RISwhois

A new tool for the Routing Information Service

René Wilhelm

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

RISwhois in 7 lines

- A new interface to data collected by RIS project
  - listens on port 43 (whois), answers in style of RPSL
- provides a view over a combined set of BGP tables
  - 11 remote route collectors in RIS
- allows for better IP to origin ASN mapping
  - as compared to the routing registries
- and supports some special RIS queries

This talk ...

- Background of RISwhois
- Examples
- How to use
- Traceroute with AS info from RIS
- Related work

The RIS project - a reminder

- Routing Information Service
  - 11 remote route collectors (RRCs)
    - at different locations (Europe, US, Japan)
    - collecting BGP updates from ~350 peering sessions
  - updates dumped to file, new file every 5 minutes
  - three times a day a full dump of the RIB
  - data transferred to central machine @RIPE NCC
  - inserted in a SQL database
- Tools
  - prefix query, asinuse, RRC looking glass …. *RISwhois*

What is RISwhois?

- A new interface to RIS data
  - "looking glass" over an *entire* set of RRC RIB dumps
  - IPv4 *and* IPv6
  - summarized view, use existing RIS tools to dig deeper
- Fast response
  - *no* connecting to SQL server or remote looking-glasses
- Listens on port 43, *whois*
- Answers are formatted like RPSL route objects

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,r
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

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

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

IPv6 Example

```
$ whois -h riswhois.ripe.net 2001:610:240:0:193:0:0:202

% 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:          2001:610::/32
origin:         AS1103
descr:          SURFNET-NL SURFnet, The Netherlands
lastupd-frst: 2003-11-09 18:11Z  2001:7f8:1::a500:1103:2@rrc03
lastupd-last: 2004-01-22 20:51Z  2001:7f8:1::a500:2914:1@rrc03
seen-at:        rrc01,rrc03,rrc05,rrc10
source:         RISWHOIS

route:          2001:610:240::/42
origin:         AS3333
descr:          RIPE-NCC-AS RIPE NCC
lastupd-frst: 2004-01-16 04:54Z  2001:7f8:b:a:1d1:a5d1:2779:65@rrc10
lastupd-last: 2004-01-22 20:51Z  2001:7f8:1::a500:2914:1@rrc03
seen-at:        rrc01,rrc03,rrc05,rrc10
source:         RISWHOIS
```

RIPE NCC has a /42 allocated by SURFnet Announced at AMS-IX, some peers propagate the prefix and it gets picked up by other RRCs

How to query?

- Default output: any whois client
  - whois -h riswhois.ripe.net *IPaddress*
- Pass options to the server:
  - RIPE whois client (ftp://ftp.ripe.net/tools/ripe-whois-latest.tar.gz)
    - whois -h riswhois.ripe.net <option> *IPaddress*
  - netcat
    - netcat riswhois.ripe.net 43
      <option> *IPaddress*
- Options
  - -m return only most specific match
  - -k persistent connection, don't close but allow multiple queries on one connection. Useful for bulk queries.
  - -F Fast, short output (AS & prefix in one line)

Traceroute with AS

- NANOG traceroute:
  - *setenv RA_SERVER riswhois.ripe.net (csh)*
  - *export RA_SERVER=riswhois.ripe.net (bash)*
  - *traceroute -A 193.0.0.1*
- LFT traceroute
  - replace *whois.ra.net* by *riswhois.ripe.net* in source code
  - recompile
- prtraceroute
  - more complicated, part of IRRtoolset
    - riswhois for ip2asn, routing registry for policy info.
    - Architectural change, RIPE NCC software group to work on it

Limitations

- A (recent) snapshot of the RRC routing tables,
  No sense of history
  - if route not present at time of a RIB dump (session reset) that RRC will be missing in the ***seen-at*** list
- Susceptible to misconfiguration on peer routers
  - default route or other bogus short prefix length present in a RIB dump, can result in false matches
- Existing RIS tools invaluable for more detailed info
  - but they take longer to answer user queries ...

Future work

- Web interface
  - with hyperlinks to RIS database prefix query CGI
  - RISwhois provides first quick view
    - click to find out more details for specific RRCs
      (ASpaths, BGP attributes, updates since time of RIB dump,…)

- Fine tuning of options and query handling
  - true support for looking up prefixes:
    - exact match, more specific, less specific

Related work

- Route views project, University of Oregon
  - like RIS, many BGP peers
  - ip2asn via DNS, zone refresh twice a day
    - Advantage: everything in place for distributed service
    - Disadvantage: not easy to integrate in existing products
- Team Cymru, Rob Thomas et.al.
  - various BGP statistics from a route server
  - only limited number of peers (17), not a wide view
  - ip2asn via whois, but not with RPSL style objects
    - not easy to integrate in existing products

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