AS112 Intro

William F. Maton Sotomayor
Ottawa Internet Exchange
DNS-OARC Ottawa 2008
What is AS 112?

- Not just another AS number!
- An anycasted DNS instance that deals with reverse map queries for RFC 1918 IP addresses
- Very similar in operation to other anycasted DNS instance, eg. F.root-servers.net
- A volunteer effort
Details

- IANA has delegated reverse maps for the following subnets:
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16
  - 169.254.0.0/16
- The project uses the 192.175.48.0/24 subnet to house the DNS server and uses AS112 as the origin in BGP.
Anycast

• Simply put, a solution to create multiple ‘clones’ of the same destination address located in geographically different places on a network
  – Typically uses a routing protocol (BGP for Internet, OSPF/IS-IS/etc otherwise)
  – Largely limited to UDP

• Some examples are f.root-servers.net and 6to4 relays (RFC3068).
Typical Node Software

• Sites use a server with usually the following software:
  – BGP provided through Zebra/Quagga
  – BIND
  – Perl/bash (for automated scripting)
  – Debian GNU/Linux/FreeBSD/etc

• For query monitoring software, there are various solutions:
  – Bindgraph (CPU intensive)
  – DSC (distributed architecture)
How many are there?

- [http://www.as112.net/](http://www.as112.net/) lists servers that have been either discovered through route-views.oregon-ix.net or via notification by volunteer operators.
  - At least 54 known nodes

- The next presentation may give us some more insight.
Operations Adventures

• Maintaining Drupal-based website for the project has been interesting (strictly Drupal-related)

• Two instances of ISPs making AS112 SOA for a domain

• Weird routing leaks
  – Commercial ISPs hear AS112 nodes from research nets and query/respond via commodity links
Numbers

• Ottawa Internet Exchange here in Ottawa runs an atypical AS112 node:
  – Announced to research networks primarily
  – Announced to OttIX peers
  – No Internet access
  – Gives a possible indication of RFC1918 network DNS misuse in a regional context.

• This node typically sees 1000 queries/s peak, dropping to 600 queries peak on weekends
Queries

- For the Ottawa node queries seem to be divided into three types:
  - SOA
  - PTR
  - Dynamic DNS updates
- Of these SOA and PTR queries dominate
- An incredibly interesting anomaly: A very periodic bunch of A queries from just one K12 org in the US (red) within an extremely short (minutes) period of time
- Top clients: By volume, from Columbia; by subnets, USA.
Query by type

Queries by QType

Query Rate (q/s)

Date

Sep15 Sep16 Sep17 Sep18 Sep19 Sep20 Sep21 Sep22
Queries by subnet
IETF Efforts

• Two drafts submitted to IETF DNSOP working group
  – *Draft-ietf-dnsop-as112-ops* documents AS112 operations for the first time in a standards body context
  – *Draft-ietf-dnsop-as112-under-attack-help-help* tries to educate users or ‘network admins’ who encounter issues with AS112 operations

• Comments on these drafts are appreciated
Future

• Some mechanisms need to be created to deal with new delegations of reverse maps
  – RFC3330 and RFC3330bis
  – IPv6 special use
  – Perhaps a new draft is required
• DNSOP’s `draft-ietf-dnsop-default-local-zones` and vendor adoption and DNS operator deployment will go a long way to alleviate such traffic and concerns.
  – Will get IANA to setup a registry that perhaps AS112 can take advantage of
• Convince more AS112 operators to make stats available
Future Imperfect

• There has been some discussion about the load on root DNS servers regarding junk TLDs (e.g. .local)
  – See http://blog.icann.org/?p=240 for more info
  – Duane Wessel’s 2002/2003 data in http://www.nanog.org/mtg-0310/pdf/wessels.pdf slide "Punchline from Last Year's Talk": Unknown TLD queries at 12.5% of total
  – This isn’t likely to get traction as it enters the ICANN/IANA political spheres
  – But if DNS operators are seeing the hit, maybe then they’ll act?