A frequent question that faces network administrators or application developers consists in identifying *who is using a specific public IP address*. This information can be utilised for instance to perform user localisation and enable location-based services or user access control. In this context, a main technical challenge is to associate the IP address with its corresponding Autonomous System (AS).

Limitations of the whois Information

A typical method to identify the AS that announces a specific IP address is to use the whois protocol. A whois command is available on main OSes and enables to query the databases of regional registries such as ARIN, RIPE, LACNINC, ... A very interesting article provides tips for using the whois command. Here is a simple example that queries the whois.ripe.net server database in order to find the origin AS of the 148.60.0.0/16.

```
$ whois -h whois.ripe.net 148.60.0.0/16 | grep origin
origin:         AS2200
```

However things get complicated very rapidly since the route object information is not always provided or may be outdated.

Another method is by looking at the actual BGP route table for the origin AS of a prefix. You could do this on your own BGP speaking routers or on a public route server with the “show ip bgp” command (or equivalent), or by using one of the public looking glasses on the web. However, this method is cumbersome, especially if you want to quickly look up something or if you have a large number of addresses that you want to analyze with a script. Team Cymru (known for its bogon prefix list) has made a whois server available which provides the announcing AS number and name for any given IP address. The information in its database is based on 17 BGP feeds and is updated twice per hour. If your operating system has a command-line whois client, simply type “whois -h whois.cymru.com” followed on the same line by the IP address you would like to look up. In addition to simple lookups as described above, the server also supports comments and multiple addresses per query. Both of these features are especially useful if you have a script to analyze a large number of IP addresses from a script. For more information about these features, see the server's web page or type “whois -h whois.cymru.com help”. Update: A similar service was announced by the RIPE RIS project. Their whois server can be queried using “whois -h riswhois.ripe.net”, and returns results in RPSL like format (as used by the RIPE whois database itself). The data is gathered from route collector boxes in various locations. For more information about this service, see this web page.

Using BGP Information

```
simurgh$ whois -h riswhois.ripe.net 217.70.180.132
% 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:        192.0.0.0/3
origin:       AS3303
descr:        SWISSCOM Swisscom (Switzerland) Ltd
lastupd-frst: 2013-11-09 23:48Z  192.65.185.140@rrc04
```

```
lastupd-last: 2013-11-09 23:48Z  192.65.185.243@rrc04
seen-at:      rrc04
num-rispeers: 2
source:       RISWHOIS

route:        217.0.0.0/8
origin:       AS3303
descr:        SWISSCOM Swisscom (Switzerland) Ltd
lastupd-frst: 2013-09-24 09:23Z  217.29.66.120@rrc10
lastupd-last: 2013-11-09 23:48Z  192.65.185.243@rrc04
seen-at:      rrc04,rrc10
num-rispeers: 3
source:       RISWHOIS

route:        217.70.176.0/20
origin:       AS29169
descr:        GANDI-AS Gandi SAS
lastupd-frst: 2013-07-04 02:06Z  198.32.176.24@rrc14
lastupd-last: 2013-11-11 15:53Z  195.69.146.99@rrc03
seen-at:
rrc00,rrc01,rrc03,rrc04,rrc05,rrc06,rrc07,rrc10,rrc11,rrc12,rrc13,rrc14,rrc1
5
num-rispeers: 114
source:       RISWHOIS
```

A Do-It-Yourself BGP Query Service