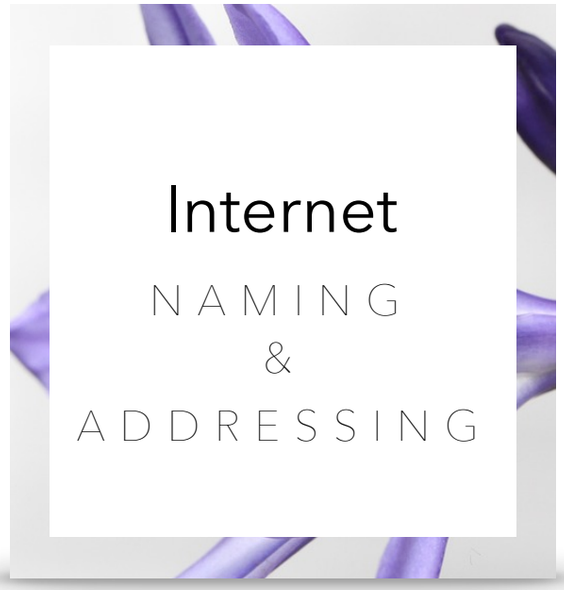


50.005 CSE

Natalie Agus
Information Systems Technology and Design
SUTD

https://websitename.com

↓

THE DOMAIN NAME SYSTEM (DNS)

Application layer protocol,
Distributed database

↓

32-bit IP address

After IP address is obtained, then end hosts can communicate with one another

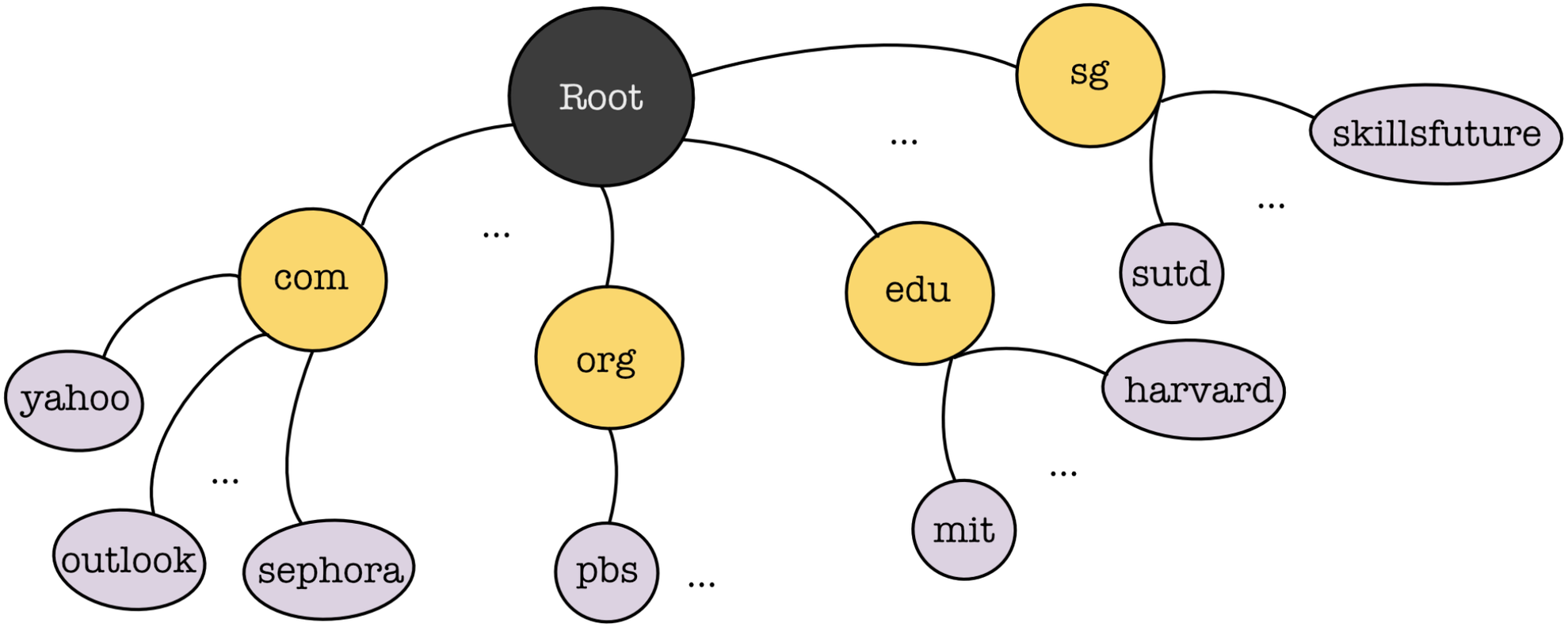
DNS SERVICES

1 **Hostname to IP translation**

2 **Host aliasing**

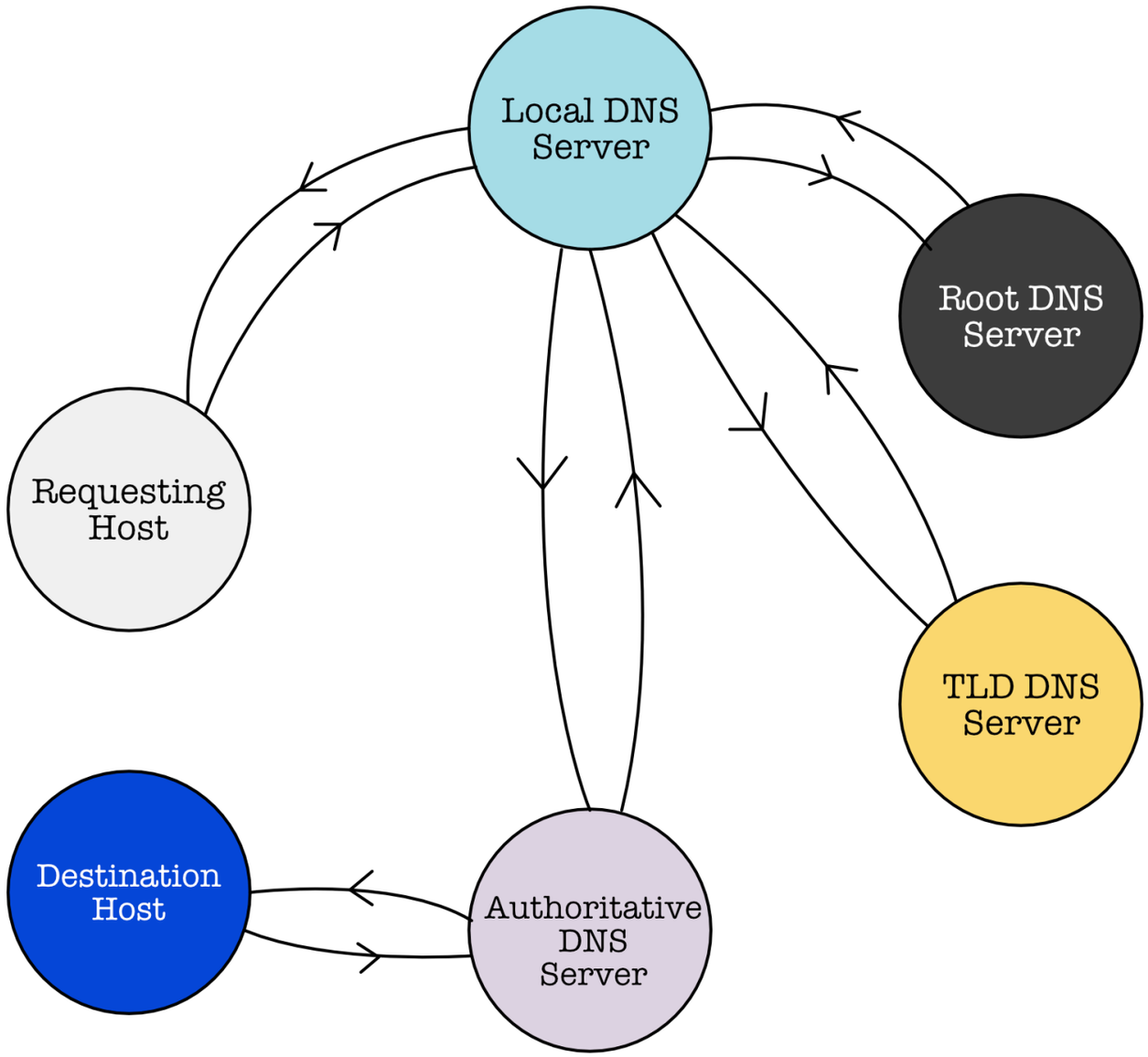
3 **Mail server aliasing**

4 **Load distribution**

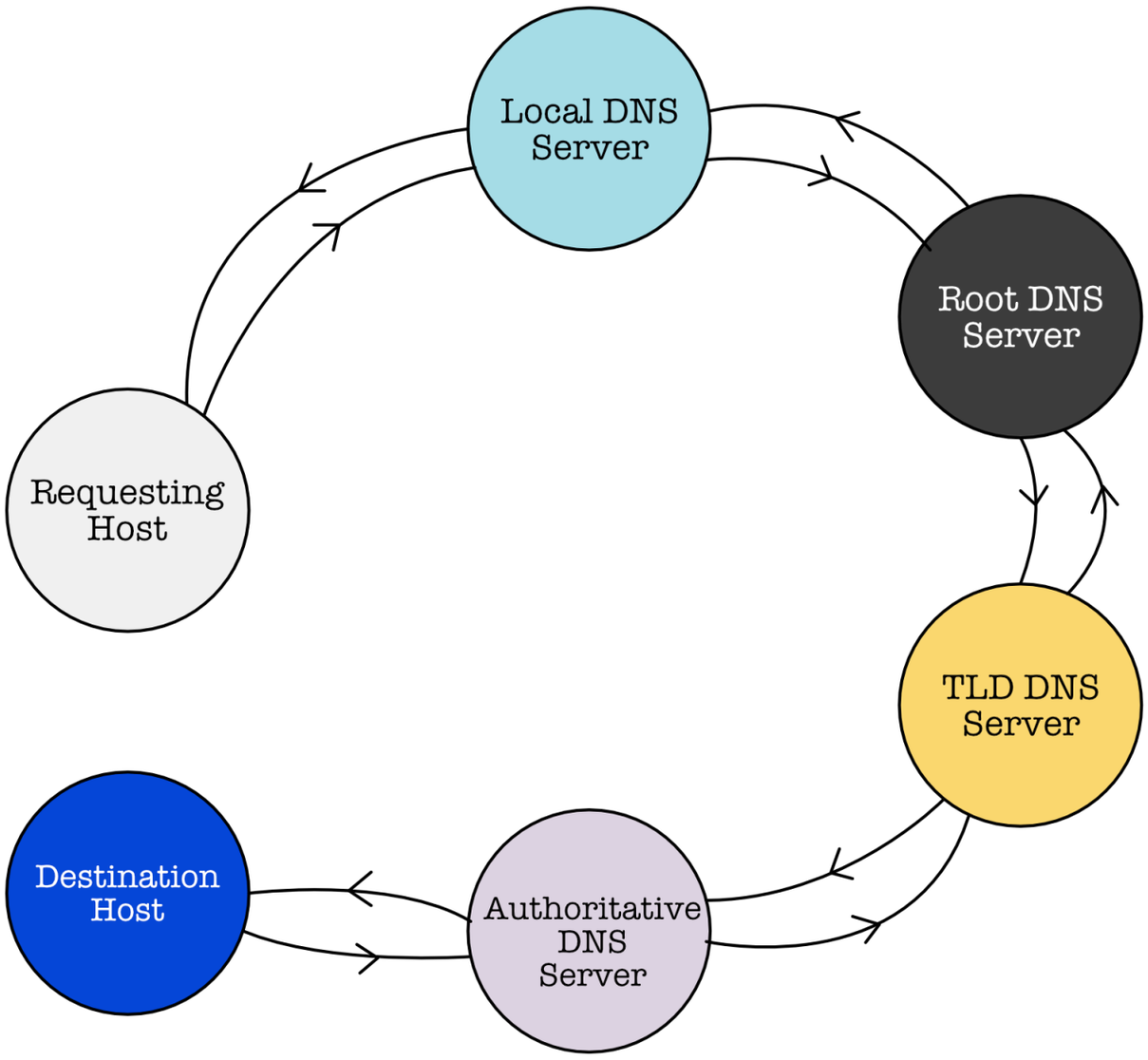


DISTRIBUTED, HIERARCHICAL DNS DATABASE

DNS NAME RESOLUTION
1. ITERATIVE QUERY



DNS NAME RESOLUTION
2. RECURSIVE QUERY



DNS CACHING

Once local name servers learns hostname-ip mapping, it **caches** the mapping

- TLD servers are typically cached in DNS local name servers, **hence faster resolution**
- Cached entries may be **out of date**
- **DNS authoritative name server (the one that hosted the website) decides the DNS record TTL**
- DNS local name server re-queries when TTL expires

DNS RECORDS

The "data structure" of a DNS resource record (RR). RR is used by clients who query hostname-IP resolution

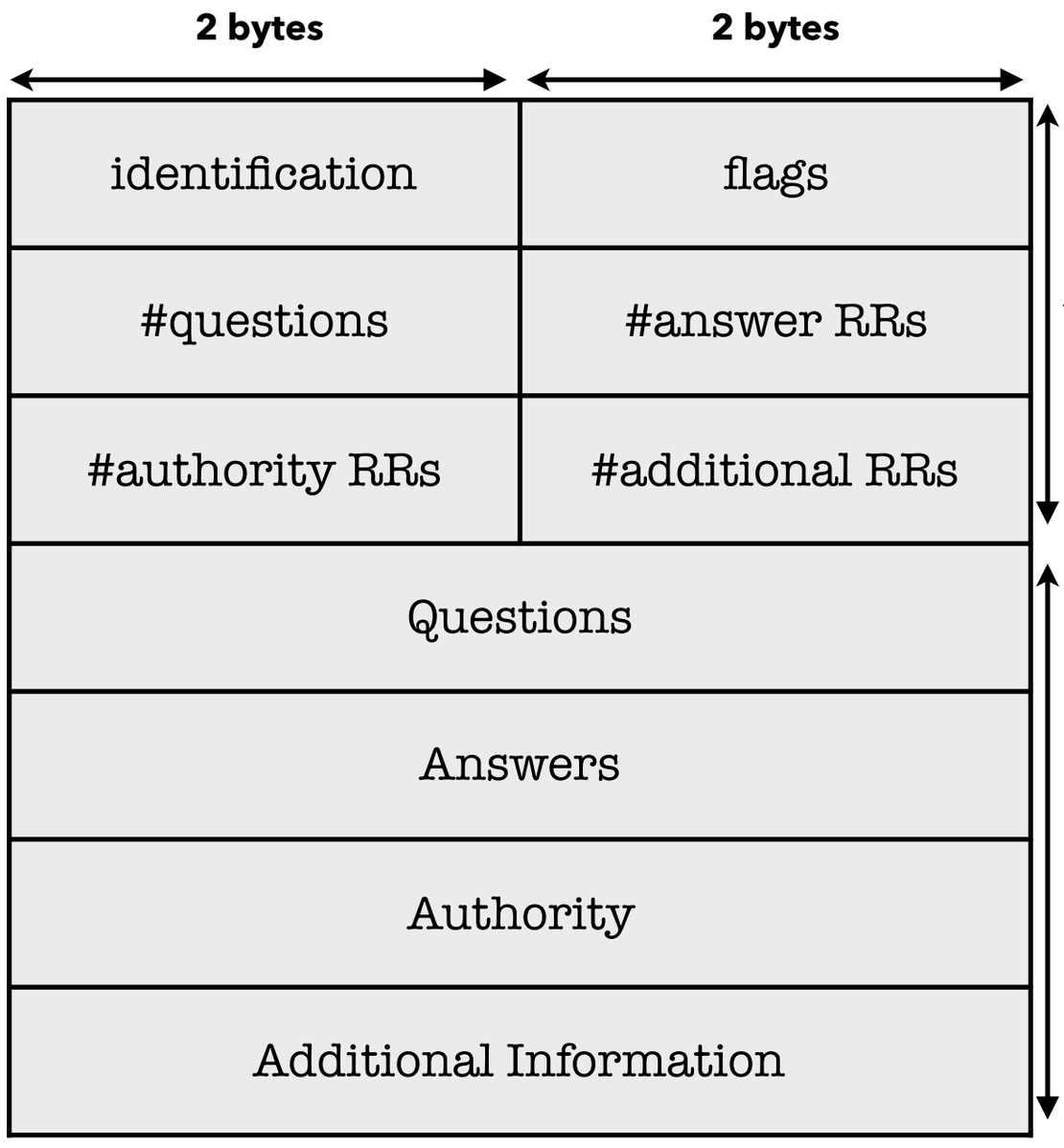
RR = (name, value, type, TTL)

Type	Name	Value	TTL
A (Authoritative)	hostname, e.g en.wikipedia.com	IP address	TTL
NS (Name Server)	domain, e.g wikipedia.com	hostname of authoritative server of this domain, e.g: en.wikipedia.com	TTL
CNAME (Canonical Name)	alias name for some canonical (real) hostname	canonical hostname name	TTL
MX (Mail)	domain, e.g: example.com	mailserver name, e.g: mail.example.com	TTL

DNS PROTOCOL

This is the protocol to make a DNS query or reply.

Both query and reply has the same message format



- Identification: 16bit # for query, reply uses the same #
- Flags:
  - Q/R
  - Recursion desired / available
  - Reply is authoritative?

16 bits so you can have 2^16 questions in a single DNS query

INSERTING DNS RECORDS

How do you insert (register) DNS records so people in the internet can find your website?

1. Register yournewwebsite.com at **DNS registrar,** e.g: Verisign registry
2. You need to provide names, IP addresses of authoritative name server (**primary and secondary server as backup**)
3. Registrar inserts the RRs into **.com TLD server,** e.g:
    - yournewwebsite.com, hostnameprimary.yournewwebsite.com, NS
    - yournewwebsite.com, hostnamesecondary.yournewwebiste.com NS
    - hostnameprimary.yournewwebsite.com, ZZZ.ZZZ.ZZZ.Z, A
    - hostnamesecondary.yournewwebsite.com, ZZZ.ZZZ.ZZZ.Z, A

ATTACKING DNS

- DDoS Attack
  - Bombard root server with traffic
  - Bombard TLD servers
- Redirect Attack
  - Man-in-the-middle
  - DNS poisoning
- Exploit DNS for DDoS