CS3103: Computer Networks Practice

Network Applications - DNS

DNS Concepts

Hierarchical Name System and Storage

DNS Protocol

Introduction to DNS Lab

Dr. Anand Bhojan
COM3-02-49, School of Computing
banand@comp.nus.edu.sg ph: 651-67351

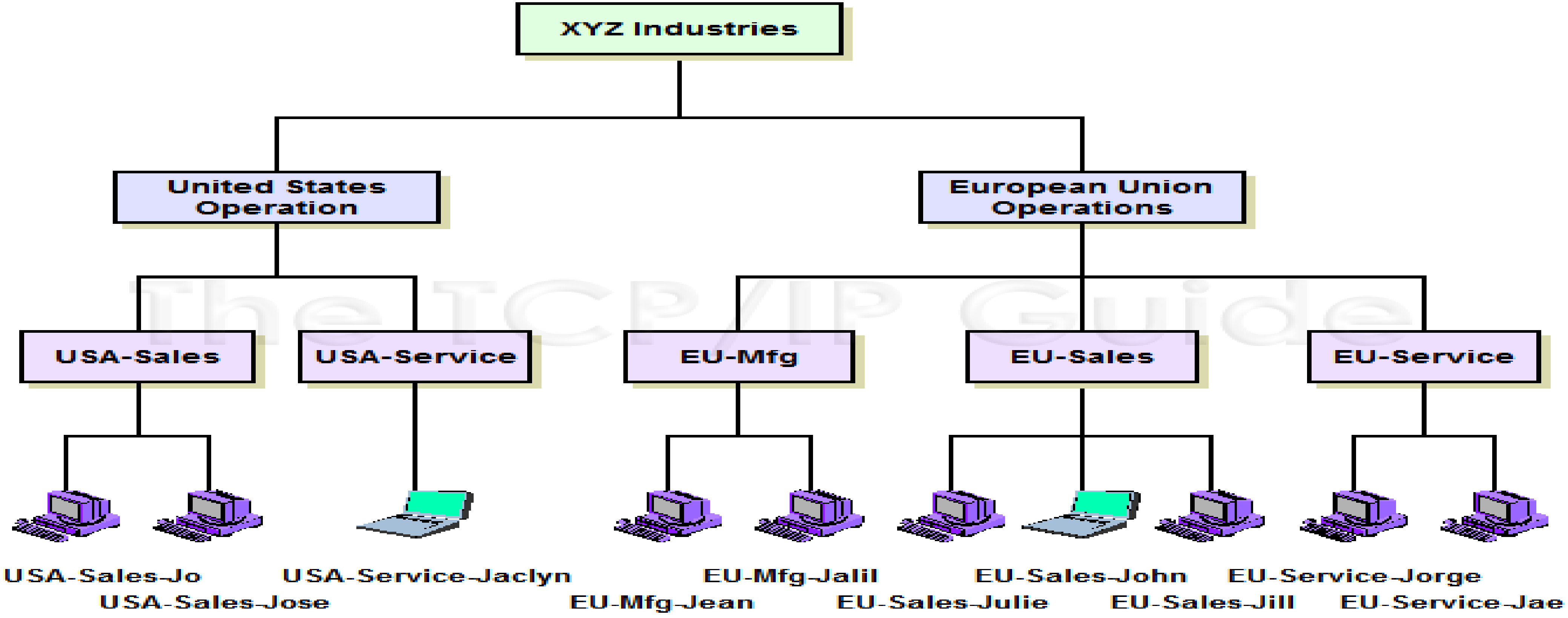
Domain Name System (DNS)

- Questions to ponder…

Q: What are some effective methods for generating unique names for every individual in the world?

Domain Name Space

HIERARCHICAL NAME SPACE

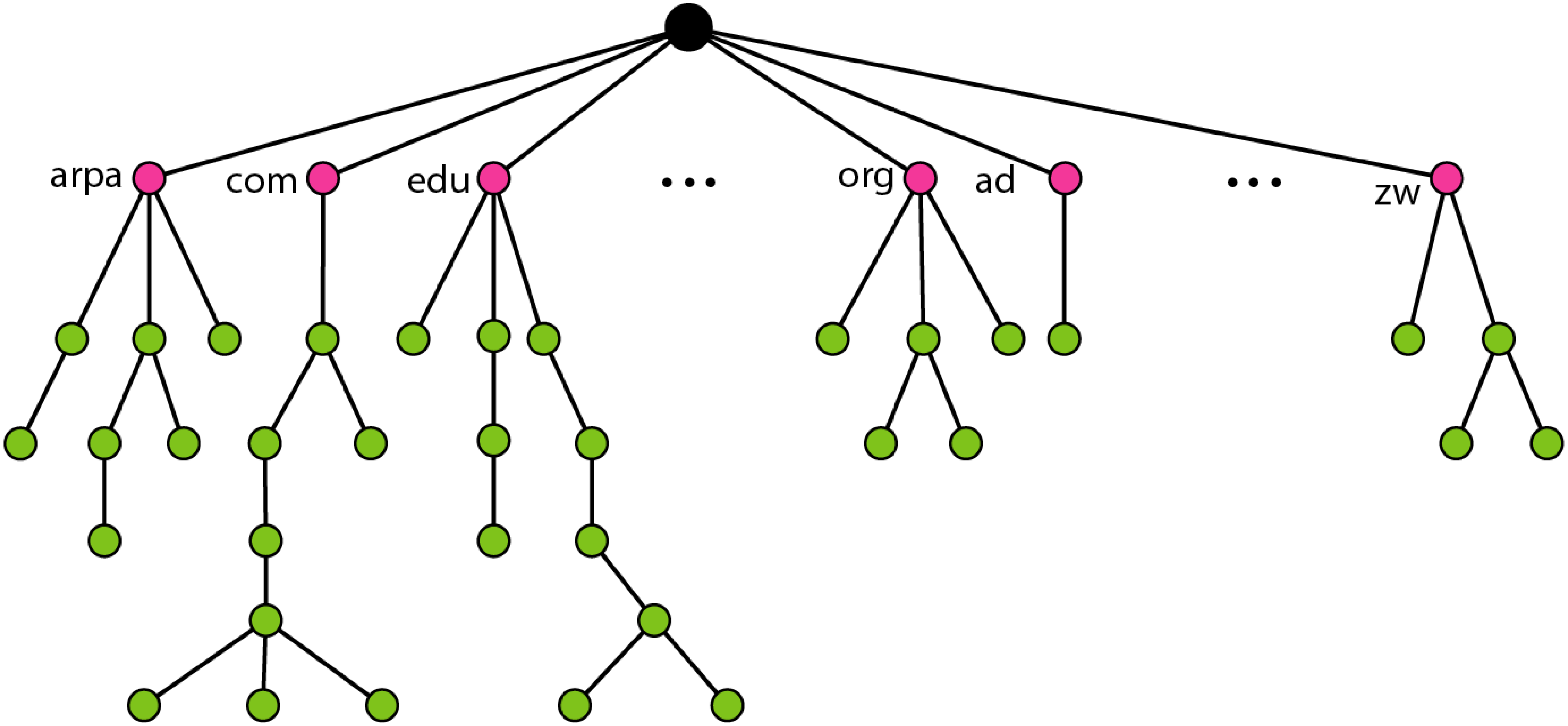


-The name consists of discrete elements that are related to each other usually using hierarchical "parent/child" semantics.

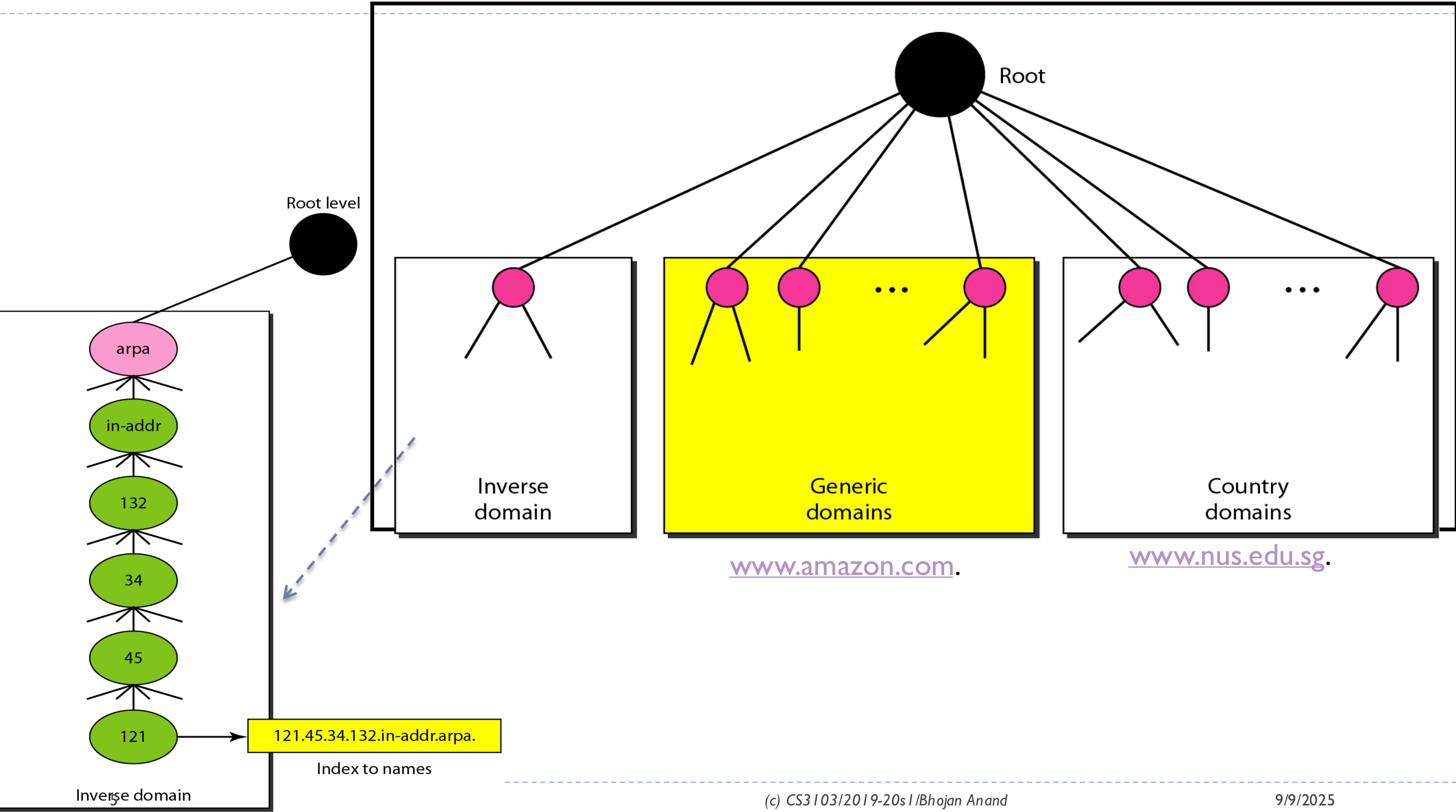
- Easy to avoid conflicts

Image source: http://www.tcpipguide.com

Domain Name Space



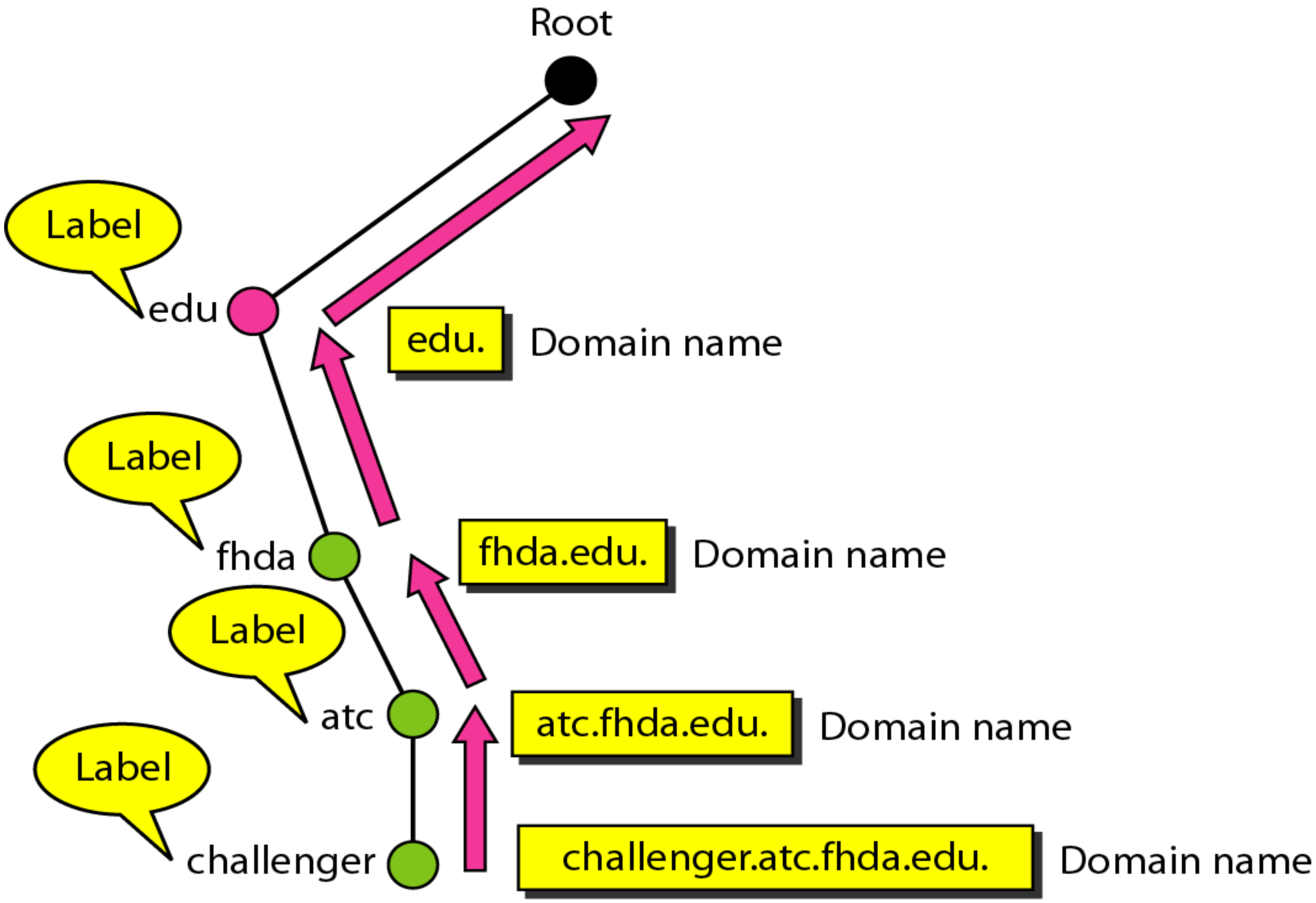
Domain Name Space in Internet



www.amazon.com.

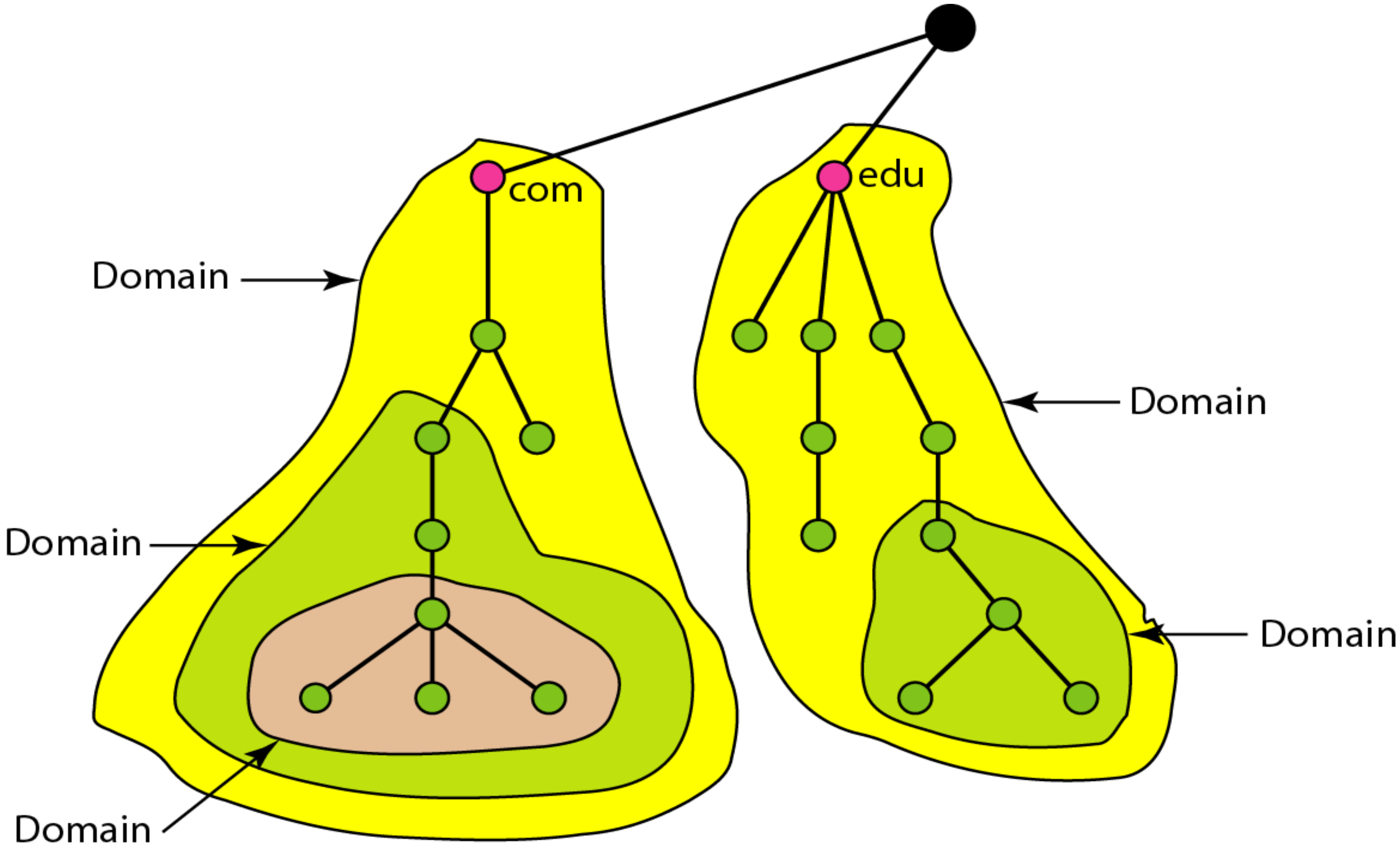
www.nus.edu.sg.

Domain Names



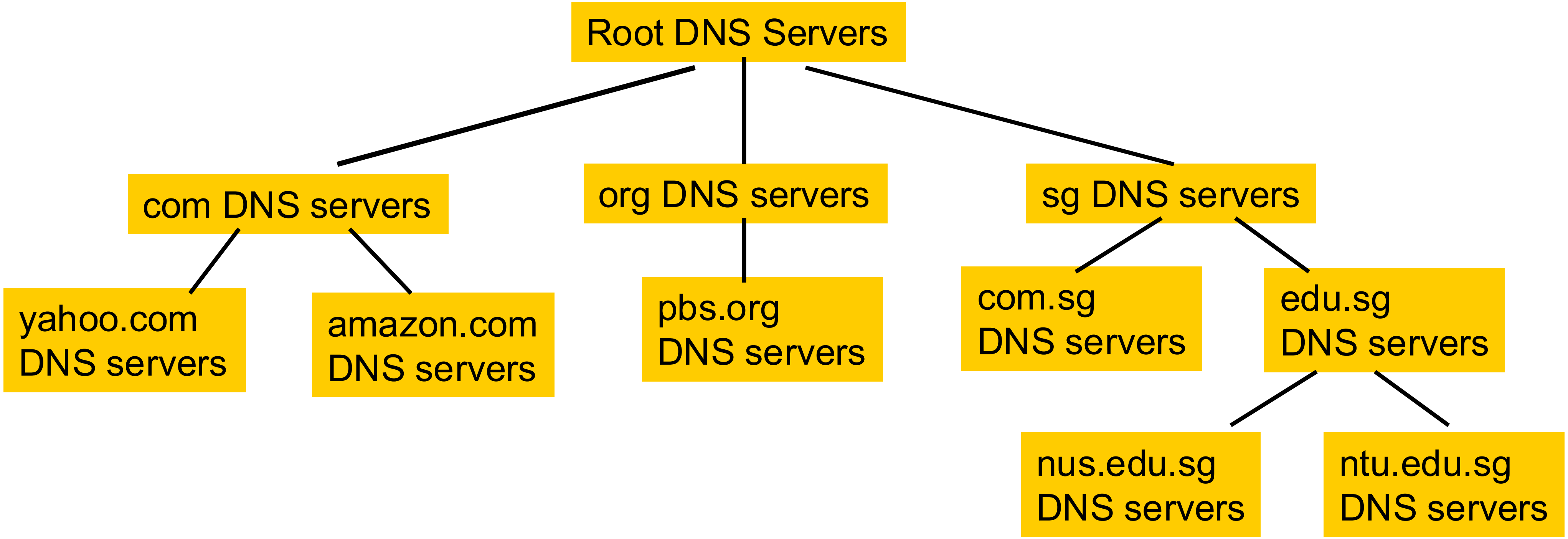
Domain

- Domain – is a subtree of the domain name space.



- The information contained in the domain name space must be stored.
  Q:Where and How? – Next slide…

Hierarchical storage of Domain Name Space



Client in NUS wants IP for www.amazon.com:

are all domains DNS?

- Client queries a NUS DNS server to find a root server
- Client queries a root server to find com DNS server
- Client queries com DNS server to get amazon.com DNS server
- Client queries amazon.com DNS server to get IP address for www.amazon.com

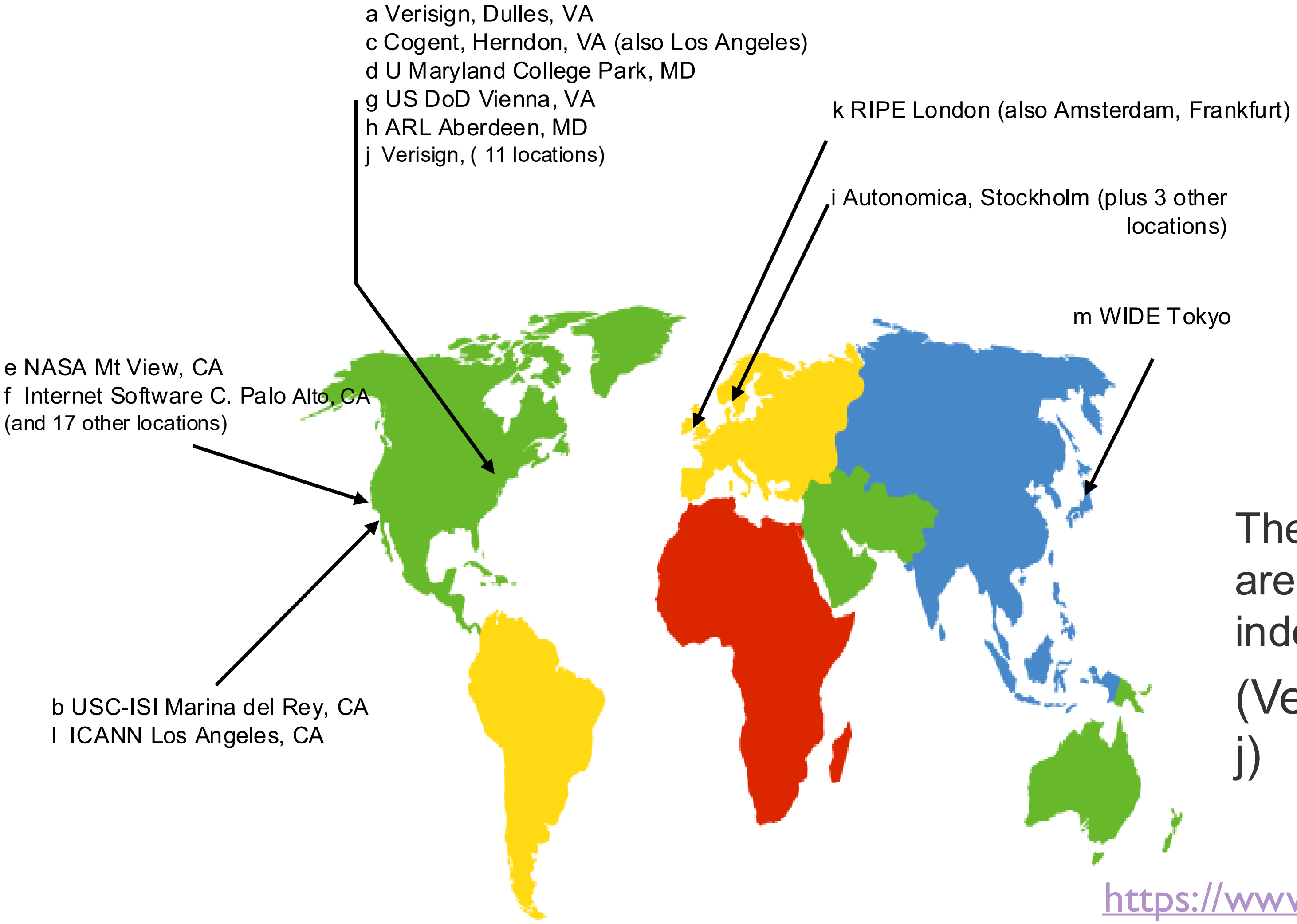
Domain Name System

- DNS Components
  - An hierarchical name system
  - Distributed database implemented in hierarchy of many name servers
  - Application on top of UDP/TCP:
    - DNS Resolver (Client)
    - DNS Server application
    - DNS server port 53.

- Q:Why not centralized DNS?

- If the size of the response message is more than 512 bytes, a TCP connection is used instead of UDP.

ROOT DNS Servers



a Verisign, Dulles, VA
c Cogent, Herndon, VA (also Los Angeles)
d U Maryland College Park, MD
g US DoD Vienna, VA
h ARL Aberdeen, MD
j Verisign, (11 locations)

k RIPE London (also Amsterdam, Frankfurt)

i Autonomica, Stockholm (plus 3 other locations)

m WIDE Tokyo

e NASA Mt View, CA
f Internet Software C. Palo Alto, CA
(and 17 other locations)

b USC-ISI Marina del Rey, CA
l ICANN Los Angeles, CA

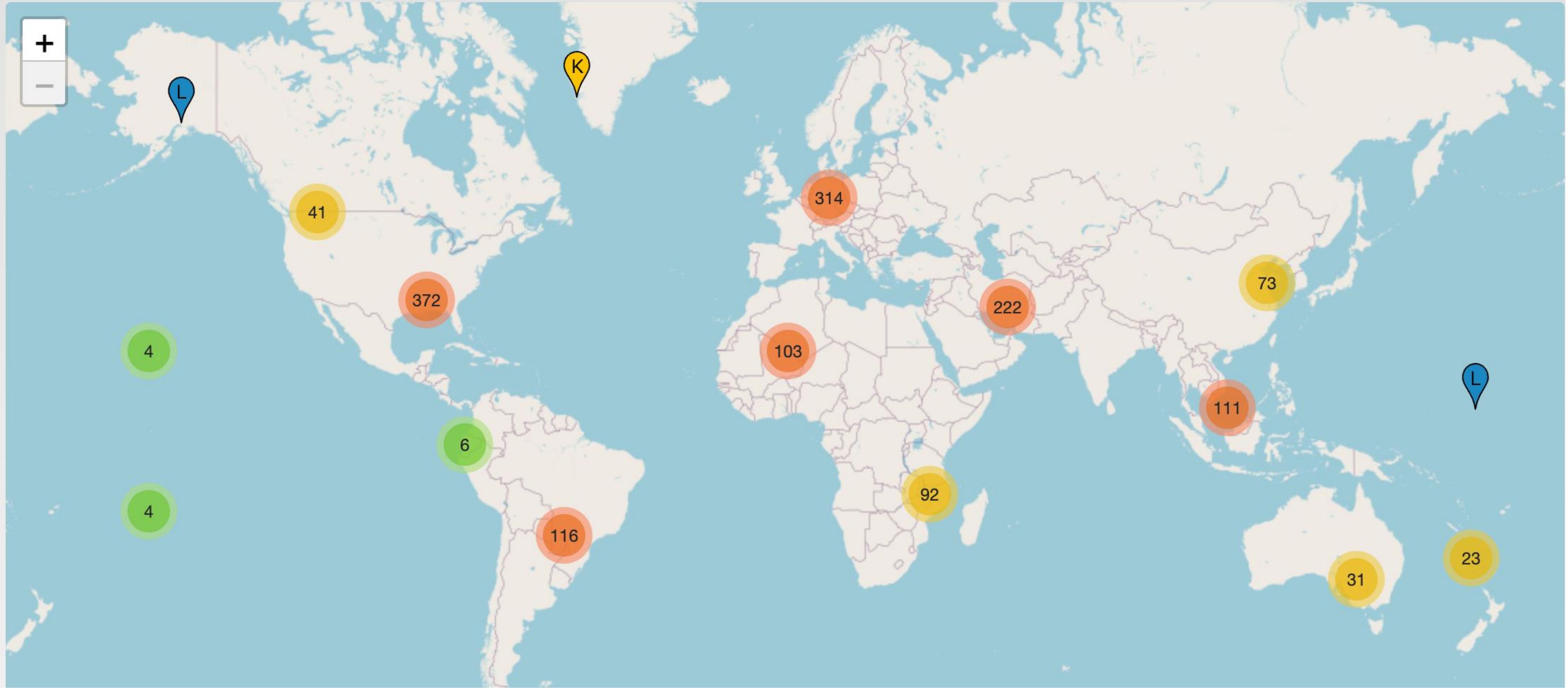
The 13 root name servers are operated by 12 independent organisations.

(Verisign operates – a & j)

https://www.iana.org/domains/root/servers

Q: What are the possible attacks on Root Servers, TLD Servers? <active learning>

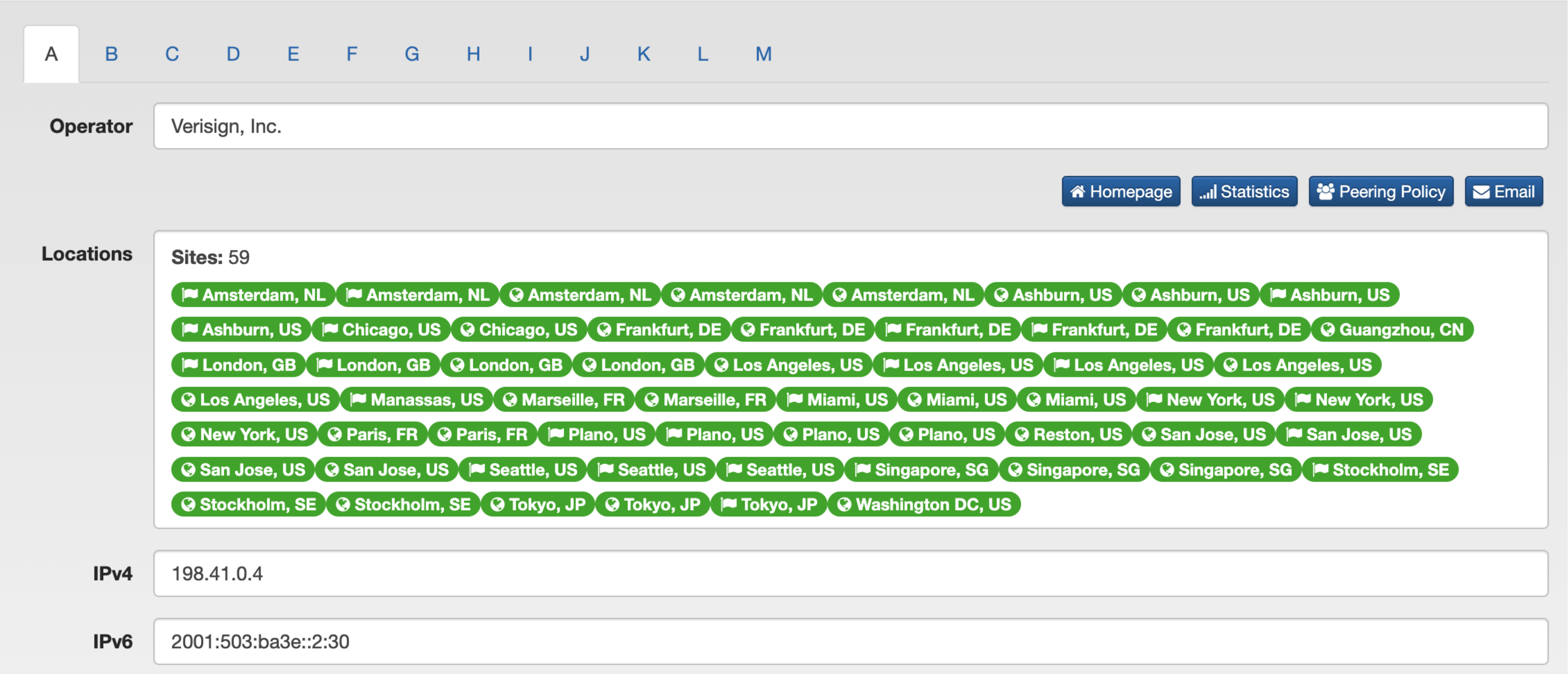
ROOT DNS Servers



http://www.root-servers.org/

As of 2024-09-09T23:01:32Z, the root server system consists of 1866 instances

A-Root Servers



Operator Verisign, Inc.

Locations

Sites: 59

⚑ Amsterdam, NL ⚑ Amsterdam, NL 🌐 Amsterdam, NL 🌐 Amsterdam, NL 🌐 Amsterdam, NL 🌐 Ashburn, US 🌐 Ashburn, US ⚑ Ashburn, US
⚑ Ashburn, US ⚑ Chicago, US 🌐 Chicago, US 🌐 Frankfurt, DE 🌐 Frankfurt, DE ⚑ Frankfurt, DE ⚑ Frankfurt, DE 🌐 Frankfurt, DE 🌐 Guangzhou, CN
⚑ London, GB ⚑ London, GB 🌐 London, GB 🌐 London, GB 🌐 Los Angeles, US ⚑ Los Angeles, US ⚑ Los Angeles, US 🌐 Los Angeles, US
🌐 Los Angeles, US ⚑ Manassas, US 🌐 Marseille, FR 🌐 Marseille, FR ⚑ Miami, US 🌐 Miami, US 🌐 Miami, US ⚑ New York, US ⚑ New York, US
🌐 New York, US 🌐 Paris, FR 🌐 Paris, FR ⚑ Plano, US ⚑ Plano, US 🌐 Plano, US 🌐 Plano, US 🌐 Reston, US 🌐 San Jose, US ⚑ San Jose, US
🌐 San Jose, US 🌐 San Jose, US ⚑ Seattle, US ⚑ Seattle, US ⚑ Seattle, US ⚑ Singapore, SG 🌐 Singapore, SG 🌐 Singapore, SG ⚑ Stockholm, SE
🌐 Stockholm, SE 🌐 Stockholm, SE 🌐 Tokyo, JP 🌐 Tokyo, JP ⚑ Tokyo, JP 🌐 Washington DC, US

IPv4 198.41.0.4

IPv6 2001:503:ba3e::2:30

There are 59 instances of a-root servers.

Q:When all these instances use same IP address, how and where the packets are routed? <active learning>

TLD, authoritative servers

top-level domain (TLD) servers:

- responsible for com, org, net, edu, aero, jobs, museums, and all top-level country domains, e.g.: uk, fr, ca, jp
- Network Solutions maintains servers for .com TLD
- Educause for .edu TLD

authoritative DNS servers:

- organization’s own DNS server(s), providing authoritative hostname to IP mappings for organization’s named hosts
- can be maintained by organization or service provider

Local DNS name server [DNS Resolver]

- does not strictly belong to hierarchy
- each ISP (residential ISP, company, university) has one
  - also called "default name server"
- when host makes DNS query, query is sent to its local DNS server
  - has local cache of recent name-to-address translation pairs (but may be out of date!)
  - acts as proxy, forwards query into hierarchy

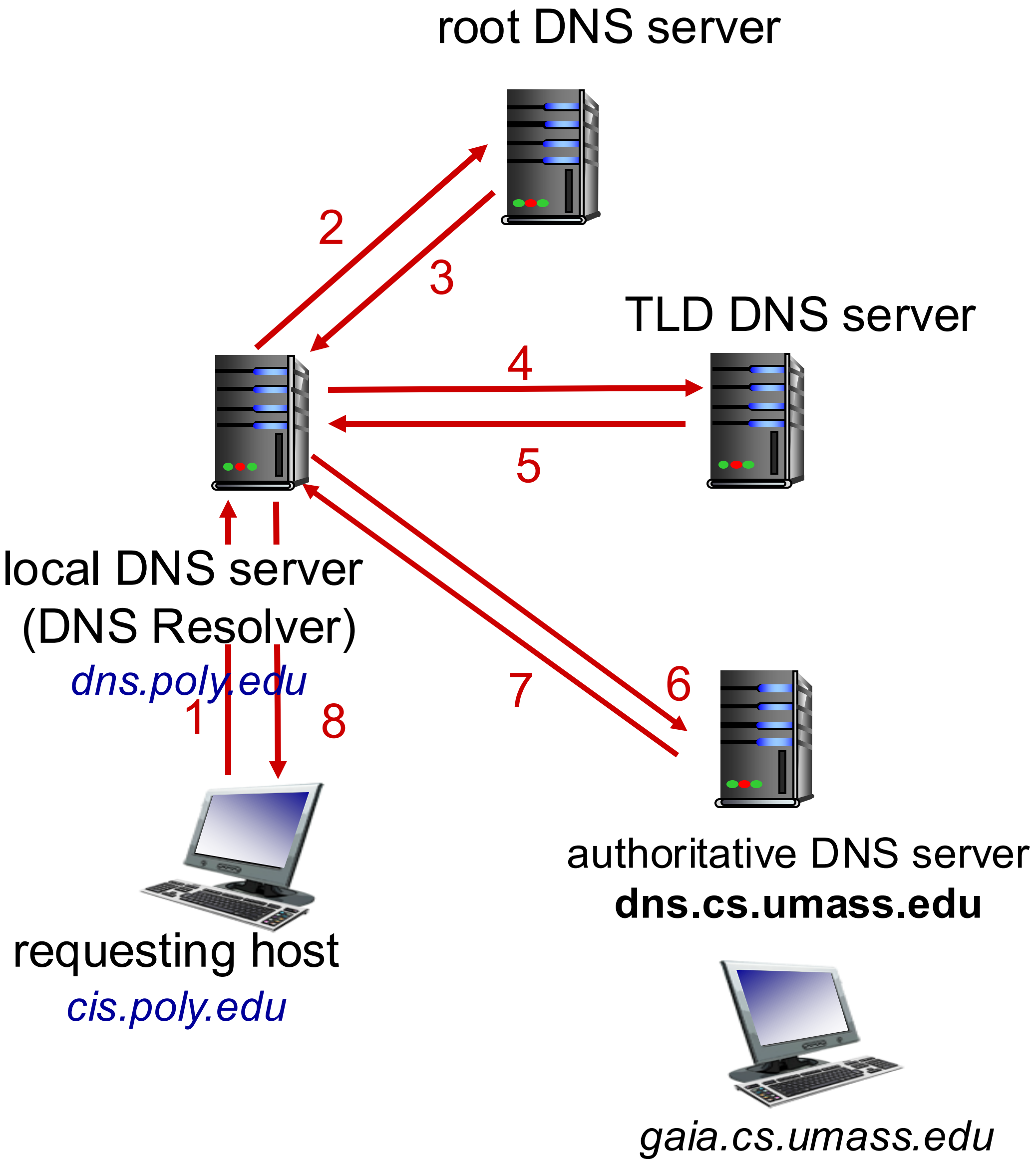
DNS name resolution example

- host at cis.poly.edu wants IP address for gaia.cs.umass.edu

iterated query:

- contacted server replies with name of server to contact
- "I don't know this name, but ask this server"

wats the difference and when is it used?

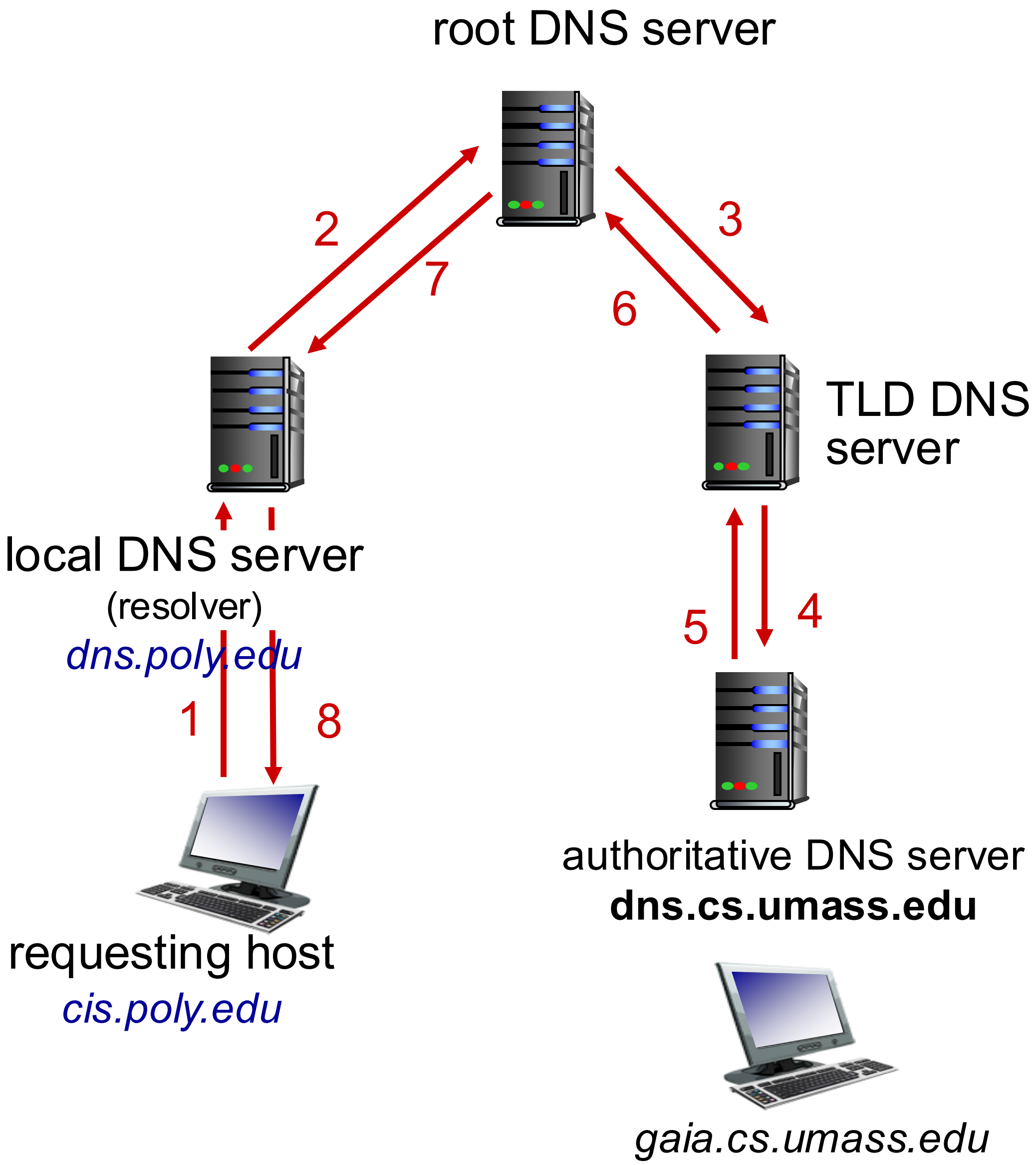


DNS name resolution example

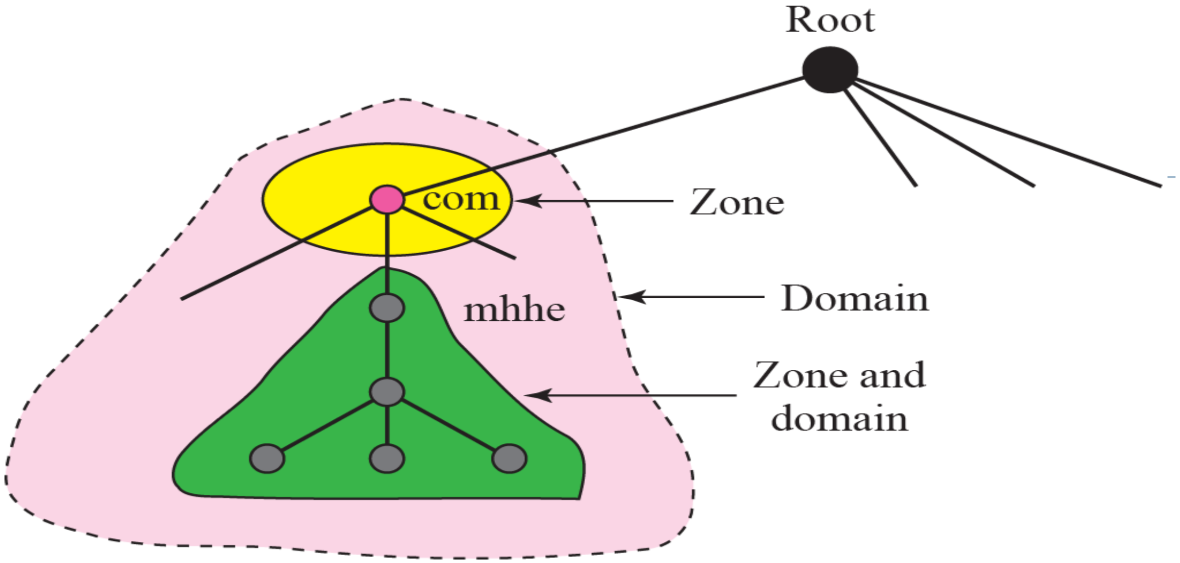
recursive query:

- puts burden of name resolution on contacted name server
- heavy load at upper levels of hierarchy?

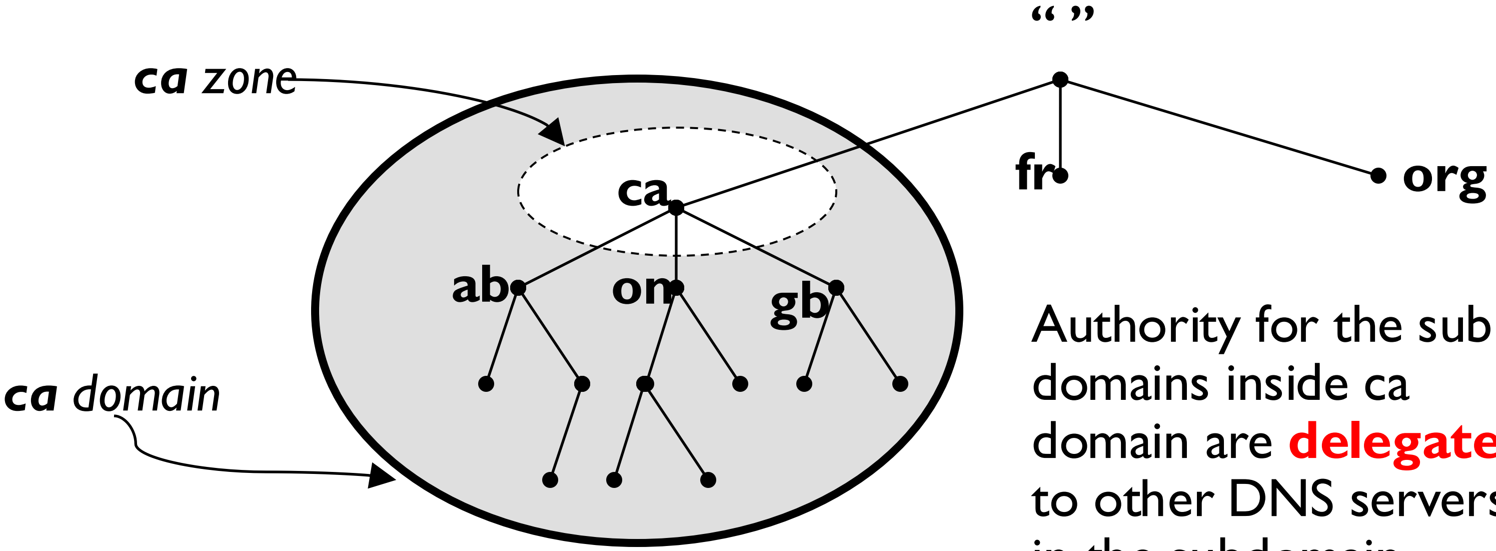
Q: Have you ever used DNS service IP: 8.8.8.8 or 8.8.4.4?



Domain & Zone



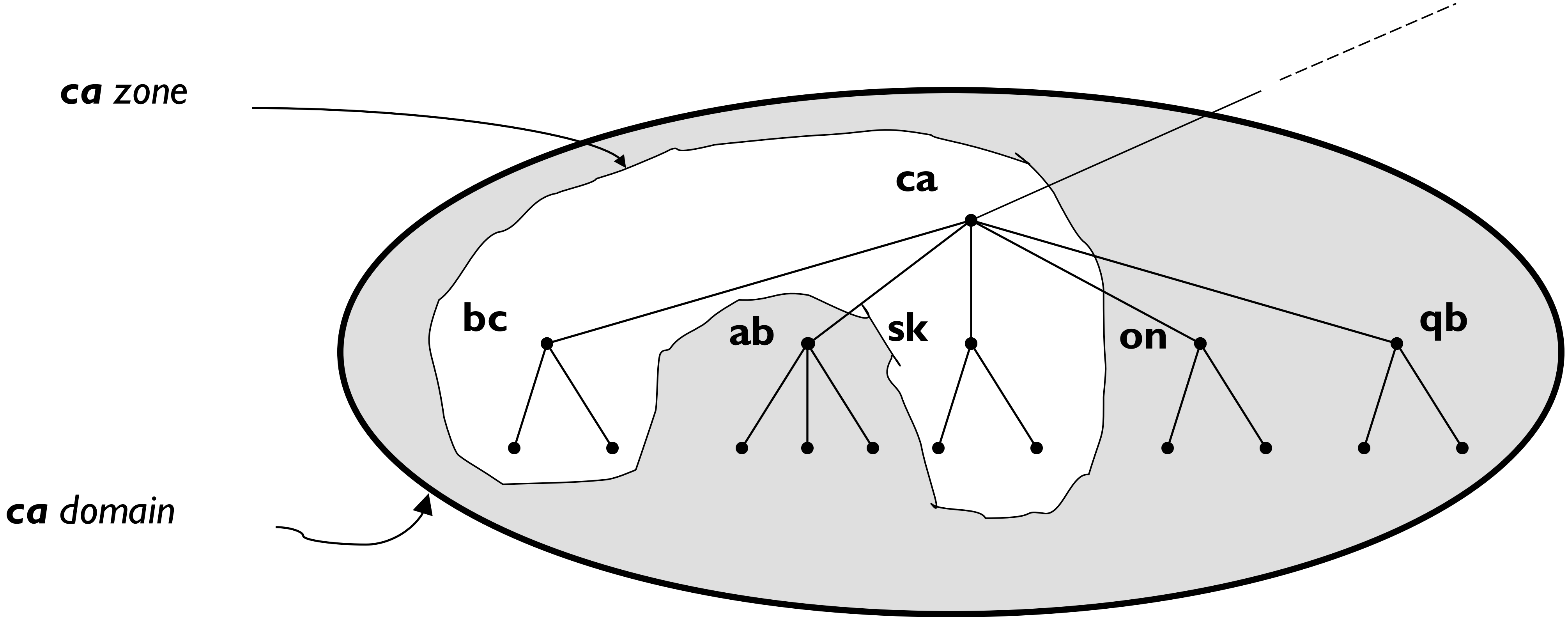
- *Domain* is a subtree of the domain name space.
- The DNS server for a domain can either store information about every node in the domain or divide the domain into sub-domains and delegate part of its authority to other servers. **What a server is responsible for or has authority over is called a *Zone*.**



Authority for the sub domains inside ca domain are **delegated** to other DNS servers in the subdomain.

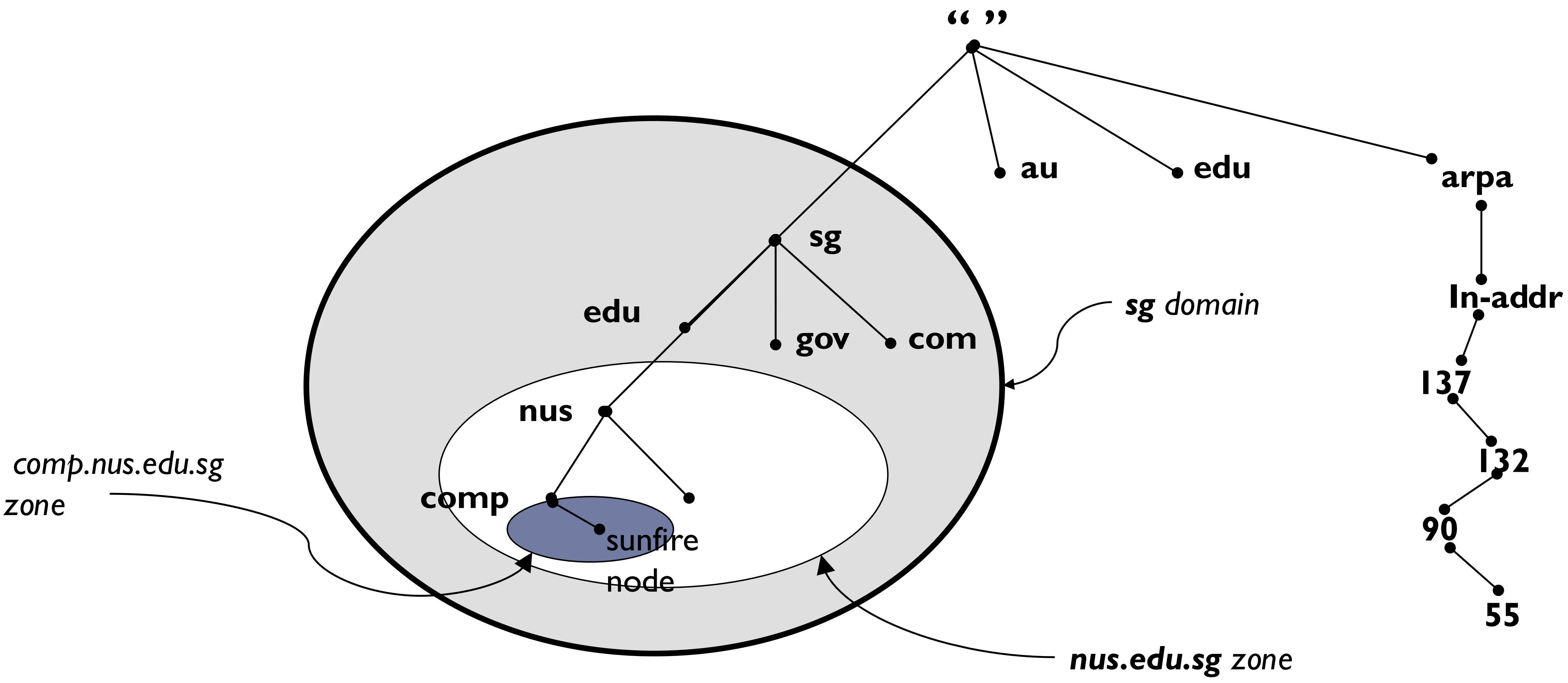
[Source: Fig 2.8 of DNS and BIND by Paul Albitz & Cricket Liu]

Domain & Zone



[Source: Fig 2.9 of DNS and BIND by Paul Albitz & Cricket Liu]

A Node in Multiple Zones



Primary/Secondary Servers

- Primary server stores information about the zone it is an authority for
  - Creates, maintains and updates zone file
- Secondary server has the complete information about a zone (transfer from primary or secondary server – zone transfer)
  - Cannot create or update zone file
- Primary and secondary servers are both authoritative for the zone they serve. They provide authoritative answer for their zone.
  - An authoritative answer from a name server (such as reading the data from the disk) is "guaranteed" to be accurate
  - A non-authoritative answer (such as an answer from the cache) may not be accurate

DNS – Resource Records

- DNS: distributed db storing resource records (RR)

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

➢Type=A

✶**`name`** is hostname

✶**`value`** is IP address

➢Type=NS (List a name server for this domain)

✶**`name`** is domain (e.g. foo.com)

✶**`value`** is hostname of authoritative name server for this domain (primary & secondary)

➢Type=CNAME

✶**`name`** is alias name for some "canonical" (the real) name

`www.nus.edu.sg` is really `mgnzsqc.x.incapdns.net`

✶**`value`** is canonical name

➢Type=MX (List a mail server for this domain)

✶**`value`** is name of mailserver associated with **`name`**

DNS – Resource Records

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

- Type=SOA (Indicates authority for this domain data)
  - **`name`** is domain (e.g. foo.com)
  - **`value`** is hostname of authoritative name server (only primary) for this domain and other info.
  - ttl – time-to-live when cached by others

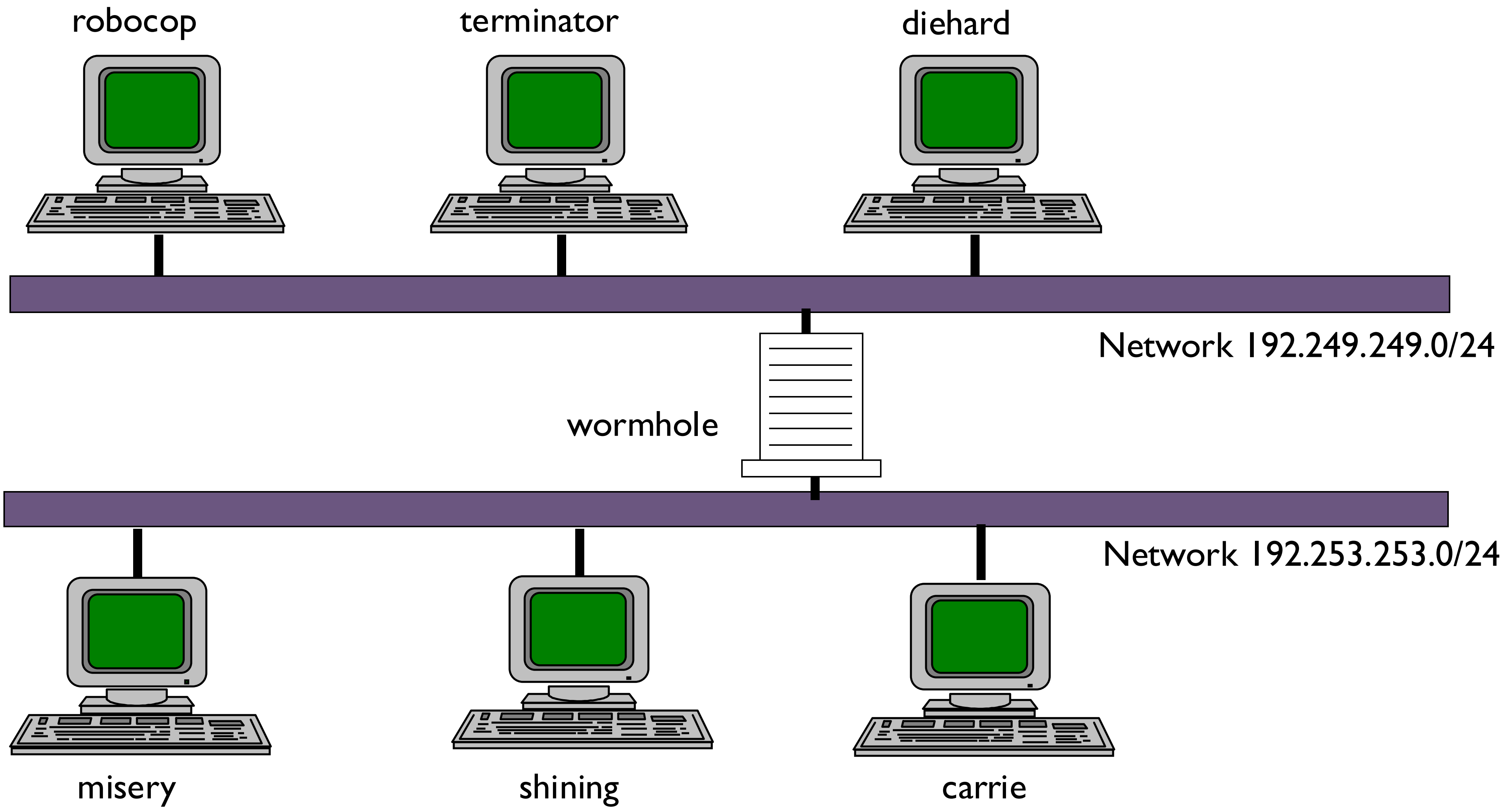
- Type=PTR
  - **`name`** is IP address (in-addr.arpa Domain)
  - **`value`** is host name

Some of the other records:

TXT	Textual information
WKS	Well-known services
HINFO	Host information
DNSKEY	Public Key
RRSIG	Signature

RR - An Example: Network used

[Source: Fig 4.1 of DNS and BIND by Paul Albitz & Cricket Liu]



RR – An Example (cont)

SOA records (Start of authority)

Indicates the domains for which it is authoritative.

```
movie.edu.   IN  SOA  terminator.movie.edu.  al.robocop.movie.edu (
                         1                ; Serial
                         10800            ; Slave refresh after 3 hours
                         3600             ; Slave retry after 1 hour
                         604800           ; Slave data expire after 1 week
                         86400 )          ; Resolver-cache Minimum TTL of 1 day
```

NS records (Name Server)

One record for each name server for the domain

```
movie.edu.    IN   NS  terminator.movie.edu.
movie.edu.    IN  NS  wormhole.movie.edu.
```

RR – An Example (cont)

A records (Address)

Provides name-to-address mapping

```
;
;Addresses for the canonical names
;
localhost.movie.edu.     IN A      127.0.0.1
robocop.movie.edu.       IN A      192.249.249.2
terminator.movie.edu.    IN A      192.249.249.3
diehard.movie.edu.       IN A      192.249.249.4
misery.movie.edu.        IN A      192.253.253.2
shining.movie.edu.       IN A      192.253.253.3
carrie.movie.edu.        IN A      192.253.253.4

wormhole.movie.edu.      IN A      192.249.249.1
wormhole.movie.edu.      IN A      192.253.253.1
```

RR – An Example (cont)

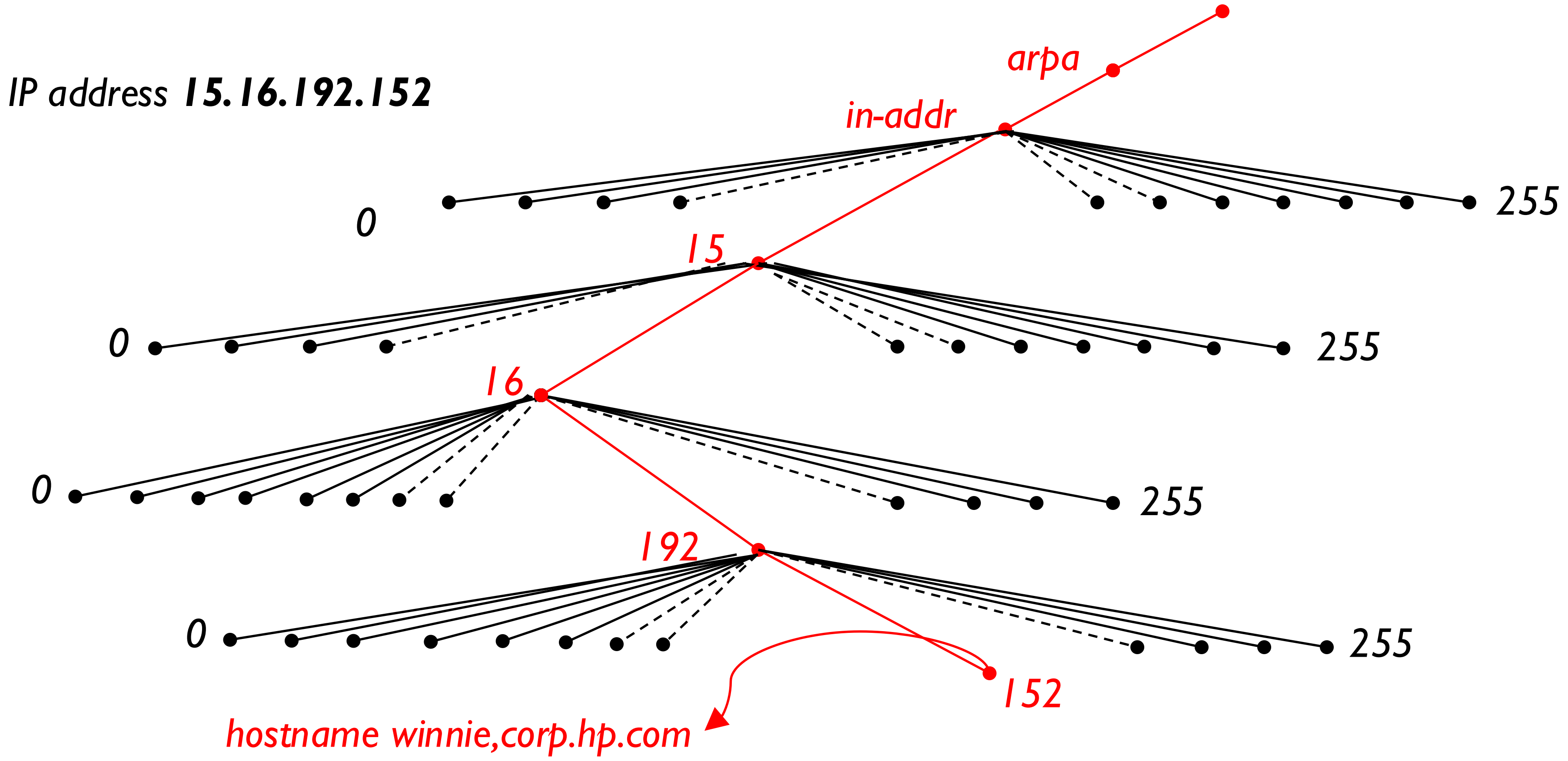
CNAME records (Alias)

Aliases are created using CNAME record (canonical name).

```
bigt.movie.edu.     IN  CNAME   terminator.movie.edu.
dh.movie.edu.       IN  CNAME   diehard.movie.edu.
wh.movie.edu.       IN  CNAME   wormhole.movie.edu.
```

Mapping Addresses to Names

- Similar technique is followed to search the name space.
- Create in-addr.arpa domain in which names are numbers!



152.192.16.15.in-addr.arpa is the address of the domain name winnie.corp.hp.com

[Source: Fig 4.1 of DNS and BIND by Paul Albitz & Cricket Liu]

RR – An Example (cont)

PTR records (Pointer)

Used for creating address-to-name mappings (inverse domain)

```
1.249.249.192.in-addr.arpa.    IN  PTR        wormhole.movie.edu.
2.249.249.192.in-addr.arpa.    IN  PTR        robocop.movie.edu.
3.249.249.192.in-addr.arpa.    IN  PTR        terminator.movie.edu.
4.249.249.192.in-addr.arpa.    IN  PTR        diehard.movie.edu.
```

DNS Database (in our Lab)

- DNS server program: named
- DNS Database is usually created using the following 3 files

  (The files are created inside 'named' folder)

  - *db.domain – for name to address mapping, cname, mail and other records*
  - *db.domain.rev – for address to name mapping records (inverse domain)*
  - *db.127.0.0 – for loopback address to name, name to address mapping*

- A configuration file for "named" program is created inside 'named' folder.
  - Filename: named.conf
  - This file points to the above 3 files which collectively contains the DNS database.
- Run the DNS Server
  - *sudo named –c named.conf*

DNS Database Example 1 *(db.domain)*

```
$TTL 86400
comp.nus.edu.sg. IN SOA  ns1.comp.nus.edu.sg.    admin.ns1.comp.nus.edu.sg.  (
   1               ;Serial
   10800           ;Refresh after 3 hours
   3600            ;Retry after 1 hour
   604800          ;Expire after 1 week
   86400 )         ;Minimum TTL of 1 day
;
; Name servers
;
comp.nus.edu.sg.            IN        NS                  ns1.comp.nus.edu.sg.
;
; Addresses for canonical names
;
anand.comp.nus.edu.sg.                IN       A                  137.132.5.10
www0.comp.nus.edu.sg.                 IN       A                  137.132.5.11
lee.comp.nus.edu.sg.                  IN       A                  137.132.5.12
mikhil.comp.nus.edu.sg.               IN       A                  137.132.5.13
;
; Aliases
;
www.comp.nus.edu.sg.                  IN       CNAME              www0.comp.nus.edu.sg.
```

DNS Database Example 2 – inverse mapping *(db.domain.rev)*

```
$TTL 86400
comp.nus.edu.sg. IN SOA  ns1.comp.nus.edu.sg.   admin.ns1.comp.nus.edu.sg. (
  1                  ;Serial
  10800              ;Refresh after 3 hours
  3600        ;Retry after 1 hour
  604800      ;Expire after 1 week
  86400 )     ;Minimum TTL of 1 day
;
;
; Name servers
;
5.132.137.in-addr.arpa.     IN     NS     ns1.comp.nus.edu.sg.
;
; Addresses point to canonical name
;
10.5.132.137.in-addr.arpa.  IN     PTR    anand.comp.nus.edu.sg.
11.5.132.137.in-addr.arpa.  IN     PTR    www0.comp.nus.edu.sg.
13.5.132.137.in-addr.arpa.  IN     PTR    mikhil.comp.nus.edu.sg.
```

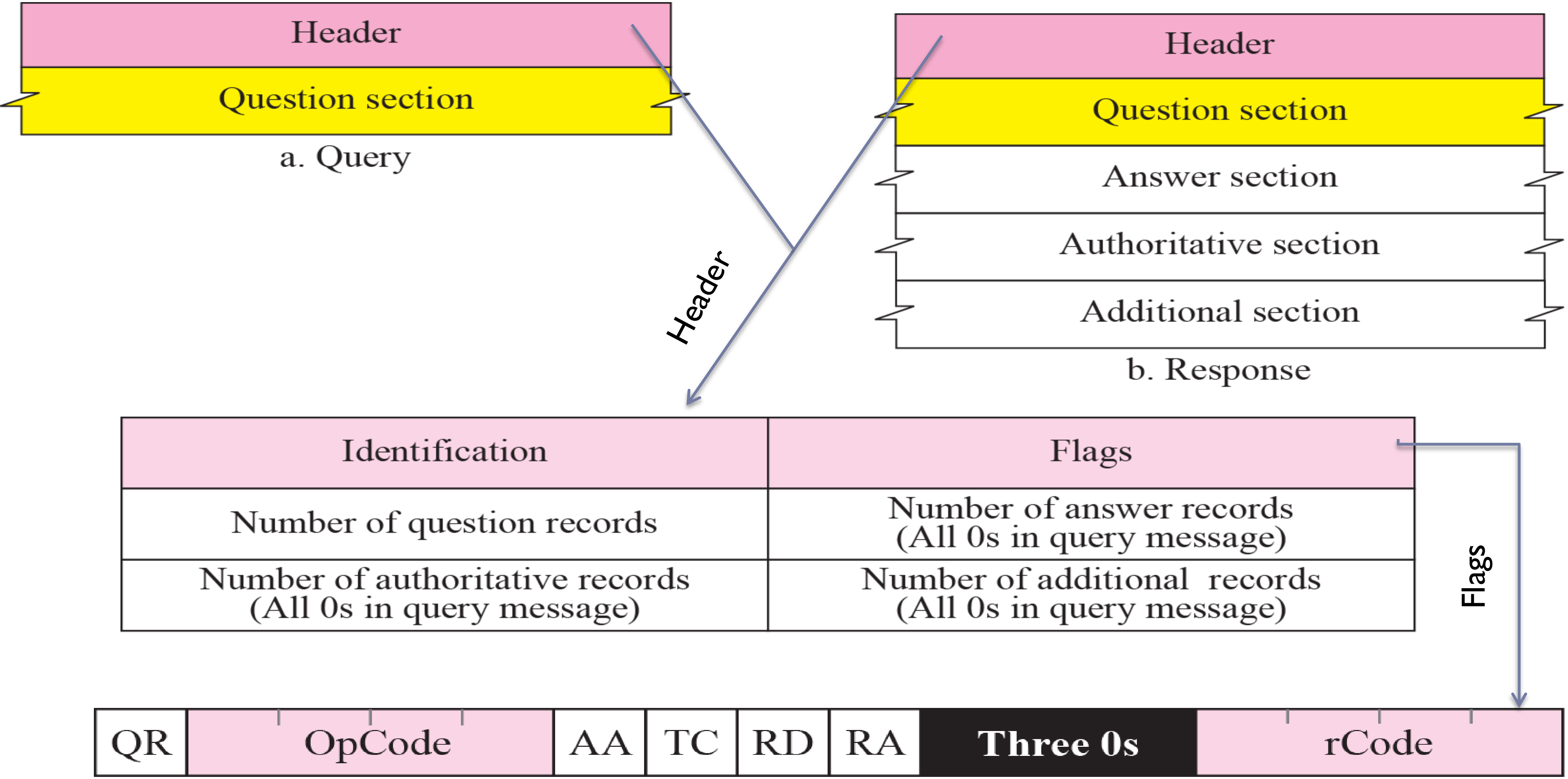
Client Configuration

- DNS Client Program must know the default DNS server (Resolver)

- $ cat /etc/resolv.conf

```
nameserver 138.23.169.10
nameserver 138.23.178.2
```

DNS Messages



Header

Question section

a. Query

Header

Question section

Answer section

Authoritative section

Additional section

b. Response

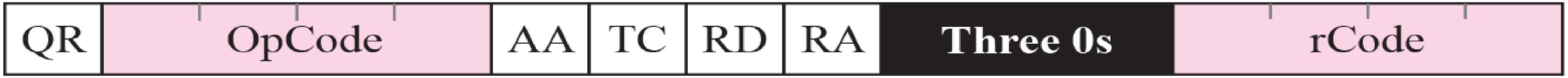
Header

Identification	Flags
Number of question records	Number of answer records (All 0s in query message)
Number of authoritative records (All 0s in query message)	Number of additional records (All 0s in query message)

Flags

QR	OpCode	AA	TC	RD	RA	Three 0s	rCode

Flags – Explained…



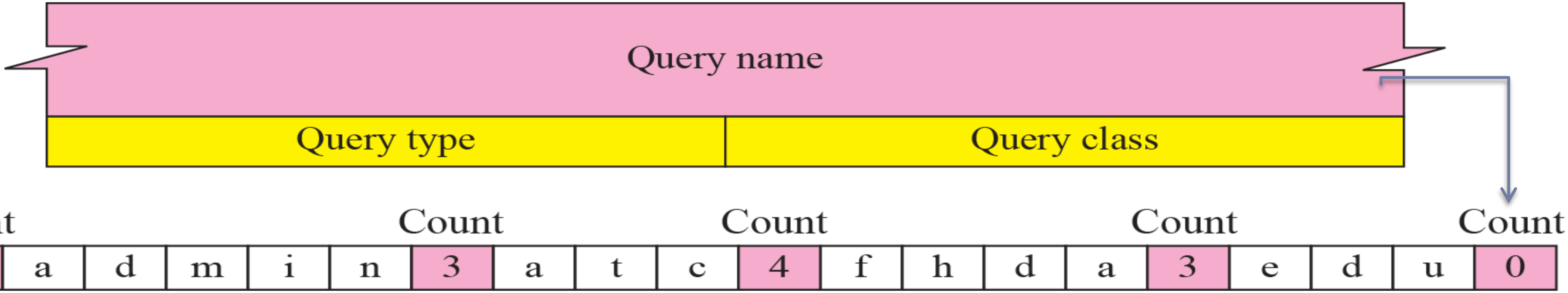
QR	OpCode	AA	TC	RD	RA	Three 0s	rCode

- Q/R - 0 for query, 1 for response
- OpCode - standard (0), inverse (1), 2 (server status)
- AA - 1 if server is authoritative
- TC - 1 if truncated to 512 (if UDP is used)
- RD - 1 if client desires recursive answer
- RA - 1 if recursive response is available
- rCode - error code

Table 19.2 *Values of rCode*

Value	*Meaning*	*Value*	*Meaning*
0	No error	4	Query type not supported
1	Format error	5	Administratively prohibited
2	Problem at name server	6–15	Reserved
3	Domain reference problem		

Question Record Format



Query name

Query type | Query class

Count						Count				Count					Count				Count
5	a	d	m	i	n	3	a	t	c	4	f	h	d	a	3	e	d	u	0

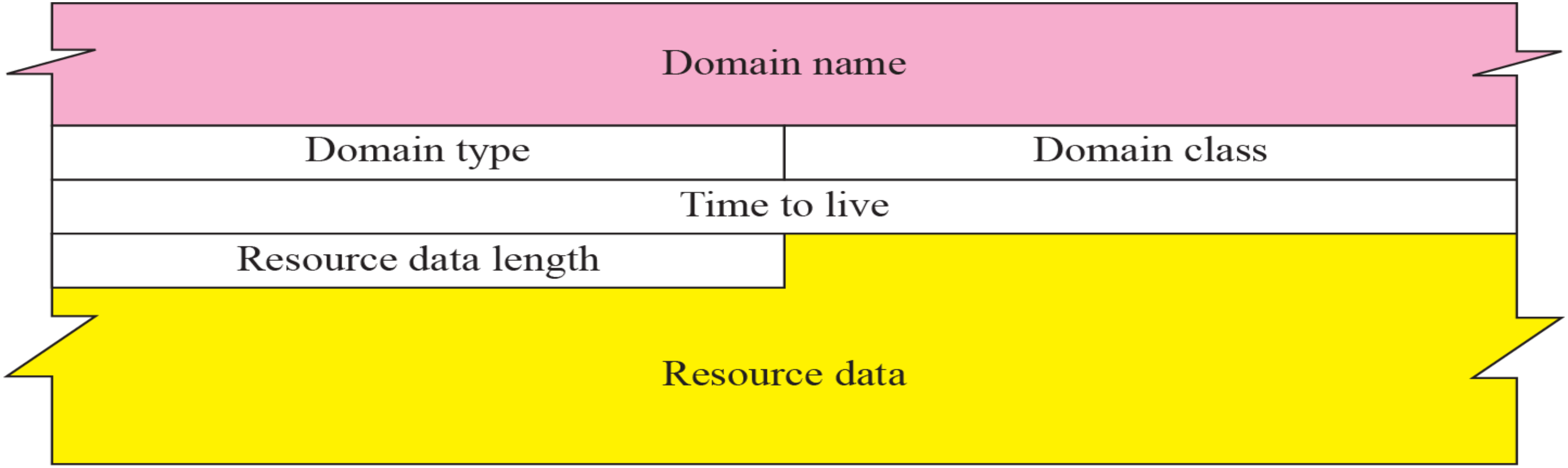
Table 19.3 *Types*

Type	*Mnemonic*	*Description*
1	A	**Address.** A 32-bit IPv4 address. It converts a domain name to an address.
2	NS	**Name server**. It identifies the authoritative servers for a zone.
5	CNAME	**Canonical name**. It defines an alias for the official name of a host.
6	SOA	**Start of authority**. It marks the beginning of a zone.
11	WKS	**Well-known services**. It defines the network services that a host provides.
12	PTR	**Pointer.** It is used to convert an IP address to a domain name.
13	HINFO	**Host information.** It defines the hardware and operating system.
15	MX	**Mail exchange**. It redirects mail to a mail server.
28	AAAA	**Address.** An IPv6 address (see Chapter 26).
252	AXFR	A request for the transfer of the entire zone.
255	ANY	A request for all records.

Class:

1 – Internet
2 – CSNET
3 – CS
4 - HS

Resource Record Format



Domain name

Domain type

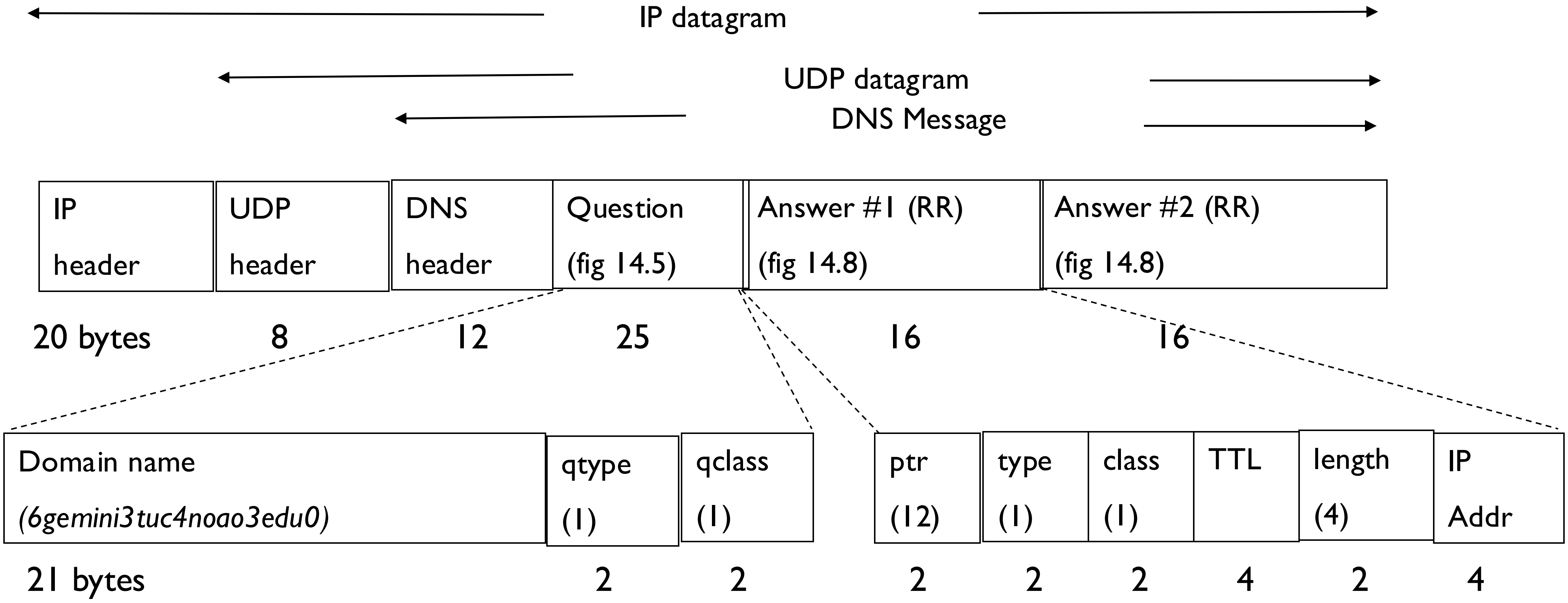
Domain class

Time to live

Resource data length

Resource data

Format of DNS Reply



IP header	UDP header	DNS header	Question (fig 14.5)	Answer #1 (RR) (fig 14.8)	Answer #2 (RR) (fig 14.8)
20 bytes	8	12	25	16	16

Domain name *(6gemini3tuc4noao3edu0)*	qtype (1)	qclass (1)
21 bytes	2	2

ptr (12)	type (1)	class (1)	TTL	length (4)	IP Addr
2	2	2	4	2	4

REGISTRARS

- How are new domains added to DNS? This is done through a registrar, a commercial entity accredited by ICANN (*Internet Corporation for Assigned Names and Numbers*). A registrar first verifies that the requested domain name is unique and then enters it into the DNS database. A fee is charged.

ICANN headquarters in Playa Vista, Los Angeles, California.

Inserting records into DNS

- Example: new startup "Anuflora Technologies"
- register name anuflora.com at *DNS registrar* (e.g., Network Solutions, Namesilo)
  - provide names, IP addresses of authoritative name server (primary and secondary)
  - registrar inserts two RRs into .com TLD server:

    ```
    (anuflora.com, dns1.anuflora.com, NS)
    (dns1.anuflora.com, 212.212.212.1, A)
    ```

- add the following to authoritative server,
  - type A record for www.anuflora.com;
  - type MX record for anuflora.com

Dynamic DNS

- When the DNS was designed, no one predicted that there would be so many address changes.
  - In DNS, when there is a change, such as adding a new host, removing a host, or changing an IP address, the change must be made to the DNS master file. The DNS master file must be updated dynamically. The *Dynamic Domain Name System* (DDNS) therefore was devised to respond to this need.

Dynamic DNS update

- In a Dynamic DNS (DDNS), the zone entries can be dynamically updated in real-time by a DDNS client. This means, for example, that the hostname records in a DNS can be updated by a DHCP server (which also functions as a DDNS client). Dynamic DNS is deployed in the SoC network.

- As a result, the use of Dynamic DNS does in fact continue to provide DHCP-configured hosts with a well-known and fixed and fully-qualified domain name. The hostname component of the client is specified in the host registration (i.e., chosen by the registered owner).

- The DDNS domain name used in SoC is d1.comp.nus.edu.sg (also, d2.comp.nus.edu.sg). DHCP clients will have their hostnames updated to this domain according to information supplied by the DHCP server.

- For example, if there is a DHCP client with the registered name host1, then when it is booted and assigned an IP by a DHCP server, the fully-qualified domain name host1.d1.comp.nus.edu.sg will be added to the Dynamic DNS and the name will point to the client's assigned IP address.

DNS tools – for self practice

- nslookup
  - `$ nslookup www.comp.nus.edu.sg`
  - `$ nslookup www.comp.nus.edu.sg ns1.comp.nus.edu.sg`
- host
  - `$ host www.comp.nus.edu.sg`
  - `$ host -t ns comp.nus.edu.sg`
  - `$ host -t mx comp.nus.edu.sg ns1.comp.nus.edu.sg`
  - `$ man host`
- dig
  - `$ dig www.comp.nus.edu.sg`
  - `$ dig comp.nus.edu.sg ns`
  - `$ dig @ns1.comp.nus.edu.sg nus.edu.sg mx`
  - `$ man dig`
- whois
  - `$ whois google.com`
  - `$ whois comp.nus.edu.sg`

Python/C library

gethostbyname(name)

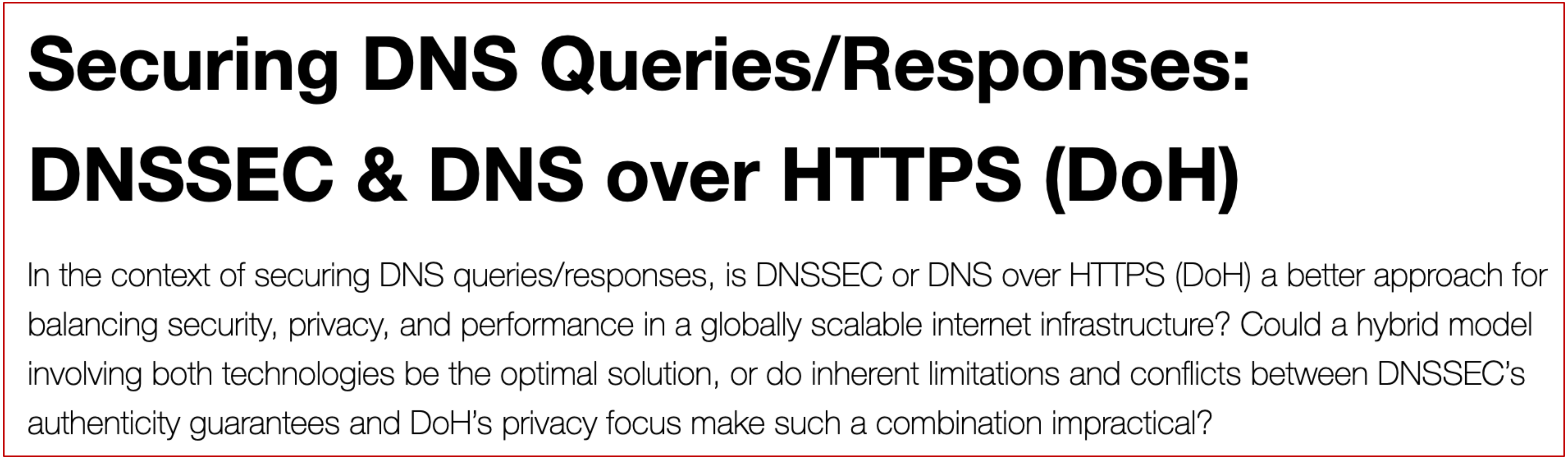
gethostbyaddr(IP)

*python calls underlying UNIX C API

https://docs.python.org/3/library/socket.html

Advanced Learners – <Active Learning in Discord>

- Topic for the Week



Securing DNS Queries/Responses: DNSSEC & DNS over HTTPS (DoH)

In the context of securing DNS queries/responses, is DNSSEC or DNS over HTTPS (DoH) a better approach for balancing security, privacy, and performance in a globally scalable internet infrastructure? Could a hybrid model involving both technologies be the optimal solution, or do inherent limitations and conflicts between DNSSEC's authenticity guarantees and DoH's privacy focus make such a combination impractical?

THE END

- **Assignment 2 due : 13 Sep**
- **Lab3: DCHP and VLAN**
- **Lab3: Pre-Lab QUIZ**
  - **Released on Monday 6pm**
  - **Due tomorrow 10am**

- **Programming Assignment Samples [examples]:**

a) Write a HTTP server program which returns the client's public IP and public port number when the default page is requested.

b) Traceroute tool using TCP-SYN segments and ICMP

Attendance

https://inetapps.nus.edu.sg/ctr/