DNS as a carrier of ENUM and other VoIP routing information

Bert Hubert
(with some help from SpeakUP BV, all mistakes are ours)

Scope

- Role of DNS on the non-VoIP internet
  - some terminology
- Very short introduction of PowerDNS
- Good points of DNS
- Bad points of DNS
- ENUM as a carrier of call routing information
- Mismatches between “the VoIP world” and DNS

Some words on DNS

- DNS has been called 'the phonebook of the internet'
  - Ironically, might soon be the phonebook of the phonebooks!
- DNS is a **distributed, global directory** of information
- Involved in almost every activity on the internet
  - browsing, email, chat
- Finds IP addresses for websites, mailservers mostly

DNS history

- Standardised since **1983**
  - RFC 882 – very recogniseable
  - Paul Mockapetris, sits on the board of sponsor Nominum
- Before there was DNS, people used 'HOSTS.TXT'
  - text file with all important hosts on the net
  - centrally managed
- Lots of problems distributing and maintaining HOSTS.TXT
  - .. should ring a bell

DNS is everywhere

- DNS underlies almost anything done on the internet
- Through 'delegations', the load is spread out over hundreds of thousands of servers
- At the center ('the root'), around 200 servers with 13 IP addresses form the core of DNS
- Busy servers process tens of thousands of DNS queries/second

DNS: Publishing and Finding data

- As a distributed directory, DNS servers can either:
  - publish information;
  - go find information on your behalf;
  - do both at same time
- “Authoritative” / “Resolver” / “Mixed”
- Distributed nature has no analogue in SQL, although LDAP does something like this

Very short introduction of PowerDNS

- PowerDNS launched in 2000
- Open Source (GPL) since 2002
  - “FREE”
- Database & Zone powered Authoritative Server
- Since 2003, Innovative Recursor (“Resolver”), as a separate product
- Powers around 40-50% of domains in western Europe, less worldwide
- Resolving DNS for 40 million internet users, growing rapidly

Unique points

- Authoritative: “Natively database driven”
  - MySQL, PostgreSQL, Sybase, Microsoft SQLServer, DB2, Oracle, SQLite, OpenDBX
  - LDAP
  - BIND-style zone files
  - Scriptable through the 'PIPE' backend
  - Geographical load balancing
- Resolver:
  - best mix of security, features and performance

DNS as 'distributed cached query service'

- While intended to do more, most DNS lookups find IP addresses (for WWW or email)
- However, DNS is also used to find information about IP addresses
- Lots of SPAM information queries over DNS
  - So called “RBLs”
- DNS can store arbitrary data
  - Not only find IP address for a hostname, but 'reverse' as well

Good points of DNS

- Stunning performance
- Very resilient towards denial of service attacks
- Highly distributed
  - problems are often localised as well – any mistakes affect mostly the one who made the mistake.. mostly
- Can cope with major misconfiguration and still function
- Low latency, automatic caching

Bad points of DNS

- Because 'Connectionless', miscreants can spoof fake questions and overload servers – easy to fake 100000 questions/second
- Distributed nature combined with high-resilience means misconfigurations can go undetected for ages
  - or cause failures for 'some' users
- Distributed means.. **no local copy**
- In extreme situation, third party mistakes can lock up your entire company

Bad points of DNS 2

- As it stands, the protocol has no widely implemented security features (but do listen to next presentation!)
- Most implementations are not as secure against “spoofing” as they could be
- DNS mostly carries small queries and small answers
  - Can also do larger answers, but loses much of its appeal then
- Hard to evolve

How words map

- SS7/ISUP -> SIP, H.323, MSN Messenger, Google
- E1, TDM, timeslots -> RTSP
- G.711 -> G.711 :-)
- Phone numbers -> Domain Names
- Point Codes -> “BGP”
- Call routing/TCAP -> ENUM?
- If you like ASN.1, you'll love DNS packets

How Phone Numbers map onto DNS

- For domain names, the end of the name is more important than the beginning
  - **www.isoc.nl ends on** nl
- Phone numbers are the other way around
  - +31-70-3140385 **starts** with +31 for Netherlands, 70 for the hague
- Age old trick, reverse phone number
  - “5.8.3.0.4.1.3.0.7.1.3.e164.arpa”
- But what do we store there?

How to connect to a phone number over IP?

- This is the very big question. Transmitting voice of the internet is well established.
- But how do we find the best way to a phone number over the internet?
  - Which protocol? Which server do we connect to? Which endpoint do we request on that server?
- IP people naturally assume the DNS will be a good fit
- So, is it?

What do we need?

- Some ranges are fixed: all numbers starting with +31-15-278 need to go to Delft University (fictional data)
  - 8.7.2.5.1.1.3.e164.arpa IN NS ns1.tudelft.nl.
  - 4.3.2.1 IN NAPTR 100 10 "u" "sip+E2U" "!^.*$!sip:bert@sip.tudelft.nl!"
- This means: +31-15-2781234 can be reached via SIP, contact user 'bert' on 'sip.tudelft.nl'.
- For sip.tudelft.nl we need an IP address, which we find.. using DNS again!

Number portability?

- On the Dutch PSTN, there is a master list of prefixes, maintained by the OPTA
- For number portability, where individual phone numbers go to another carrier, there is the 'COIN' list
- Carriers can get a copy of this list, needs to be synchronised
- Can DNS deal with this, while remaining distributed?
  - Ideally, original owner would only list 'migrated to provider X'

Number portability 2

- “ENUM is not intended to serve this function, as there are very significant **technical**, regulatory, security, and operational limitations in using ENUM for this purpose. ENUM is a shared resource discovery service, not an industry provisioning service.”
- DNS is a hierachical, it assumes x.company.com will know everything about ***.x.company.com**.
- Limited facilities for 'redelegating' blah.x.company.com to company2.com
  - Especially for ranges

Public/private ENUM

- Public ENUM is provided on E164.ARPA
  - anybody can query
  - some countries already delegated
- However, DNS can also be used privately as a very fast query service
  - everybody CAN have their own local table
  - some benefits of ENUM remain, some drawbacks go away
  - “Carrier/Infrastructure ENUM”

So.. is DNS a good match?

- DNS has some very good points in its favour
- However, DNS is DNS, and was built on different principles
- The problem space is not that difficult however