1. DNS (rough)

03 February 2025 11:57

DNS Services

- hostname to IP
- canonical and alias names
  - www.abc.example.com
  - www.example.com
- mail server aliasing: www.mail.example.com → bob@example.com
- load distribution
  - many IPs → 1 name

DNS Hierarchy

Root: managed by ICANN (Internet Cooperation for Assigned Names & Numbers)
DNSSEC → security

↓

Top level Domain: .com, .net, .org, .edu; .cn, .uk, in etc.

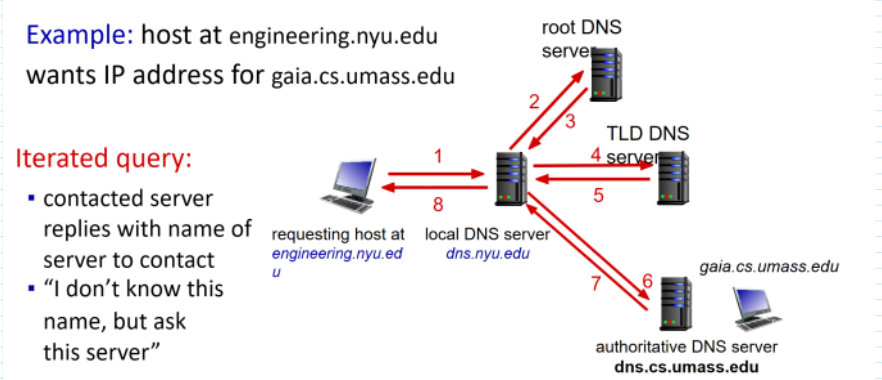
↓

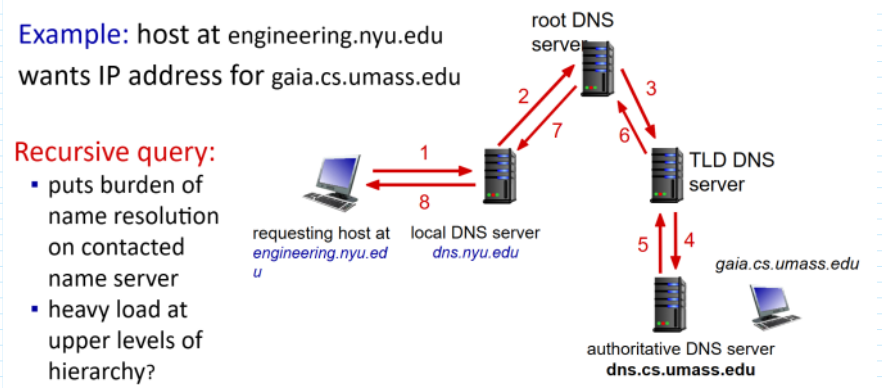
Authoritative: Organisations / service providers: provides authoritative hostname

Local/Name Servers:

- Every ISP has one
- Acts as proxy, forwards request to hierarchy if name-address not available in local cache
- Once a mapping is learned → cached with TTL

Disadvantage: May be out of date
If host changes IP, will not be known until TTL expires





DNS Records

DNS → distributed database containing resource records (RRs)

type = A

name: hostname

value: IP address

some.example.foo.com, 123.45.67.890, A

type = NS

name: domain (foo.com)

value: hostname of authoritative name server for domain

foo.com, dns.foo.com, NS

type = CNAME

name: some alias for canonical name

www.ibm.com → servereast.backup2.ibm.com

value: canonical name

ibm.com, servereast.backup2.ibm.com, CNAME

type = MX

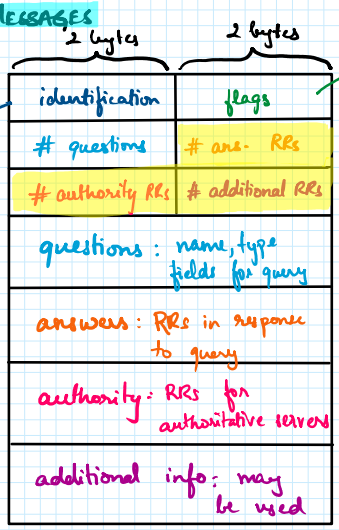
name: alias hostname

value: canonical name of mail server associated with alias hostname

example.com, mail.example.com, MX

RR format: (name, value, type, ttl)

DNS Protocol Messages



16 bit no. for query

☐ T: 0 in query messages

12 bytes

authoritative reply

query/reply

recursion desired (query) / available (reply)

truncation (TC): if it exceeds 512 bytes

opcode: 4 bit, determines type of query (CNAME, A, NS, MX)

Note: Both DNS query and reply messages have the same format