Whowas

A resource history service at APNIC

APNIC

What is it?

- A service for accessing the details of an internet resource, or resource range, over a period of time
- A product of APNIC Labs (Byron Ellacott and George Michaelson)

Why is it useful?

- For transfer recipients: see the organizations that have used this range in the past
- During disputes: see the changes that have been made to contact or authorization details
- For law enforcement: find contact details for a specific time period
- For researchers: access historical data for analysis/investigation

Previous approaches

- Whois has supported a limited historical query function for a long time
- Available via the `–list-versions` and `–show-version` command line flags
- Object history only: does not survive deletion
- Deleted objects cannot be viewed

How does it work?

- API is defined as an RDAP extension
  - RDAP (Registration Data Access Protocol) is the successor to the port 43 Whois protocol
- API uses existing RDAP structures where possible
- Draft specification: https://tools.ietf.org/html/draft-ellacott-historical-rdap-00

How does it work?

- RDAP has many advantages over port 43 Whois:
  - Internationalisation
  - Redirects
  - Use existing HTTP-based services (e.g. CDNs)
- These advantages are equally useful for both standard RDAP and the Whowas service

How are queries performed?

- `https://rdap.apnic.net/history/{rdap-query}`
  - E.g. `https://rdap.apnic.net/history/ip/1.2.3.4`
  - Supports `ip`, `domain`, `autnum`, `entity`
  - IRR objects, like `route` and `route6`, are not supported in RDAP and also not supported by this extension

What do the responses look like?

- RDAP returns a single record
- Whowas returns a set of records
  - Each record has an ‘applicability’ date range, indicating when it was present in Whois

```
{
    “rdapConformance”: [ “history_0”, … ],
    “notices”: [ … ],
    “records”: [
        …,
        { “applicableFrom”:  “2010-12-17T01:17:46Z”,
          “applicableUntil”: “2011-03-09T06:01:50Z”,
          “content”: {
            “objectClassName”: “autnum”,
            “handle”: “AS4608”,
            “entities”: [  { “handle”: “NO4-AP”, … },
                           { “handle”: “HM20-AP”, … } ] },
        { “applicableFrom”:  “2011-03-04T06:01:50Z”,
          “content”: {
            “objectClassName”: “autnum”,
            “handle”: “AS4608”,
            “entities”: [  { “handle”: “NO4-AP”, … },
                           { “handle”: “HM20-AP”, … },
                           { “handle”: “IRT-APNIC-AP”, … } ] }
    ],
    …
}
```

How are IP ranges handled?

- Entities, domains, and ASNs are ‘single’ objects, and queries are generally ‘for’ one object
- IP address ranges are a bit different
- Currently, the service returns the history for all address ranges that are more-specific or less-specific than the queried-for range

Is there a front-end?

- `https://www.apnic.net/static/whowas-ui`
  - Displays records using diff-like format
  - Allows for seeing results from parent ranges

APNIC Whowas 1.2.3.4

1.2.3.0 - 1.2.3.255
1.0.0.0 - 1.255.255.255
0.0.0.0 - 255.255.255.255

From Thu 22 Sep 2011 to the present

	network name	Debogon-prefix
	network	1.2.3.0 - 1.2.3.255
	country	AU
	type	ASSIGNED PORTABLE
	description	APNIC Debogon Project APNIC Pty Ltd
+	handle	AR302-AP
+	name	APNIC RESEARCH
+	kind	group
+	address	PO Box 3646 South Brisbane, QLD 4101 Australia
+	voice	+61-7-3858-3188
+	fax	+61-7-3858-3199
+	email	research@apnic.net
+	remarks	++++++++++++++++++ + Address blocks listed with this contact + are withheld from general use and are + only routed briefly for passive testing. + + If you are receiving unwanted traffic + it is almost certainly spoofed source + or hijacked address usage. + + http://en.wikipedia.org/wiki/IP_address_spoofing + http://en.wikipedia.org/wiki/Regional_internet_registry + ++++++++++++++++++

From Wed 10 Aug 2011 to Thu 22 Sep 201

+	network name	Debogon-prefix
	network	1.2.3.0 - 1.2.3.25
+	country	AU
+	type	ASSIGNED PORT
+	description	APNIC Debogon Pr APNIC Pty Ltd
+	handle	IRT-APNICRAND
+	name	IRT-APNICRAND
+	kind	group
+	address	PO Box 2131 Milton, QLD 4064 Australia
+	email	abuse@apnic.net
+	email	abuse@apnic.net
+	handle	GM85-AP
+	name	George Michaelso
+	kind	individual
+	address	PO Box 3646 South Brisbane, Q Australia
+	voice	+61-7-3858-310
+	fax	+61-7-3858-319
+	email	ggm@apnic.net

What improvements are planned?

- Stabilize API
  - Possible changes to support domain name RDAP services
  - Discussion in standards bodies

What improvements are planned?

- Further UI improvements
  - Easier to drill down into changes
  - Mobile-friendly
  - Work in progress is available at https://apnic-net.github.io/rdap-history-ui/

Last slide

- Feedback on API/UI very welcome: please send to or create Github issues as appropriate
- Questions?