Internet Engineering

241-461

Robert Elz

kre@munnari.OZ.AU
kre@coe.psu.ac.th

http://fivedots.coe.psu.ac.th/~kre

DNS Limits

- Max Label - 63 bytes
  - Fixed in Protocol
- Max Domain Name - 255 bytes
  - Protocol convention (could be altered)
- Max UDP Packet size - 512 bytes
  - Protocol Convention
    - Avoid Fragmentation
    - Guarantee Buffer Space
- Only one RR in Question Section
  - Convention - enforced by protocol limitations

Exceeding DNS Limits

- Label length
  - Cannot be done - protocol error to try
- Domain Name Length
  - Implementation defined - typically reject name
- UDP Packet Size
  - Can only be exceeded in Reply
  - DNS Query max size:
    - One Question
      - Max Length 255 + 2 + 2
    - Plus Header (12)
      - Total 271
  - TC bit in reply indicates Truncation
    - Repeat query using TCP

Contents

Zone Transfer

- Used by Secondary Server
  - to update its copy of zone file
- SOA Resource Record drives zone transfers

```
psu.ac.th.  12H IN SOA   (
        ns.psu.ac.th. netadmin.ratree.psu.ac.th.
        2001080801      ; serial
        10800           ; refresh -  3 hours
        1200            ; retry   - 20 minutes
        1209600         ; expiry  -  2 weeks
        43200 )         ; minimum - 12 hours
```

- Serial number
  - defines whether zone is up to date

Zone Transfer (2)

- Secondary uses SOA.serial
  - compare with primary
- If older (smaller)
  - do AXFR query
  - fetch updated copy of zone
- Serial numbers cycle
  - 0, 1, 2, ..., 2^32-1, 0, 1, 2, ...
- Zones generally larger than 512 bytes
  - so AXFR uses TCP
- SOA parameters guide secondary
  - refresh - how often to poll primary
  - retry - how often to retry if refresh fails
  - expiry - how long to serve zone data
    - if unable to refresh

Contents

Mapping Addresses to Names

- DNS Inverse Query (Opcode == 1)
  - Client gives the answer
  - Server fills in the Question
- Which server???
  - The server that knows the answer...
  - But must ask the question to find that server
    - or potentially ask every server
- Not a rational approach!

Mapping Addresses to Names (2)

- Treat address as a key in the database
- Do a normal Lookup
  - (for an RR type that contains a domain name as data)
- For IPv4
  - Address 1.2.3.4
  - Lookup 4.3.2.1.IN-ADDR.ARPA
  - Look for PTR type
- PTR is simply a DNS type
    - that contains a pointer to another place in the DNS tree
  - ie: contains a domain name
- For IPv6
  - Similar, but with much longer names
  - IP6.INT or IP6.ARPA