DNS: Domain Name System

People: many identifiers:

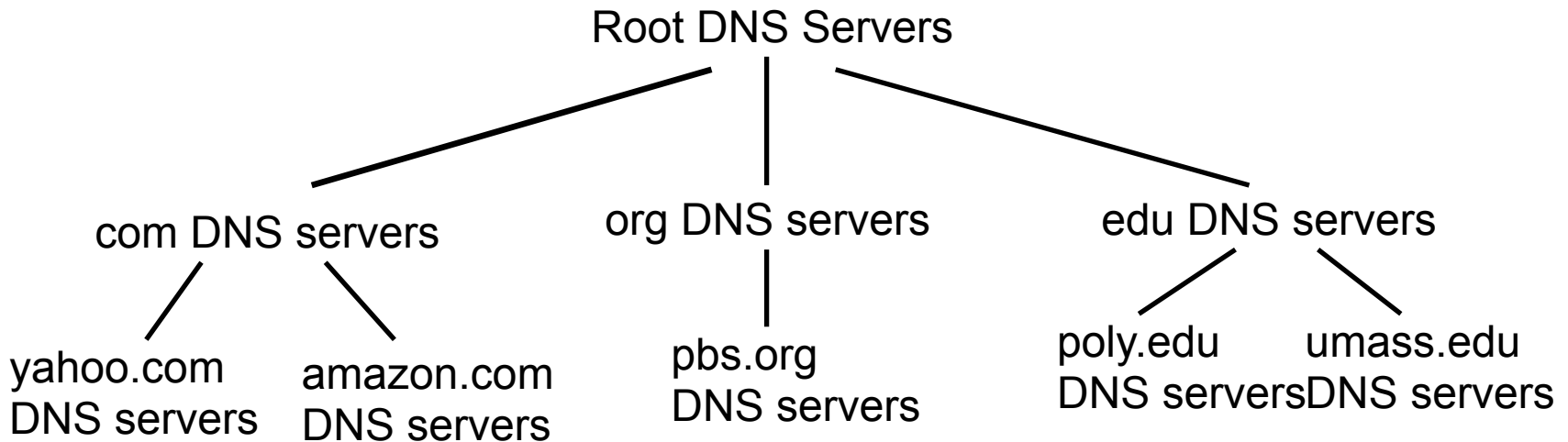- ❖ SSN, name, passport #

Internet hosts, routers:

- ❖ IP address (32 bit) - used for addressing datagrams
- ❖ "name", e.g., ww.yahoo.com - used by humans

Q: map between IP addresses and name ?

Domain Name System:

- ❐ distributed database implemented in hierarchy of many name servers
- ❐ application-layer protocol host, routers, name servers to communicate to resolve names (address/name translation)
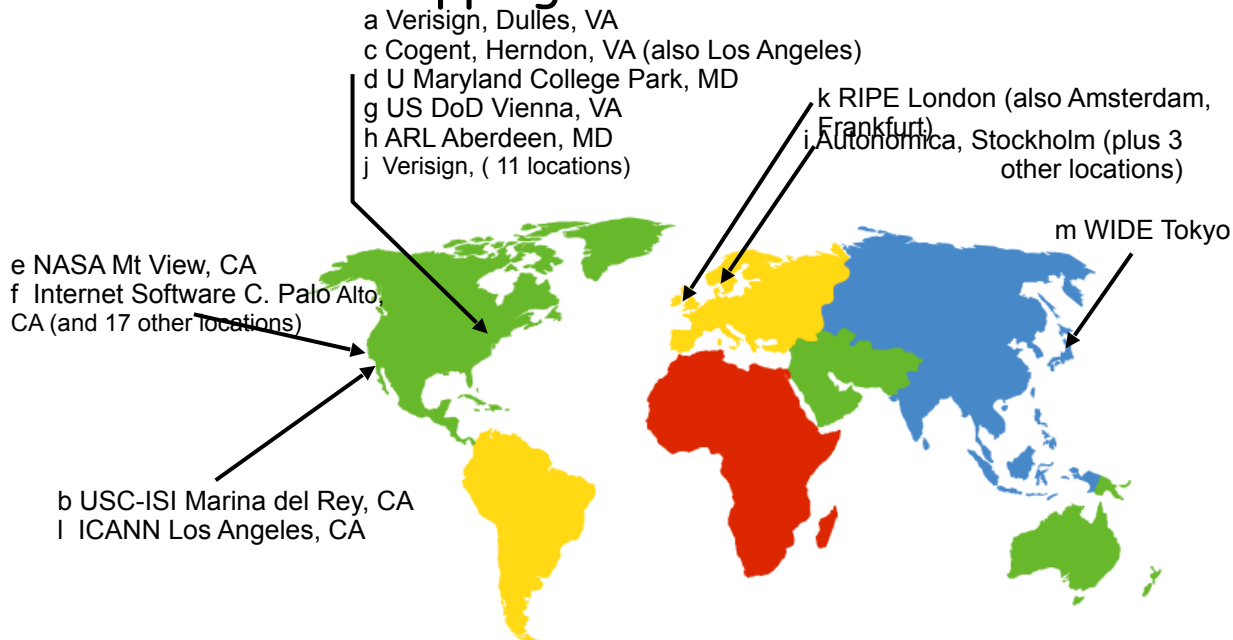
Distributed, Hierarchical Database

Root DNS Servers

com DNS servers   org DNS servers   edu DNS servers

yahoo.com
DNS servers   amazon.com
DNS servers   pbs.org
DNS servers   poly.edu
DNS servers   umass.edu
DNS servers

Client wants IP for www.amazon.com; 1st approx:

☐ 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

DNS: Root name servers

□ contacted by local name server that can not resolve name

□ root name server:

 ❖ contacts authoritative name server if name mapping not known

 ❖ gets mapping

 ❖ returns mapping to local name server

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

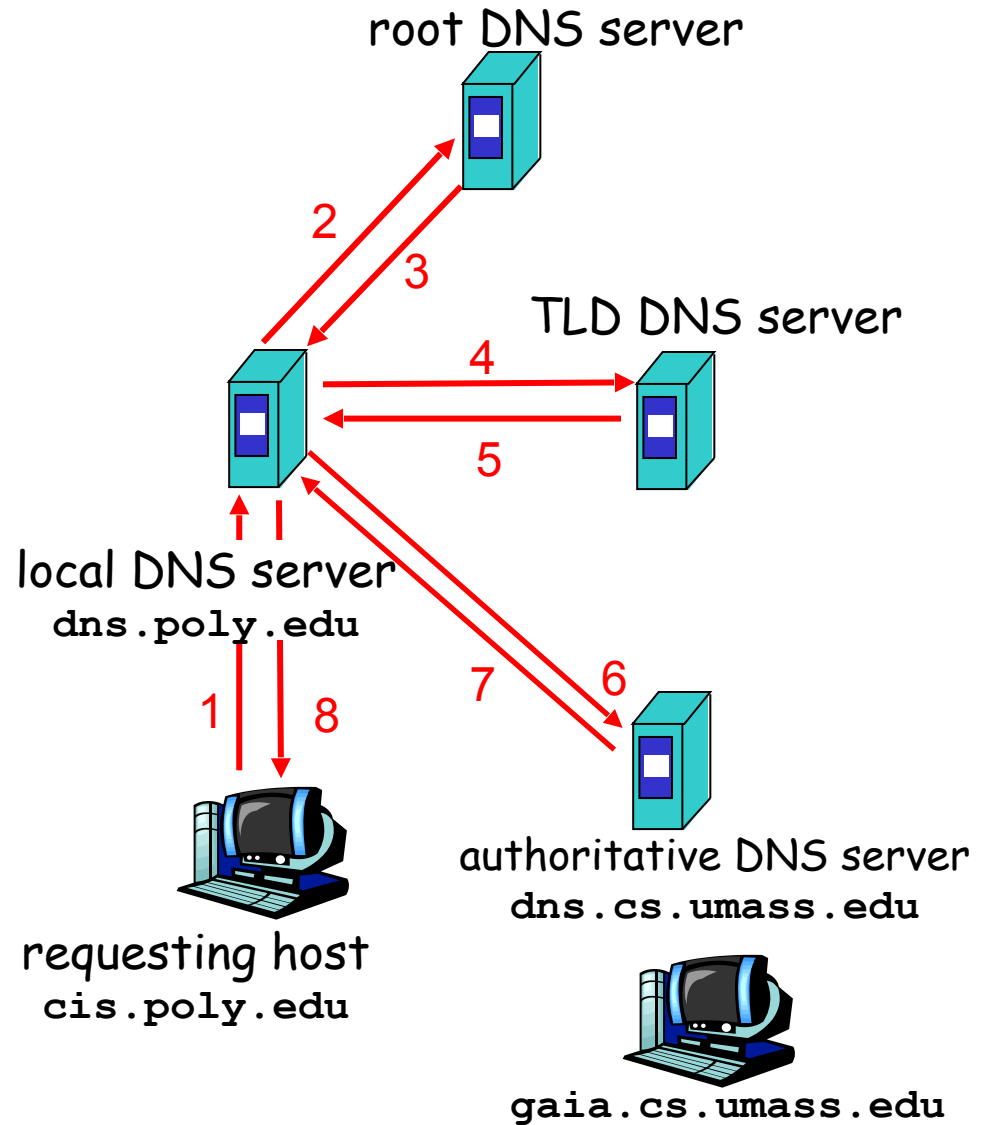13 root name servers worldwide

TLD and Authoritative Servers

□ Top-level domain (TLD) servers: responsible for com, org, net, edu, etc, and all top-level country domains uk, fr, ca, jp.

  ❖ Network solutions maintains servers for com TLD
  ❖ Educause for edu TLD

□ Authoritative DNS servers: organization's DNS servers, providing authoritative hostname to IP mappings for organization's servers (e.g., Web and mail).

  ❖ Can be maintained by organization or service provider

Local Name Server

❒ Does not strictly belong to hierarchy

❒ Each ISP (residential ISP, company, university) has one.

❖ Also called "default name server"

❒ When a host makes a DNS query, query is sent to its local DNS server

❖ Acts as a proxy, forwards query into hierarchy.

Example

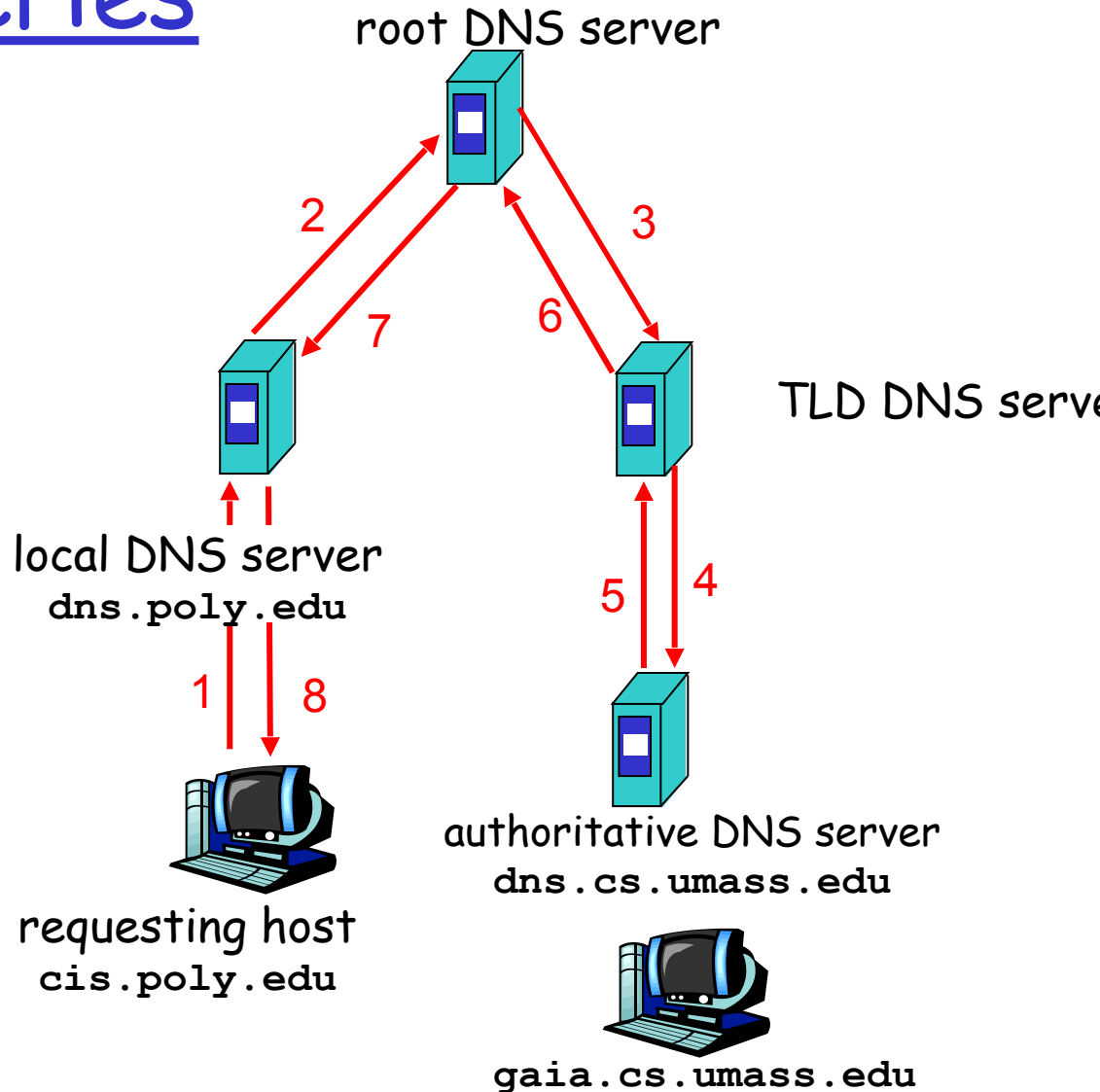□ Host at cis.poly.edu wants IP address for gaia.cs.umass.edu

root DNS server

2

3

TLD DNS server

4

5

local DNS server
dns.poly.edu

1   8

7   6

requesting host
cis.poly.edu

authoritative DNS server
dns.cs.umass.edu

gaia.cs.umass.edu

Recursive queries

recursive query:

- puts burden of name resolution on contacted name server
- heavy load?

iterated query:

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

root DNS server

2   3

7   6

local DNS server
dns.poly.edu

TLD DNS server

5   4

1   8

requesting host
cis.poly.edu

authoritative DNS server
dns.cs.umass.edu

gaia.cs.umass.edu

DNS: caching and updating records

- once (any) name server learns mapping, it caches mapping
  - cache entries timeout (disappear) after some time
  - TLD servers typically cached in local name servers
    - Thus root name servers not often visited
- update/notify mechanisms under design by IETF
  - RFC 2136
  - http://www.ietf.org/html.charters/dnsind-charter.html

DNS 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
- ❖ **name** is domain (e.g. foo.com)
- ❖ **value** is hostname of authoritative name server for this domain

❐ Type=CNAME
- ❖ **name** is alias name for some "canonical" (the real) name
  `www.ibm.com` is really `servereast.backup2.ibm.com`
- ❖ **value** is canonical name

❐ Type=MX
- ❖ **value** is name of mailserver associated with **name**

DNS protocol, messages

DNS protocol : query and reply messages, both with same message format

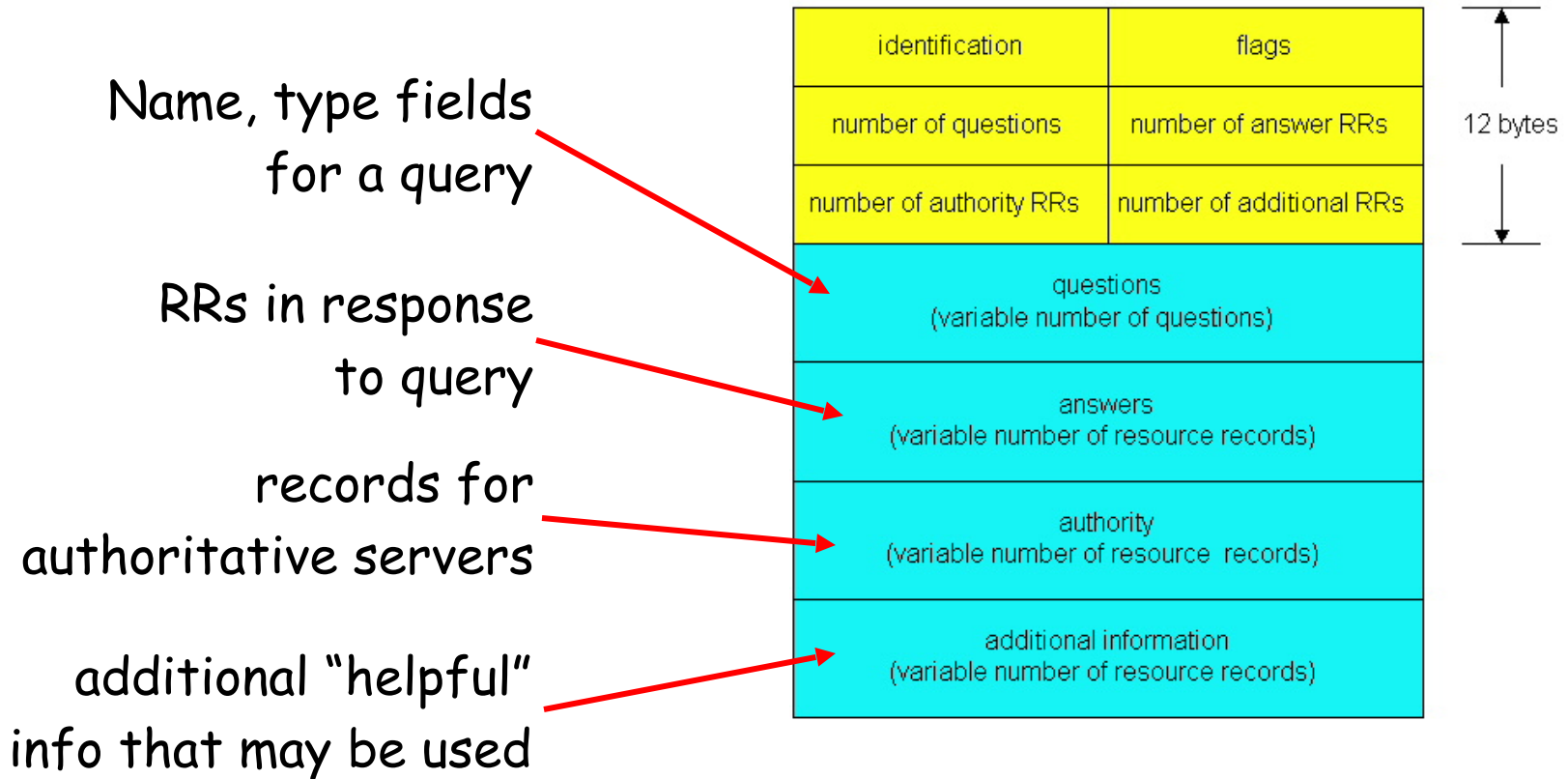## msg header

- identification: 16 bit # for query, reply to query uses same #
- flags:
  - query or reply
  - recursion desired
  - recursion available
  - reply is authoritative

identification	flags
number of questions	number of answer RRs
number of authority RRs	number of additional RRs

12 bytes

questions
(variable number of questions)

answers
(variable number of resource records)

authority
(variable number of resource records)

additional information
(variable number of resource records)

DNS protocol, messages

Name, type fields
for a query

RRs in response
to query

records for
authoritative servers

additional "helpful"
info that may be used

identification	flags
number of questions	number of answer RRs
number of authority RRs	number of additional RRs

12 bytes

questions
(variable number of questions)

answers
(variable number of resource records)

authority
(variable number of resource records)

additional information
(variable number of resource records)

Inserting records into DNS

- Example: just created startup "Network Utopia"
- Register name networkuptopia.com at a registrar (e.g., Network Solutions)
  - ❖ Need to provide registrar with names and IP addresses of your authoritative name server (primary and secondary)
  - ❖ Registrar inserts two RRs into the com TLD server:

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

- Put in authoritative server Type A record for www.networkuptopia.com and Type MX record for networkutopia.com
- How do people get the IP address of your Web site?