ENUMbers

Climbing (parts of) E164.ARPA

Peter Koch
DENIC eG
pk@denic.de

RIPE ENUM Working Group
Amsterdam
2005-10-13

Tour Outline

- History
- Method
- Preliminary Results
- Future Work

Earlier Tours

- RIPE Hostcount has been in place since early 1990s
- Counts number of Hosts in the RIPE region
- . . . and, more importantly, growth of that figure
- Recursively walks through ccTLDs in the RIPE region
- ENUM data and coverage is interesting!

Stumbling during earlier excursions

- Hostcount based on AXFR
  - Full transfer of TLD and child, grandchild, . . . zones
  - `AXFR` not alway available
  - Alternative counting technique needed
  - Exhaustive Search is too time/resource consuming
- Security by obscurity: Hide IPv6 nodes in the large address space
  - IPv6 networks sparsely populated ($n : 2^{64}$)
  - . . . you still cannot hide
  - `IP6.ARPA` is well structured, similar to `E164.ARPA`

Deviation: Empty Non-Terminals

- Nodes in the DNS tree own RRs (RRSets)
- Leaves: A, AAAA, MX, NAPTR,
- Inner nodes: NS, SOA, MX,
- Special case: *Empty Non Terminals* (ENT)
- Not every Domain is delegated (Domain != Zone)
- Example:
  - `9.4.E164.ARPA` delegated ex `E164.ARPA`
  - ==> `4.E164.ARPA` empty but existent (ENT)

This gives the perfect Route

- Start at `9.4.E164.ARPA`
- Check all potential child nodes for existence
- Only `0` through `9` are candidates due to name space structure
- Recursively follow existing child nodes
- Non existing nodes (`NXDOMAIN`) help prune the tree
- Depth First or Breadth First Search in the DNS tree

Take Care when Climbing!

- Wildcards
  - Camouflage ENTs
  - . . . but are not perfect in hinding
- Lame Delegations
- Bugs
  - BIND 9 < 9.3 incorrectly handles ENTs
  - `NXDOMAIN` instead of `NOERROR`/`NODATA`

Nice Views

- Search tree pruned at 13th level
- below 9.4.E164.ARPA (3600 delegations)
- approx. 26400 NAPTR-RRs
- with approx. 13600 owners
- up to 13 NAPTR
- 50 DNS Wildcards
- <100 `SERVFAIL` Responses
- Walked through zones with `AXFR` restrictions

NAPTR in a Looking Glass

- 20 E2U+ Services:
  - tel, sip, http, mailto, msg:mailto
  - iax2, voice:sip, msg, iax, fax, h323
  - email, ftp, voice:tel, h323:voice
  - email:mailto, vpim:ldap, mailto:msg
  - web:http, service:sip, ifax:mailto
- Legacy +E2U-Services (RFC 2916):
  - sip+E2U, IAX2+E2U
  - tel+E2U, mailto+E2U,

Distant View

- Current prototype implementation is a resource hog
- Better caching necessary
- Could take advantage of intelligently examining negative responses
- Regular surveys might be able to document growth
- Further postprocessing of collected (NAPTR) data
- RFC 3761 vs RFC 2916
- Syntax Checks
- Surveying NAPTR *Culture*
- Counter measures?