Using ARIN WHOIS data for BGP Prefix Filters

Job Snijders – job@ntt.net

NANOG 72

What is the IRR

- “Internet Routing Registry”
- What NTT, YYCIX, others, use as a source to generate per customer prefix filters
- Publicly available, to help debugging and provide transparency
- By making our source for filter generation publicly available, other parties can inspect what we take into consideration.

A route object: the atom

```
$ whois -h rr.ntt.net 192.147.168.0/24

route:          192.147.168.0/24
descr:          Job Snijders
origin:         AS15562
notify:         job@instituut.net
mnt-by:         MAINT-JOB
changed:        job@ntt.net 20161003
source:         NTTCOM

(only the bold lines are relevant in
the process)
```

Generating a prefix filter

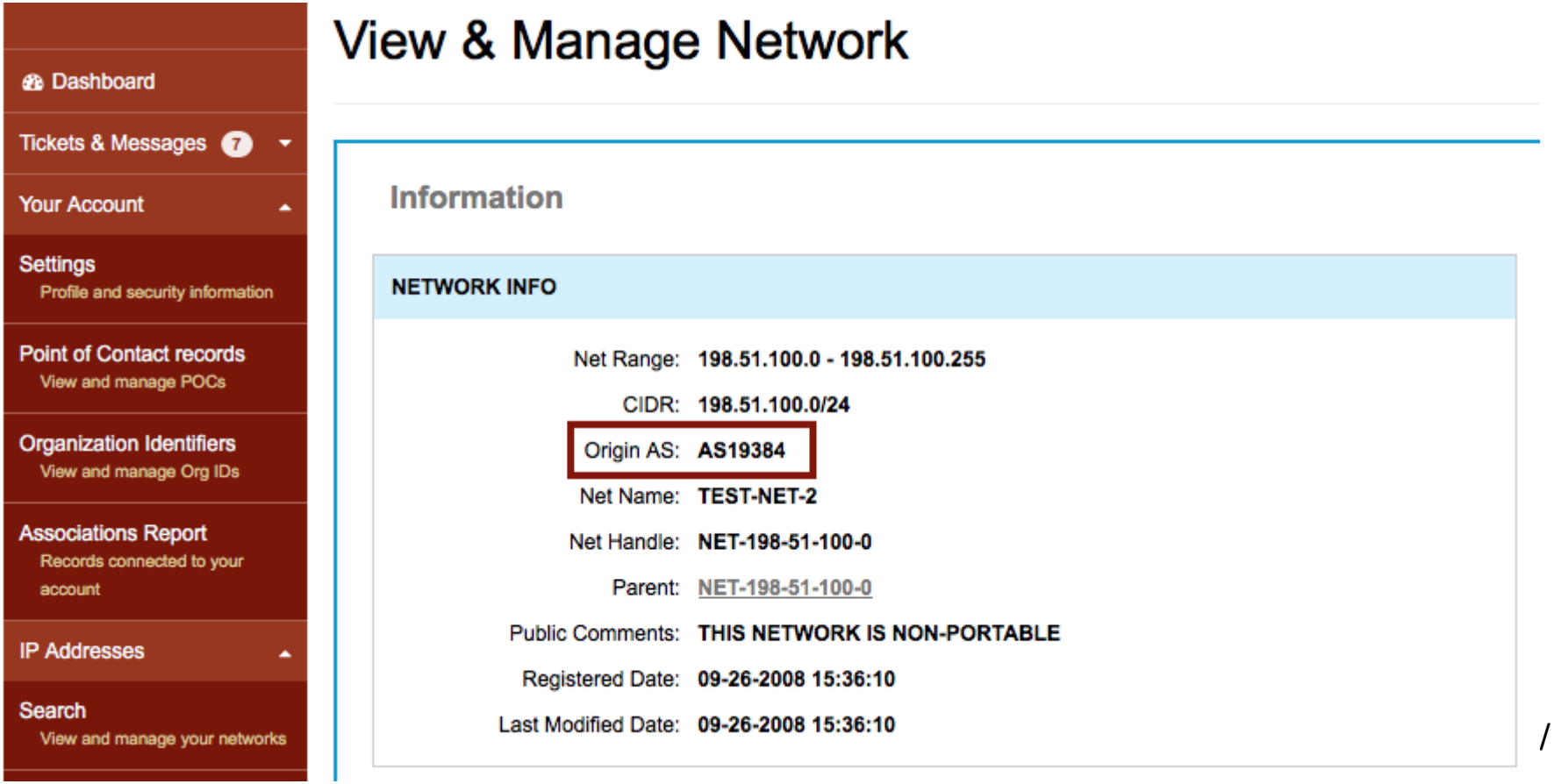
```
job@vurt ~$ whois -h rr.ntt.net '!gAS15562'
A212
165.254.255.132/32 165.254.255.26/32
165.254.255.0/25 165.254.255.144/28
165.254.255.133/32 192.147.168.0/24
165.254.255.160/28 165.254.255.149/32
209.24.0.0/16 204.42.254.192/26
165.254.255.0/24 67.221.245.0/24
C
job@vurt ~$
```

A case study: YYCIX

- Calgary Internet Exchange – 30 peers ~ 80K prefixes at the route server
- YYCIX converted to filtered (secure) Route Servers in October 2017.
- After deploying we noticed that ~ 6500 “invalid” announcements
- Research indicated that ~ 1700 (23%) could be validated against ARIN WHOIS data

What is this ARIN WHOIS thing?

- Remember from the third slide that we **only** care about the CIDR + Origin AS tuple?



Using ARIN WHOIS

- It is a trustworthy authoritative source of data
- We download a 3.5GB XML dump from ARIN once a day
- We convert the XML into “route:” objects
- We load those IRR objects into rr.ntt.net
- This is to offer customers easier choices
  - Setting up IRR can be cumbersome

Example output

```
$ whois -h rr.ntt.net 199.43.0.44
route:        199.43.0.0/24
descr:        NET-199-43-0-0-1
origin:       AS10745
remarks:      This route object represents authoritative
              data retrieved from ARIN's WHOIS service.
remarks:      The original data can be found here:
              https://whois.arin.net/rest/net/NET-199-43-0-
0-1
remarks:      This route object is the result of an
              automated WHOIS-to-IRR conversion process.
mnt-by:       MAINT-JOB
changed:      job@ntt.net 20150715
source:       ARIN-WHOIS
```

http://irrexplorer.nlnog.net

Source code a

Search

Prefix: 199.43.0.43

Matching prefixes

prefix	bgp	level3	arin	rpki	arin-whois	advice
199.43.0.0/24	10745	22773	10745	10745	10745	Multiple route-object exist with different origins

Showing 1 to 1 of 1 entries

How to get the data?

- A JSON dump generated by NLNOG (non-authoritative) http://irrexplorer.nlnog.net/static/dumps/arin-whois-originas.json.bz2
- However, I recommend: Sign the (free) ARIN Bulk Whois agreement and fetch the data from ARIN