","32","APNIC AS0 Root"
"0","27.124.64.0/20","32","APNIC AS0 Root"
"0","27.126.156.0/22","32","APNIC AS0 Root"
"0","36.50.0.0/16","32","APNIC AS0 Root"
"0","43.227.184.0/22","32","APNIC AS0 Root"
"0","43.228.104.0/22","32","APNIC AS0 Root"
"0","43.228.164.0/22","32","APNIC AS0 Root"
"0","43.228.172.0/22","32","APNIC AS0 Root"
"0","43.229.16.0/22","32","APNIC AS0 Root"
"0","43.231.130.0/24","32","APNIC AS0 Root"
"0","43.241.244.0/22","32","APNIC AS0 Root"
"0","43.248.56.0/22","32","APNIC AS0 Root"
"0","43.250.180.0/22","32","APNIC AS0 Root"
"0","45.65.56.0/23","32","APNIC AS0 Root"
"0","45.115.16.0/22","32","APNIC AS0 Root"
"0","45.117.56.0/22","32","APNIC AS0 Root"
"0","45.117.132.0/22","32","APNIC AS0 Root"
"0","45.119.120.0/22","32","APNIC AS0 Root"
```

Open questions for the community?

- Is the overall plan acceptable?
- Are you comfortable with implementation in stages
  - And the stages as described
- Is the decision to align with delegated statistics acceptable?
- Is the initial deployment to a separate TAL acceptable?
- Should this be a global policy so that all RIRs perform the same actions?
- Is a collection of ROA rather than one ROA acceptable?
  - Does the community prefer one ROA per prefix (65,000 objects)