RISwhois

A new tool for the Routing Information Service

the routing-wg cut

René Wilhelm

New Projects Group
RIPE NCC
<wilhelm@ripe.net>

What is RISwhois?

- A new interface to data collected by RIS project
  - listens on port 43 (whois), answers in style of RPSL

- "looking glass" over an *entire* set of BGP routing tables
  - 11 route collectors in RIS
  - summarized view, use existing RIS tools to dig deeper
  - for IPv4 *and* IPv6

- allows for better IP to origin ASN mapping
  - as compared to the routing registries

Example RISwhois Object

RIPE NCC's own address space:

```
whois -h riswhois.ripe.net 193.0.0.1
```

```
route:          193.0.0.0/21
origin:         AS3333
descr:          RIPE-NCC-AS RIPE NCC
lastupd-frst:   2003-11-06 12:38Z   194.153.154.17@rrc03
lastupd-last:   2004-01-23 13:48Z   193.10.252.5@rrc07
seen-at:        rrc00,rrc01,rrc02,rrc03,rrc04,rrc05,rrc06,rrc07,rrc08,
source:         RISWHOIS
```

Example RISwhois Object (2)

```
route:          193.0.0.0/21
```
prefix in routing table

```
origin:         AS3333
```
AS Number originating the prefix

```
descr:          RIPE-NCC-AS RIPE NCC
```
description of the AS

```
lastupd-frst: 2003-11-06 12:38Z  194.153.154.17@rrc03
lastupd-last: 2004-01-23 13:48Z  193.10.252.5@rrc07
```
timestamps and source of last updates seen by RIS route collectors

```
seen-at:        rrc00,rrc01,rrc02,rrc03,rrc04,rrc05,rrc06,
rrc07,rrc08,rrc09,rrc10
```
route collectors at which the prefix was seen

```
source:         RISWHOIS
```

What is it good for?

- A quick view in the distributed route collector data
  - how is my address space announced worldwide?

- Assigning origin AS numbers to IP addresses
  - traceroute with AS info, AS level traces
  - up to now, tools consulted routing registry
    - not well maintained, 20% unmatched in TTM study (RIPE46)
  - whois style format allows for easy replacement

- Queries which need a combined set of RIS data
  - find prefixes with multiple origins in entire RIS

IPv4 Example

```
$ whois -h riswhois.ripe.net 212.3.66.1
% This is RIPE NCC's Routing Information Service
% whois gateway to collected BGP Routing Tables
% IPv4 or IPv6 address to origin prefix match
%
% For more information visit http://www.ripe.net/ris/riswhois.html


route:         212.3.64.0/19
origin:        AS8900
descr:         Global One Hungary Internet and extranet provider network
lastupd-frst:  2004-01-20 19:06Z   164.128.32.11@rrc09
lastupd-last:  2004-01-20 19:06Z   164.128.32.11@rrc09
seen-at:       rrc09
source:        RISWHOIS

route:         212.3.66.0/24
origin:        AS10282
descr:         DIALIP-PR GLOBAL ONE
lastupd-frst:  2003-11-20 04:15Z   202.12.28.190@rrc00
lastupd-last:  2004-01-23 10:28Z   64.211.147.146@rrc00
seen-at:       rrc00,rrc01,rrc02,rrc03,rrc04,rrc05,rrc06,rrc07,rrc08,rrc09,rrc10
source:        RISWHOIS
```

The *aggregate* /19 announcement is only seen at *one* of the eleven Route Collectors

IPv4 Example (2)

```
$ whois -a -T route -h whois.ripe.net 212.3.66.1

% This is the RIPE Whois server.
% The objects are in RPSL format.
%
% Rights restricted by copyright.
% See http://www.ripe.net/ripencc/pub-services/db/copyright.html

route:          212.3.64.0/19
descr:          Global One Hungary Internet and extranet provider network
descr:          including our subscribers' networks
descr:          Budapest, Hungary
origin:         AS8900
notify:         peter.patzay@globalone.net
mnt-by:         AS8900-MNT
changed:        peter.patzay@globalone.net 19980915
source:         RIPE


route:          212.3.64.0/19
descr:          Verestar
origin:         AS11908
remarks:        Verestar
notify:         maintainer@verestar.net
mnt-by:         VERE
changed:        support@verestar.com 20010711
source:         RADB
```

**RIPE routing registry has /19 of Global One
RADB routing registry has /19 of Verestar
The /24 is NOT registered**

What it is NOT...

- **RISwhois is *not* a database**
  - directly processes RIB dumps from route collectors
  - no (slow) SQL server to query

- **RISwhois is *not* a registry**
  - results really reflect what was *seen* on the Internet
  - not what was registered some time in the past

- **RISwhois is *not* a real-time looking glass**
  - only 3 RIB dumps from the RRCs per day
  - results can be up to 8 hours old

Conclusion

- RISwhois expands the set of RIS query tools

- Useful for a first look in collected RIS data

- More accurate results mapping IP to origin AS

- First public ip2asn service for IPv6

Questions / Discussion