Hunting the Bogon

Geoff Huston

May 2003

Research activity
supported by APNIC

What’s a “BOGON” ?

- A “bogon” is the advertisement in BGP of an address block or an Autonomous System number that is not registered as being allocated
- Example:
  - Advertise an address block drawn from the RFC 1918 private address space: 10.0.1.0/24

What’s “allocated” ?

- There are 3 primary resources that need to be examined to answer this query:
  - IANA registry report
    - Determines what number blocks have been allocated to RIRs and what number blocks are reserved and are not to be used
  - The RIR ‘stats files’ report
    - A summary of number allocations that list the number block and the date of allocation –these files are updated periodically (daily or monthly, depending on the RIR)
  - RIR whois data
    - An online database query tool used to list RIR information relating to the allocation of a particular number

1. IANA Registries

- AS number registry
  - http://www.iana.org/assignments/as-numbers
- IPv4 address registry
  - http://www.iana.org/assignments/ipv4-address-space

There are also other IANA address registries listed at

- http://www.iana.org/ipaddress/ip-addresses.htm

Inconsistencies in IANA Data

- Why are these entries different?

036/8 Jul 00 IANA - Reserved (Formerly Stanford University - Apr 93)

049/8 May 94 Joint Technical Command (Returned to IANA Mar 98)
050/8 May 94 Joint Technical Command (Returned to IANA Mar 98)

  - i.e. are 49/8 and 50/8 held in reserve by IANA or not?

Inconsistencies in IANA Data

- Why are these entries the same?

  197/8 May 93 IANA - Reserved

  240/8 Sep 81 IANA - Reserved

  - It would be useful for the IANA registry to consistently distinguish between IPv4 global unicast address space that is assignable and useable as unicast address space, and those blocks of address space that are currently reserved by the IETF pending a protocol standards action to define their interpretation and use

Inconsistencies in IANA Data

- From RFC3330:

  39.0.0.0/8 Reserved but subject to allocation
  128.0.0.0/16 Reserved but subject to allocation
  191.255.0.0/16 Reserved but subject to allocation
  192.0.0.0/24 Reserved but subject to allocation
  223.255.255.0/24 Reserved but subject to allocation
  240.0.0.0/4 Reserved for Future Use

  - What is the difference between "Reserved", "Reserved for Future Use" and "Reserved but subject to allocation"?

2. RIR Stats Files

- Produced every month (ARIN, LACNIC) or every day (APNIC, RIPE)
  - Contains a summary of the RIR’s allocations for all number blocks that are managed by the RIR

Inconsistencies in RIR Stats Data

- Its incomplete
  - Some additional data can be found in the ERX areas in ARIN
  - The RIRs whois databases appear to contain additional records not found in the stats data - These records describe allocations of address space not listed in the stats files
  - For RIPE the ‘issued’ files contain some additional allocations not listed in the stats file

3. RIR whois Data

- RIPE: ftp://ftp.ripe.net/base/ripe.db.gz
- APNIC: ftp://ftp.apnic.net/apnic/whois/apnic.181.db.gz
- ARIN, LACNIC
  - Whois databases appear to be updated daily
  - Perform the individual queries
    - And be careful about whois query rate throttles

Inconsistencies in RIR Whois Data

- RIPE whois has some strange data:
        - E.g. 2.6.190.56/29 and 5.163.66.80/28
    - It is not obvious (to me) to identify which whois database entries are authoritative
- APNIC, LACNIC and ARIN whois has entries that are not listed in the stats files
    - Are these authoritative entries?
- This is being worked on by the RIRs

+ Historical IANA allocations

- A number of allocations performed by IANA do not appear to be recorded in the RIR data files
  - whois.nic.mil contains additional information
  - BUT some blocks appear to have been assigned to the DDN without any record
    - E.g. AS1451 – AS1533

What’s a Bogon?

IF

- its not listed in the IANA registry as reserved

AND

- If its not listed in collection of RIR stats files and whois allocation data

AND

- Its being advertised as reachable and connected in the global BGP table

THEN

- It could be a bogon advertisement

- Or it could be a data inconsistency in the RIR’s records

A Bogon is NOT…

- The hijacking or otherwise unauthorized use of allocated number resources
  - All the bogon check performs is a lookup for any registry data for each advertised address block and AS using RIR stats and whois data.
  - It does not perform any form of consistency checks relating to the identity of the advertiser of the address space and the identity listed in the registry data

Bogon Listing

- www.cidr-report.org
  - Updated hourly
  - Bogon databases updated daily
  - Includes list of possibly Bogon AS and IP Address advertisements

Bogon Counts (5 May 2003)

- 54 AS numbers cannot be located in the RIR data
- 264 address block advertisements are bogon advertisements

So what?

- The integrity of the Internet depends on uniqueness of addresses.
- Uniqueness depends on the integrity of the records that describe deployment of address space and integrity of the network operators to use address space in accordance with this recorded information

If you find your address space listed in the Bogon Report…

- What should you do?
  1. Check your records to confirm that you have been allocated the number resources that are listed as being a bogon
  2. Check with your RIR about the history of the address record
- Ultimately, there are 2 ways to get off the report:
  1. Stop using the address resources and ensure that you are only using and advertising resources that are validly listed with the RIRs
  2. The RIR updates its database to correct an anomaly and the address space is listed in the updated RIR stats file report

Next Steps:…

- Obviously, it would be good to motivate IANA and the RIRs to resolve inconsistencies in the current databases
- And it would be good to have tools to allow network operators to efficiently identify what may be an invalid routing advertisement