APNIC Routing Registry and ROAs

SANOG 33

9 Jan, 2019

Overview

- Role APNIC plays in the IRR

- Known limitations in IRR services

- Ideas to address those limitations

APNIC database and the Internet Routing Registry (IRR)

- APNIC Whois Database
    - Two databases in one

- Public network management database
    - Whois information about networks and contacts (IP addresses, ASNs and so forth)

- Routing Registry (RR)
    - Contains routing information (routes, filters, peers and so forth)
    - APNIC RR is part of the global IRR

Routing Registry objects

aut-num

route

rtr-set

as-set

route6

filter-set

route-set

peering-set

route and route6 object

Represents a single IPv4/IPv6 route injected into the Internet routing mesh.

```
route6:          2001:df2:ee01::/48
descr:           Prefix for APNICTRAINING LAB DC
origin:          AS45192
mnt-by:          MAINT-AU-APNICTRAINING
last-modified:   2016-06-23T14:32:38Z
source:          APNIC
```

```
route:           202.125.97.0/24
descr:           Prefix for APNICTRAINING LAB DC
origin:          AS45192
mnt-by:          MAINT-AU-APNICTRAINING
country:         AU
last-modified:   2016-06-16T23:23:17Z
source:          APNIC
```

aut-num object

Contains details of the registered holder of an Autonomous System number and their routing policy for that AS.

```
aut-num:       AS24021
as-name:       APNICRANDNET-TUI-AU
descr:         TUI experiment
country:       AU
import:        from AS1221
action         pref=100;
accept         ANY
import:        from AS109
action         pref=100;
accept         ANY
export:        to AS1221
announce       AS24021
export:        to AS109
announce       AS24021
default:       to AS1221
action         pref=10;
networks       ANY
```

as-set object

A group of Autonomous Systems with the same routing policies.

```
as-set:        AS17821:AS-APNICTRAINING-ISP
descr:         AS-SET for APNIC Training ISP
tech-c:        AT480-AP
admin-c:       AT480-AP
mnt-by:        MAINT-AU-APNICTRAINING
members:       AS131107, AS45192, AS135541, AS135540, AS135533
members:       AS135534, AS135535, AS135536, AS135537, AS135538
last-modified: 2018-12-28T02:41:05Z
source:        APNIC
```

Accuracy of aut-num object registration

- ASNs assigned to member organizations (portable)
  - Members assign portable ASNs to their customers

- ASNs assigned to member's customers (non-portable)
  - Members reassign ASNs to new customers

- Missing aut-num objects
  - Members accidentally delete their aut-num object

aut-num object registration improvements

- APNIC-HM maintainer is now used to protect aut-num object

- MyAPNIC improvements to manage aut-num object

- Visibility of portable and non-portable ASN in MyAPNIC?

Member query

"Network Admin of AS17970 has removed 203.76.192.0/18 and some other prefix at APNIC, but seems their ISP didn't help them to remove that at IRR DBs, such as RADB and NTT

We use a tool called BGPQ3 to resolve AS-SET at RADB as our BGP incoming prefix filters. While we specify the host of APNIC, it shows the below error"

```
$ bgpq3 -h whois.apnic.net -A -l RADIUS -m 24 AS-RADIUS-PH

ERROR:Wrong reply: %ERROR:101: no entries found
```

4th Dec, 2018

IRRd syntax support

- whois.apnic.net does not support IRRd syntax queries

```
bgpq3 -h whois.radb.net -S APNIC -A -l RADIUS -m 24 AS-RADIUS-PH

no ip prefix-list RADIUS
ip prefix-list RADIUS permit 27.126.152.0/22
ip prefix-list RADIUS permit 27.126.152.0/22 ge 24 le 24
ip prefix-list RADIUS permit 43.247.16.0/22 le 24
ip prefix-list RADIUS permit 43.255.216.0/22
```

- Setup rr.apnic.net server to support IRRd syntax queries?

- Separation of delegation and routing registry?

Out of date route objects

```
whois –h whois.radb.net 203.76.192.0/24
```

```
route:          203.76.192.0/24
descr:          Proxy-registered
origin:         AS55821
source:         NTTCOM
```

```
route:          203.76.192.0/24
descr:          Proxy-registered
origin:         AS17970
source:         RADB
```

```
route:          203.76.192.0/24
descr:          REACH (Customer Route)
origin:         AS23944
source:         REACH
```

Out-of-region route objects in RIPE IRR

- Need for operators to have route objects for out-of-region prefixes

- No workable solution for cross-registry authorization

- Routes created using a well-known maintainer with public password

- Authorization by prefix custodians was unverified
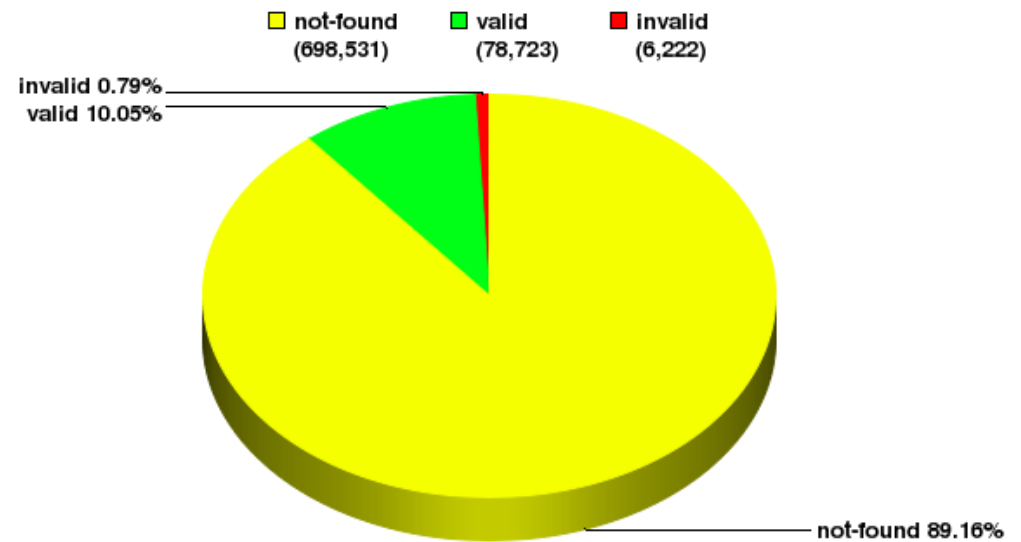
Changing views in the RIPE community

- Increase in out-of-region prefix hijacks with false route objects

- RIPE DB working group declared consensus on stopping this service
  - No new route objects for out-of-region prefixes in RIPE RR
  - "source:" attribute of existing objects modified to RIPE-NONAUTH
  - Policy Proposal 2018-06: ROA to clean up RIPE-NONAUTH

RPKI: ROA

- ROA (Route Origin Authorization) is a digitally signed, cryptographic object which is generated by the Resource Certification service.

- What's contained in a ROA?
  - The AS number you have authorized
  - The prefix that is being originated from it
  - The most specific prefix (maximum length) that the AS may announce

RPKI Status – Global

Valid	10.05%
Invalid	0.79%

783,476 Unique IPv4 Prefix/Origin Pairs

■ not-found (698,531)　■ valid (78,723)　■ invalid (6,222)

invalid 0.79%
valid 10.05%

not-found 89.16%

NIST RPKI Monitor 2018-10-20

APNIC

RPKI Status – APNIC Region

197,006 Unique IPv4 Prefix/Origin Pairs

- not-found (185,121)
- valid (10,039)
- invalid (1,846)

invalid 0.94%
valid 5.10%

not-found 93.97%

NIST RPKI Monitor 2018-10-20

Valid	5.10%
Invalid	0.94%

- Provide tools in MyAPNIC to ensure your ROAs are up to date?

https://rpki-monitor.antd.nist.gov
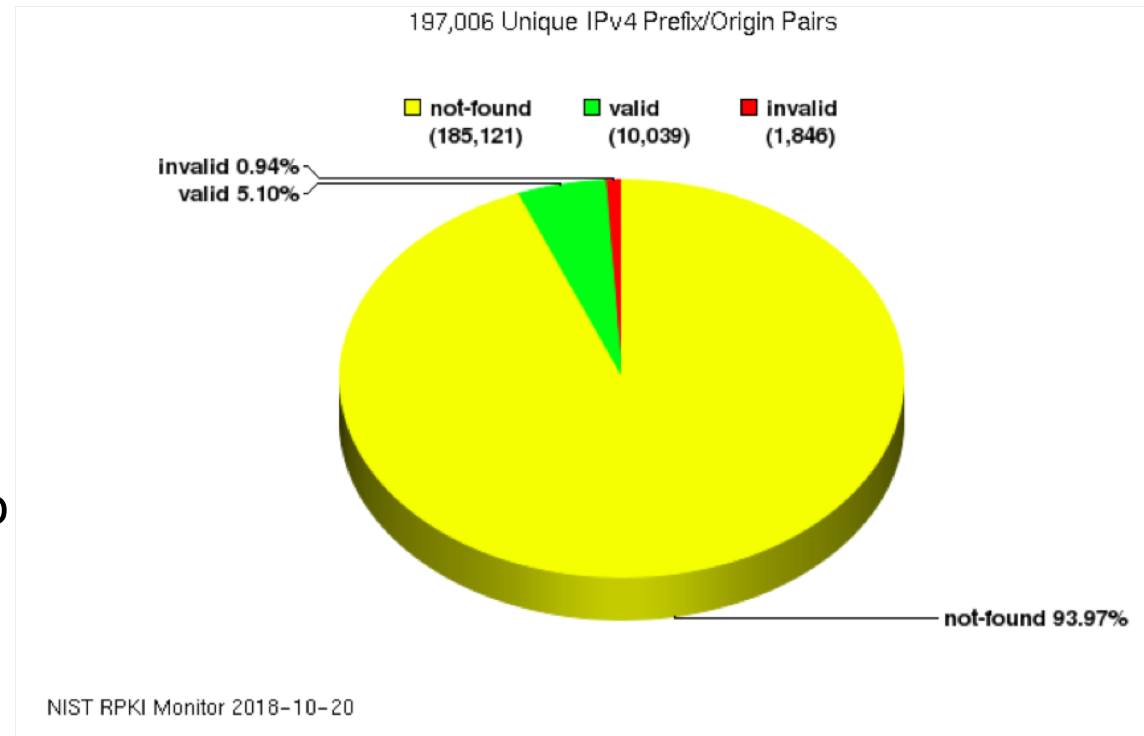
APNIC

Resource Certification

Measure	1/1/2018	Current	Growth
Members with certs	13.0%	14.4%	**1.4%**
Members with ROAs	7.4%	9.0%	**1.6%**
IPv4 under ROAs	3.3%	5.0%	**1.7%**
IPv6 under ROAs	0.9%	5.85%	**4.95%**

apnic.net/rpki

Member query

"Dear helpdesk,

We want to check the routes announced by some small ISPs or customers to make sure that the routes are correct. If we want to do it through RPKI, is there any interface or other way that could be used, so we can get all the RPKI routes from some specific AS."

18th Dec, 2018

RPKI based routes

```
whois -h rr.ntt.net -s RPKI -i origin AS131107
route:        202.125.96.0/24
descr:        RPKI ROA for 202.125.96.0/24
remarks:      This route object represents routing data retrieved from the RPKI
remarks:      maxLength 24
origin:       AS131107
mnt-by:       MAINT-JOB
changed:      job@ntt.net 20190101
source:       RPKI  # Trust Anchor: APNIC RPKI Root
```

- NTT IRRd based service covering our region?

- RPKI validator as a service?

Summary of ideas

- MyAPNIC
  - Visibility of portable and non-portable ASN
  - Tools to ensure your ROA are up to date

- APNIC Routing Registry
  - Setup rr.apnic.net server to support IRRd syntax queries
  - Separation of delegation and routing registry
  - NTT IRRd based service covering our region
  - RPKI validator as a service

Thanks!

vivek@apnic.net