Lameness in Reverse DNS

Anand Buddhdev
DNS Services Manager, RIPE NCC

History

- Request from DNS working group in 2006 to monitor DNS lameness
- RIPE-400 produced in January 2007
  - Definition of lameness
  - High-level description of the measurement process
- Software development started in the latter half of 2007

Measurement Details

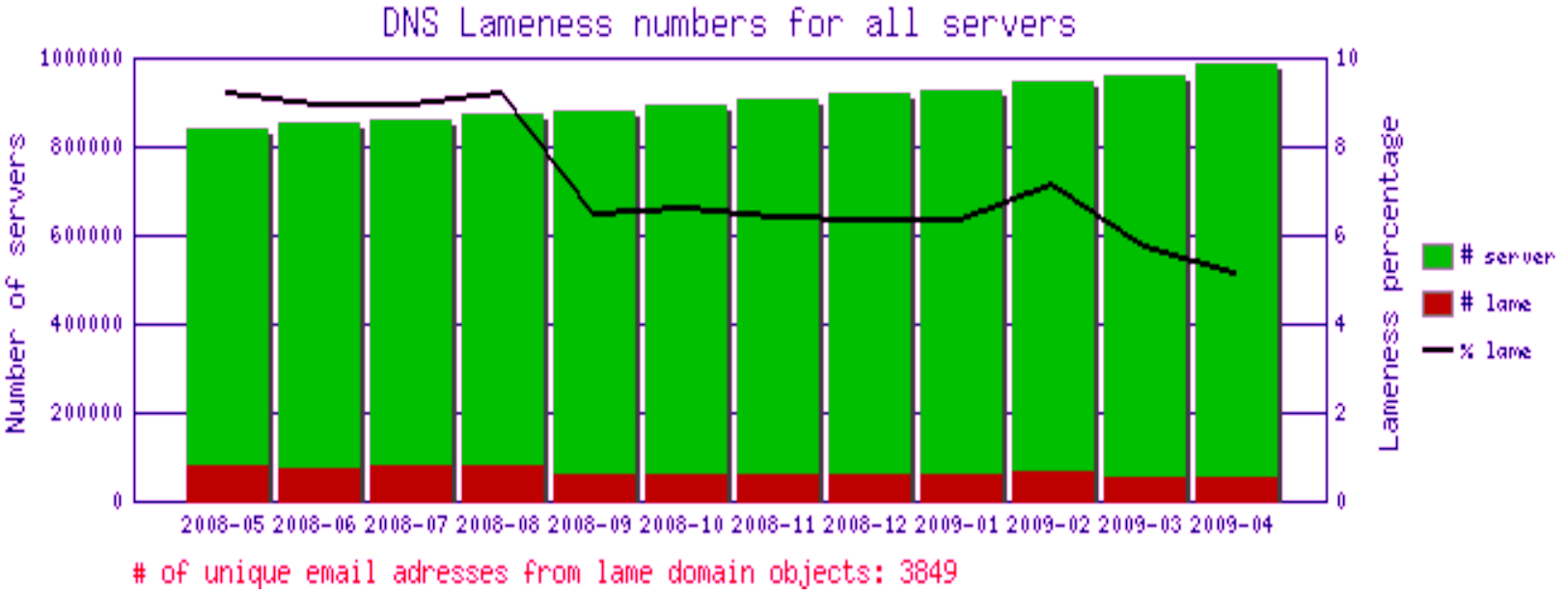
- Measurements from a server at the RIPE NCC
- First, a snapshot of all the delegations is taken
- Every name server of each zone is resolved into A and AAAA records – several attempts are made in case of temporary failures
- Every IP address found is queried for the SOA record of the associated zone – several attempts are made in case of temporary failures
- The query is done over UDP and is non-recursive

Expected Responses

- If there was a response
  - Response from the same address that the query was sent to
  - RCODE is “NOERROR”
  - Response has AA bit set
  - QNAME in the response and query is the same
  - Only one SOA record is returned
- Lack of a response, or non-compliance with any of the above conditions results in the server being marked as lame for the associated zone

Initial Observations

- Just over 6% of all the delegations are lame
- Drop in September 2008 - fixed an IPv6 bug
- Slight peak in February 2009 – measurement problems



Phase 2: Email Alerts

- Our software builds a database of email contacts from 2 sources:
  - The RNAME field of a zone's SOA record
  - The notify and mnt-by attributes in the zone's domain object in the RIPE Database
- At the end of every measurement cycle, we can send an email alert to contacts associated with lame delegations
- Emails are sent with unique envelope senders to help us capture bounces

Phase 2: Email alerts

- Test run in September 2008
- Full-scale alerts from February 2009
- 6695 emails sent in February; 1239 bounced
- 4173 emails sent in March; 937 bounced
- Observable effect – number of lame delegations has gone down to about 5%

Effect of Email Alerts

- As we expected, we got a mixed response
- Several people silently corrected their configurations – lameness went down
- A few people wrote to thank us for the alert
- Some people didn't know why they received the alerts
- A few people were quite annoyed

Known issues

- Measurement:
  - No record of date and time of probes – end-user doesn't know when we queried a particular server
  - A fixed timeout of 3 seconds for all SOA record queries – should probably be increased when a query times out
  - Measurements done from a single server at the RIPE NCC – no second opinion
  - More detailed documentation about how our probes and interpretation of results

Known issues

- Email alerts
  - Email address lookup method isn't optimal – we should look up admin-c, tech-c and zone-c in domain objects
  - No opt-out facility
  - Alert frequency too high – once every 3 months is probably better than every month
- Diagnostics
  - Users cannot request our system for a check after correcting their configuration

Future Plans

- Useful service, despite teething problems
- Incorporate various ideas and suggestions for measurement and alerts
- Improve documentation with even more details and examples
- Hand over ticket handling to our customer services team

Questions?