Who is Using This IP Address?

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 utilized for instance to perform user localization and enable location-based services or user access control. In this context, a main technical challenge is to associate the IP address or prefix with its corresponding Autonomous System (AS).

A typical method to identify the AS that announces a specific IP prefix 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However things get complicated very rapidly since the route object information is not always provided or may be outdated. Trying for example to identify the AS announcing 203.178.141.194 (corresponding to the famous www.kame.net), no answer is obtained since the corresponding route object is not registered by WIDE.

```
$ whois -h whois.apnic.net 203.178.141.194 | grep origin
```

An alternative method for identifying the AS that announces a specific IP prefix consists in studying the BGP routing information. Typically, each BGP speaking router stores in a BGP table the routing announcements received for each prefix together with some protocol attributes such as the AS-PATH. This attribute contains the list of ASes traversed by the BGP announcement, with the first AS being the origin AS for the IP prefix! Therefore, the problem boils down to parsing the BGP routing information, matching the IP address or prefix, and then extracting the origin AS from the AS-PATH attribute. Such process is obviously optimal when the router has a global view of the Internet: this is the case for routers participating in the Default Free Zone (DFZ) where the BGP tables contain *all the prefixes* announced in the Internet. As of 2014, these routers have around 500 000 active BGP entries according to the latest statistics.
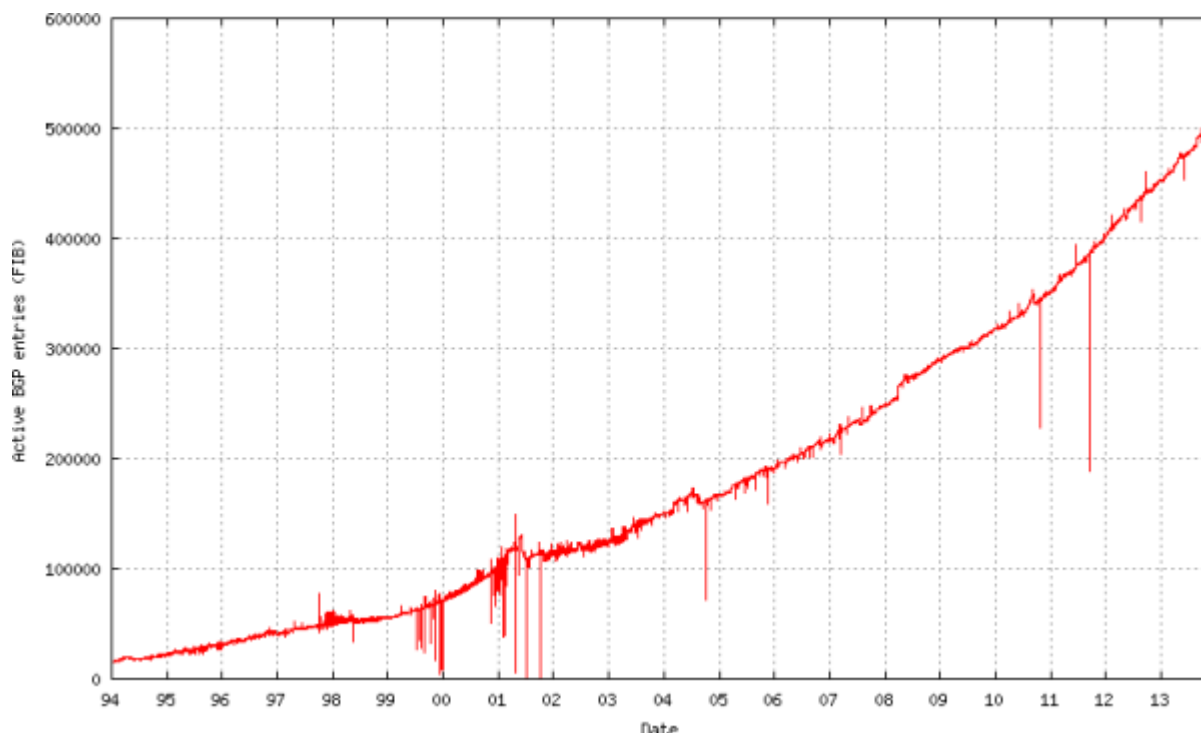
Figure 1. Active BGP entries

However, having access to a DFZ BGP router is not easy in practice. Alternatively, it is possible to find similar routing information on looking glasses or route servers that are made public by network operators (see for example a list of servers on www.routeserver.org). Such devices are originally deployed in order to contribute to the monitoring or the tracking of BGP anomalies in the Internet. Let us try for example to log on the Allstream route server in Canada and identify the origin AS of 148.60.0.0/16. The output of the `show ip bgp` command shows the AS path 15290 3356 1273 2200 in the BGP announcements. Therefore, the first AS, *i.e.*, AS 2200 is the origin AS of the studied prefix.

```
$ telnet route-server.east.bb.allstream.net
route-server.east>show ip bgp 148.60.0.0/16
BGP routing table entry for 148.60.0.0/16, version 270487514
Paths: (4 available, best #4, table default)
  Not advertised to any peer
  15290 3356 1273 2200
    199.212.162.69 from 199.212.162.69 (199.212.162.69)
      Origin IGP, localpref 100, valid, external
      Community: 15290:3356 15290:64995 15290:65050 15290:65506
  15290 3356 1273 2200
    199.212.162.68 from 199.212.162.68 (199.212.162.68)
      Origin IGP, localpref 100, valid, external
      Community: 15290:3356 15290:64995 15290:65050 15290:65506
  15290 3356 1273 2200
    199.212.162.66 from 199.212.162.66 (199.212.162.66)
      Origin IGP, localpref 100, valid, external
      Community: 15290:3356 15290:64995 15290:65050 15290:65506
  15290 3356 1273 2200
    199.212.162.67 from 199.212.162.67 (199.212.162.67)
      Origin IGP, localpref 100, valid, external, best
```

```
          Community: 15290:3356 15290:64995 15290:65050 15290:65506
```

Despite its availability, this method remains 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. Fortunately, RIPE NCC and Team Cymru have already answered these questions: they provide solutions that combine the versatility of the whois protocol with the accuracy of the BGP information. In other words, you keep on using the legacy whois command but you get BGP-based results. Let us examine these solutions:

- Team Cymru implements the `whois.cymru.com` server which provides the announcing AS number and name for any given IP address. The information in its database is based on the BGP feeds from 50+ BGP peers, and is updated at 4 hour intervals. Here is a simple example for using the cymru service:

```
$ whois -h whois.cymru.com 148.60.0.0/16
AS       | IP               | AS Name
2200     | 148.60.0.0       | FR-RENATER Reseau National de
telecommunications pour la Technologie
```

and another example that demonstrates the possibility of sending multiple addresses in the same query:

```
$ whois -h whois.cymru.com 148.60.0.0/16 203.178.141.194
AS       | IP               | AS Name
2200     | 148.60.0.0       | FR-RENATER Reseau National de
telecommunications pour la Technologie
AS       | IP               | AS Name
2500     | 203.178.141.194  | WIDE-BB WIDE Project
```

- 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.

```
$ 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
```

Start by downloading multiple routing tables for routeviews or RIPE RIS servers. Transform these tables into parsable format bu using bgpdump. Use any scripting language to perform a best prefix match and output the origin AS of your desired IP prefix.

From:
http://wiki.lahoud.fr/ - **wikiroute**

Permanent link:
http://wiki.lahoud.fr/doku.php?id=who_is_using_this_ip_address&rev=1391894489

Last update: **2014/02/08 22:21**