



Providing A Subset of Whois Data Via DNS

Shuang Zhu

Xing Li

CERNET Center



Problem Statement

- Network operators frequently need to check the consistency of the Internet routing
 - Wrong IP prefix announcements (e.g. PA holes)
 - Unauthorized IP prefix announcements
- But it is sometimes difficult to tell which AS an IP originates and should originate from.



Problem Statement

- A standardized mechanism to determine the AS origin of an IP address would be useful, particularly as a diagnostic aid for operators.



Current Practices

- To tell which AS an IP address originates from
 - sort of routeviews projects, CIDR report,
 - analysis of routing tables
- To determine which AS an IP address should originate from
 - route registration is a part of the services of IRR



IRR Providers

Global scope IRR providers, typically are:

- RIR
 - APNIC, RIPE,
- Non-RIR
 - RADB, SAVVIS,



The Observations

- There exist some shortcomings of IRR
 - lack of authority
 - less accuracy
 - not kept up to date



The Observations

- RIR IRRs
 - have the authority of route blocks
 - Need membership to register the route, by specifying mnt-routes in inetnum objects
 - however, ISPs are sometimes lazy or reluctant to maintain
 - In APNIC route database, only about 10% allocated IP addresses registered routes there.



The Observations

- Non-RIR IRRs
 - No authority of the route blocks
 - No check, No accuracy guarantee



Non-RIR IRR Examples

- For example, the answer to the following IRR whois query is obviously incorrect, for 211.64.0.0/13 actually originates from CERNET AS4538.

```
% whois -h whois.radb.net. 211.64.0.0
```

```
% whois -h rr.savvis.net. 211.64.0.0
```

```
route:          211.64.0.0/13
descr:          China United Telecom
origin:         AS9800
mnt-by:         MAINT-AS9800
changed:        noc@cnuninet.com 20050112
source:         SAVVIS
```



Are There Alternatives?

- Can we indicate IRR route origin, a subset of whois data, via DNS?
 - RIR's IP Allocation database is authoritative
 - APNIC, ARIN, RIPE,
 - There is also a natural authorization, along with the delegation of reverse DNS of the route block



How To Do Via DNS

- Network operators publish the AS origin of their routing announcements by use of TXT RR in its reverse DNS

`<reverse>.in-addr.arpa. IN TXT "<as number>" "<network number>" "<prefix length>"`

e.g.

`64.211.in-addr.arpa. IN TXT "4538" "211.64.0.0" "13"`

`65.211.in-addr.arpa. IN TXT "4538" "211.64.0.0" "13"`

`66.211.in-addr.arpa. IN TXT "4538" "211.64.0.0" "13"`

`67.211.in-addr.arpa. IN TXT "4538" "211.64.0.0" "13"`

....



Example Details

- 211.64.0.0/13 is the allocation from APNIC for CERNET

```
inetnum:      211.64.0.0 - 211.69.255.255
netname:      CERNET-CN
descr:        China Education and Research Network
descr:        Room 224, Tsinghua University
descr:        Beijing, China
country:      CN
...
mnt-by:       APNIC-HM
mnt-lower:    MAINT-CERNET-AP
changed:      hostmaster@apnic.net 19990917
status:       ALLOCATED PORTABLE
changed:      hm-changed@apnic.net 20041214
source:       APNIC
```



Example Details

- 211.64.0.0/13 is the allocation from APNIC for CERNET

```
inetnum:      211.70.0.0 - 211.71.255.255
netname:      CERNET
descr:        China Education and Research Network
descr:        Room 224, Tsinghua University
descr:        Beijing, China
country:      CN
...
mnt-by:       APNIC-HM
mnt-lower:    MAINT-CERNET-AP
changed:      hostmaster@apnic.net 20000801
status:       ALLOCATED PORTABLE
source:       APNIC
```



Example Details

- APNIC delegates 64-71.211.in-addr.arpa. to CERNET name servers.

```
% dig @ns1.apnic.net. +norecurse 64.211.in-addr.arpa. ns
```

```
:: QUESTION SECTION:
```

```
;64.211.in-addr.arpa.      IN      NS
```

```
:: AUTHORITY SECTION:
```

```
64.211.in-addr.arpa.  172800 IN      NS      dns2.edu.cn.
```

```
64.211.in-addr.arpa.  172800 IN      NS      dns.edu.cn.
```

```
64.211.in-addr.arpa.  172800 IN      NS      ns2.net.edu.cn.
```



Example Details

- CERNET makes 211.64.0.0/13 announcement
- CERNET sets up 64.211.in-addr.arpa. zone data

```
64.211.in-addr.arpa.  IN  SOA  NS2.NET.EDU.CN.  
    HOSTMASTER.NET.EDU.CN. 2006072518 28800 7200 604800 86400  
64.211.in-addr.arpa.  IN  NS   NS2.NET.EDU.CN.  
64.211.in-addr.arpa.  IN  NS   DNS.EDU.CN.  
64.211.in-addr.arpa.  IN  NS   DNS2.EDU.CN.  
64.211.in-addr.arpa.  IN  TXT  "4538" "211.64.0.0" "13"
```



Example Details

- Network operators make the query, with /16, /24 reverse names

```
%dig 64.211.in-addr.arpa. txt
```

```
:: QUESTION SECTION:
```

```
;64.211.in-addr.arpa.      IN      TXT
```

```
:: ANSWER SECTION:
```

```
64.211.in-addr.arpa. 86400 IN      TXT      "4538" "211.64.0.0" "13"
```

```
...
```




Advantages

- Natural authorization along with the delegation of reverse dns of the route block
- The DNS TXT records are maintained locally, and most likely easy to keep up to date
- The DNS is a prevalent distributed service with easy adoption
- No obvious disadvantage.



Conclusion

- We propose an alternative for establishing IP to AS origin mapping via DNS, hopefully overcoming the drawbacks of IRR.
- We think this mechanism of providing a subset of Whois Data via DNS is helpful, and easy to implement.



Thanks for your time!

Comments?