ENUM-Count

Eine Klettertour durch 9.4.e164.arpa

Peter Koch <koch@denic.de>

Frankfurt/Main, 28. September 2005

Wanderkarte

- Historie
- Methode
- Erste Ergebnisse
- Künftige Pläne

Frühere Exkursionen

- Seit etwa 1992 existiert der RIPE-Hostcount
  - Ermittelt die Anzahl der „Hosts“ im europäischen Internet
  - … und insbesondere das Wachstum dieser Größe
  - Rekursiver Durchlauf durch die ccTLDs
- ENUM-Daten sind ebenfalls interessant (und wir sind neugierig!)

Stolpersteine früherer Exkursionen

- Hostcount nutzt AXFR
  - Vollständiger Zonentransfer (DE und Kinder, Enkel, ...)
  - Nicht immer zugänglich
  - Es bedarf einer Alternative
  - Vollständige Suche ist erheblich zu aufwendig

- Überlegungen zum „Verstecken“ von Adressen im IPv6-Adreßraum
  - Anzahl der Hosts pro Netz sehr gering (n:2^64)
  - ... funktioniert trotzdem nicht,
  - Denn `IP6.ARPA` ist strukturiert, vergleichbar `E164.ARPA`

Kleiner Umweg: „Empty Non-Terminals“

- Knoten im DNS-Baum enthalten RRs (RRSets)
  - Blätter: A, AAAA, MX, NAPTR, ...
  - Innere Knoten: NS, SOA, MX, ...
- Sonderfall leerer innerer Knoten (ENT)
  - Nicht jede Domain ist delegiert (Domain != Zone)
  - Beispiel:
    - 9.4.e164.arpa wird aus der Zone e164.arpa delegiert
    - ==> 4.e164.arpa ist leer, aber existent

Wie erkennt man „Empty Non-Terminals“?

```
; <<>> DiG 9.2.2 <<>> 4.e164.arpa. naptr
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35432
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;4.e164.arpa.    IN   NAPTR

;; AUTHORITY SECTION:
e164.arpa.   900  IN   SOA    (ns-pri.ripe.net. e164-contacts.ripe.net.
                  2005062454 14400 3600 2419200 14400 )

;; Query time: 13 msec
;; SERVER: 192.168.32.27#53(192.168.32.27)
```

Damit ist die Route vorgegeben

- Start bei 9.4.e164.arpa
- Alle potentiellen Kindknoten auf Existenz prüfen
  - Wegen der Struktur nur „0“ … „9“
- Existierende Knoten rekursiv weiterverfolgen
- Nicht existierende Knoten (NXDOMAIN) verkürzen den Weg
- Tiefen- oder Breitensuche im DNS-Baum

Vorsicht beim Klettern!

- Wildcards
  - Täuschen die ENT-Entdeckung
  - … taugen dennoch nicht zur Tarnung
- Lame Delegations
- Software-Bugs
  - BIND 9 < 9.3 behandelt ENTs falsch
  - `NXDOMAIN` statt `NOERROR/NODATA`

Schöne Aus- und Ansichten

Erste Ergebnisse mit einer *Proof-of-Concept*-Implementierung

- Tiefe der Suche begrenzt (13 Ziffern)
- Unter 9.4.e164.arpa
  - Ca. 26400 NAPTR-RRs
  - Bei ca. 13600 Ownern
    - Bis zu 13 NAPTR
  - 50 DNS-Wildcards
  - <100 SERVFAIL-Responses
- Auch AXFR-begrenzte Zonen durchsucht

NAPTR aus der Nähe betrachtet

- 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
- Aber auch +E2U-Services (RFC 2916)
  - sip+E2U, IAX2+E2U
  - tel+E2U, mailto+E2U, ...

Fernblick

- Die aktuelle Implementierung ist ein Ressourcenfresser
  - Besseres Caching notwendig
  - Intelligentere Auswertung der (negativen) Antworten
- Regelmäßige Untersuchungen können Wachstum verfolgen
- Stärkere Verwertung der gesammelten Daten
  - RFC 3761 vs RFC 2916
  - Syntax-Checks
  - Erfassung der „NAPTR-Kultur“
- Gegenmaßnahmen?