DNS –
Domain Name system

Application layer

- DNS Le port DNS (Domain Name System)

- Port 53 en UDP :Utilisé pour la résolution de noms classique, comme lorsqu'un client demande l'adresse IP d'un nom de domaine (ex: google.com).C'est le plus courant pour les requêtes simples.

- Port 53 en TCP :Utilisé pour les transferts de zone DNS (zone transfers entre serveurs DNS).
  - Aussi utilisé lorsque la réponse dépasse 512 octets (dans certaines situations ou avec DNSSEC par exemple).

DNS: Domain Name System

people: many identifiers:

- SSN, name, passport #

Internet hosts, routers:

- IP address (32 bit) - used for addressing datagrams
- “name”, e.g., www.yahoo.com - used by humans

Q: map between IP address and name, and vice versa ?

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)
  - note: core Internet function, implemented as application-layer protocol
  - complexity at network’s “edge”

DNS

DNS services

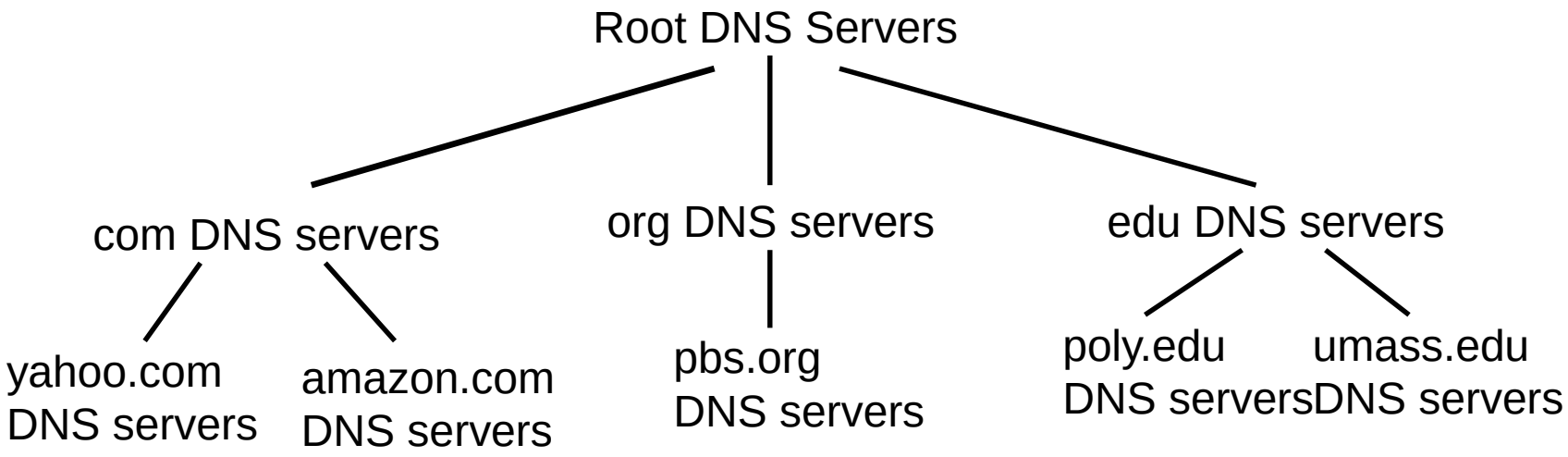
- hostname to IP address translation
- host aliasing
  - Canonical, alias names
- mail server aliasing
- load distribution
  - replicated Web servers: set of IP addresses for one canonical name

Why not centralize DNS?

- single point of failure
- traffic volume
- distant centralized database
- maintenance

doesn't *scale!*

Distributed, Hierarchical Database

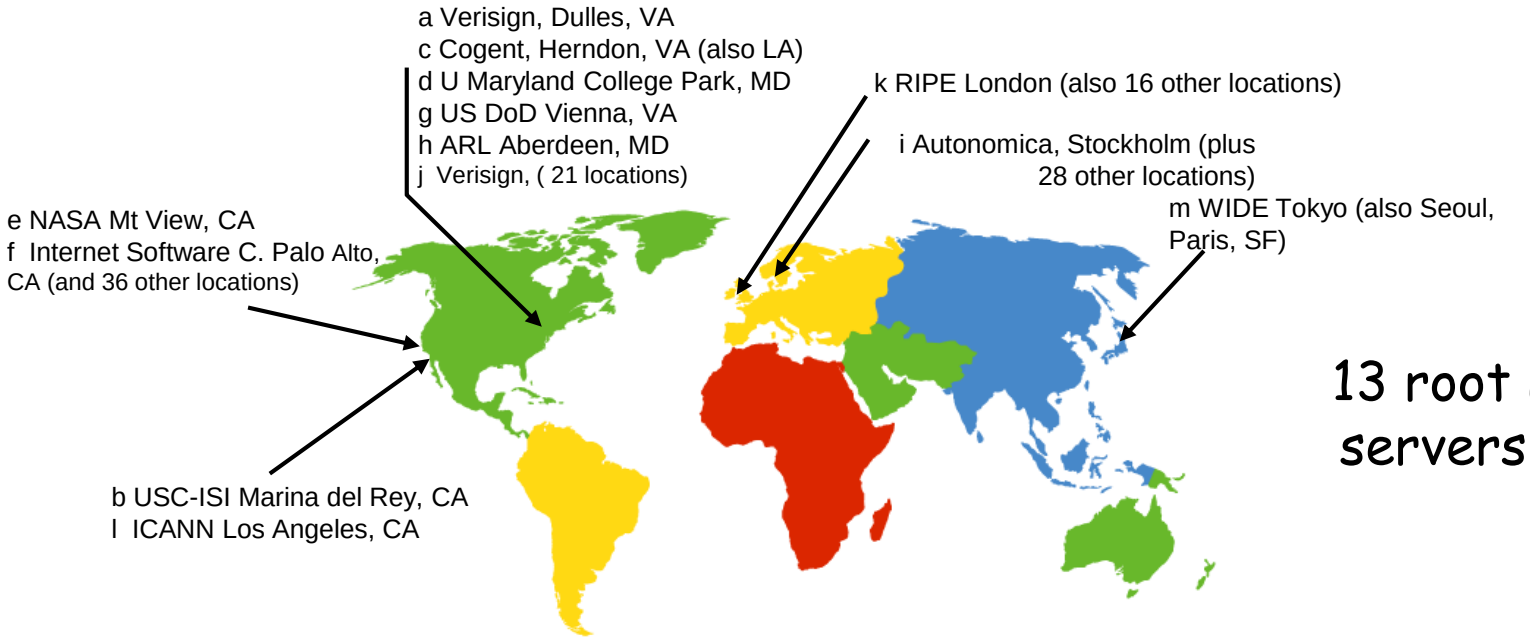


client wants IP for www.amazon.com; 1st approx:

- 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



13 root name servers worldwide

Google’s public DNS server

- Accessible at the IPv4 addresses - 8.8.8.8 and 8.8.4.4
- IPv6 addresses-2001:4860:4860::8888 and 2001:4860:4860::8844
- Services a total of 80 Billion name resolution requests per day!!!(stat obtained from Google’s official blog dated 2012) - around 1,000,000 requests per second!!!
- Works hand in hand with the IETF
- Today, about 70 percent of its traffic comes from outside the U.S. with strong presence in North America, South America and Europe, and Asia.
- Other such public DNS providers – OpenDNS .

TLD and Authoritative Servers

Top-level domain (TLD) servers:

- Domain Name consists of one or more parts called Labels .
- Right most label conveys the Top level domain and each label to the left specifies a sub division or sub domain to the label on the right.
- Domain names include 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

Authoritative DNS servers:

- An Authoritative only server returns answers only to queries about domain names that have been specifically configured by the administrator.
- An organization's DNS servers, providing authoritative hostname to IP mappings for organization's servers (e.g., Web, mail).
- It can be maintained by organization or service provider

Local Name Server

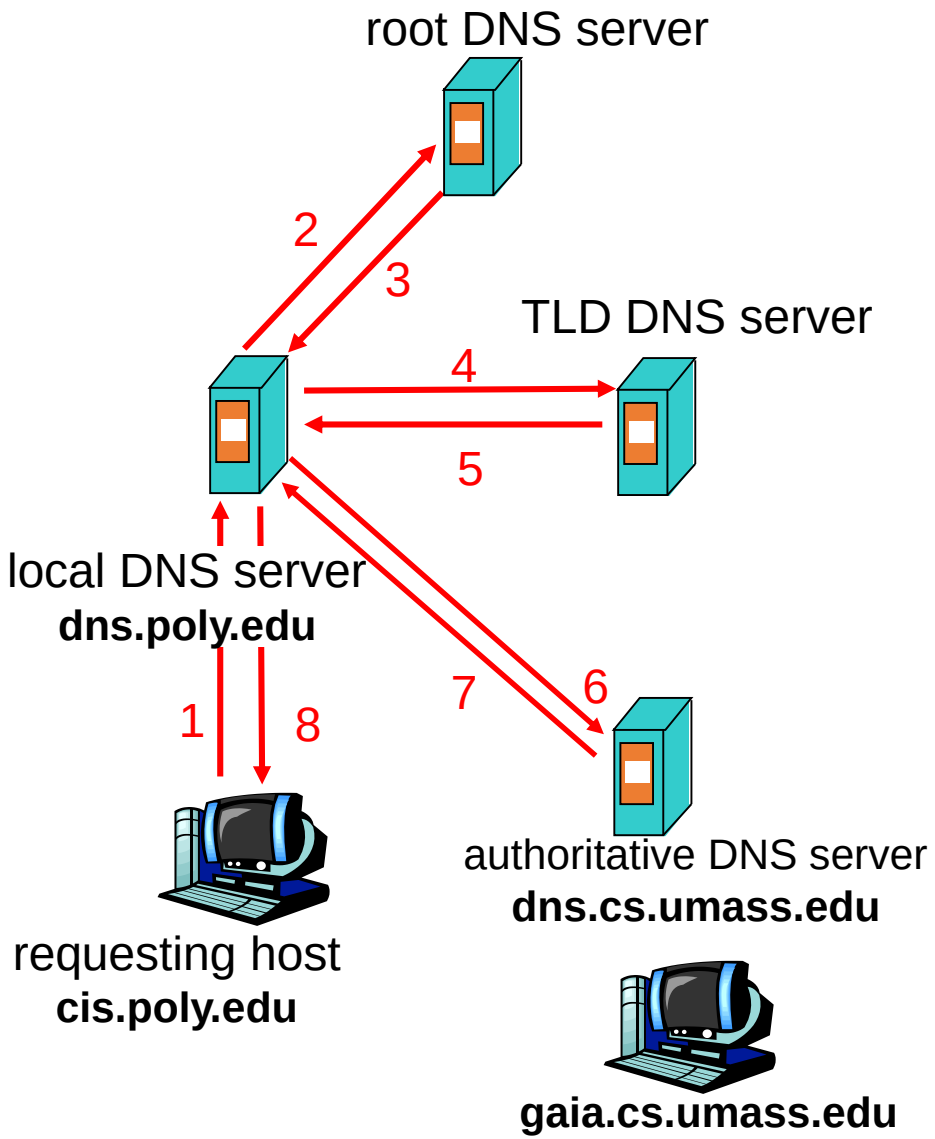
- Local Name Servers do not strictly belong to hierarchy
- Every ISP (residential ISP, company, university) has a local server also called “default name server”
- When a host makes a DNS query, query is sent to its local DNS server which acts as proxy, forwards query into hierarchy.
- These local networks implement cache resolvers to improve the efficiency.

DNS name resolution example

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

Iterated query:

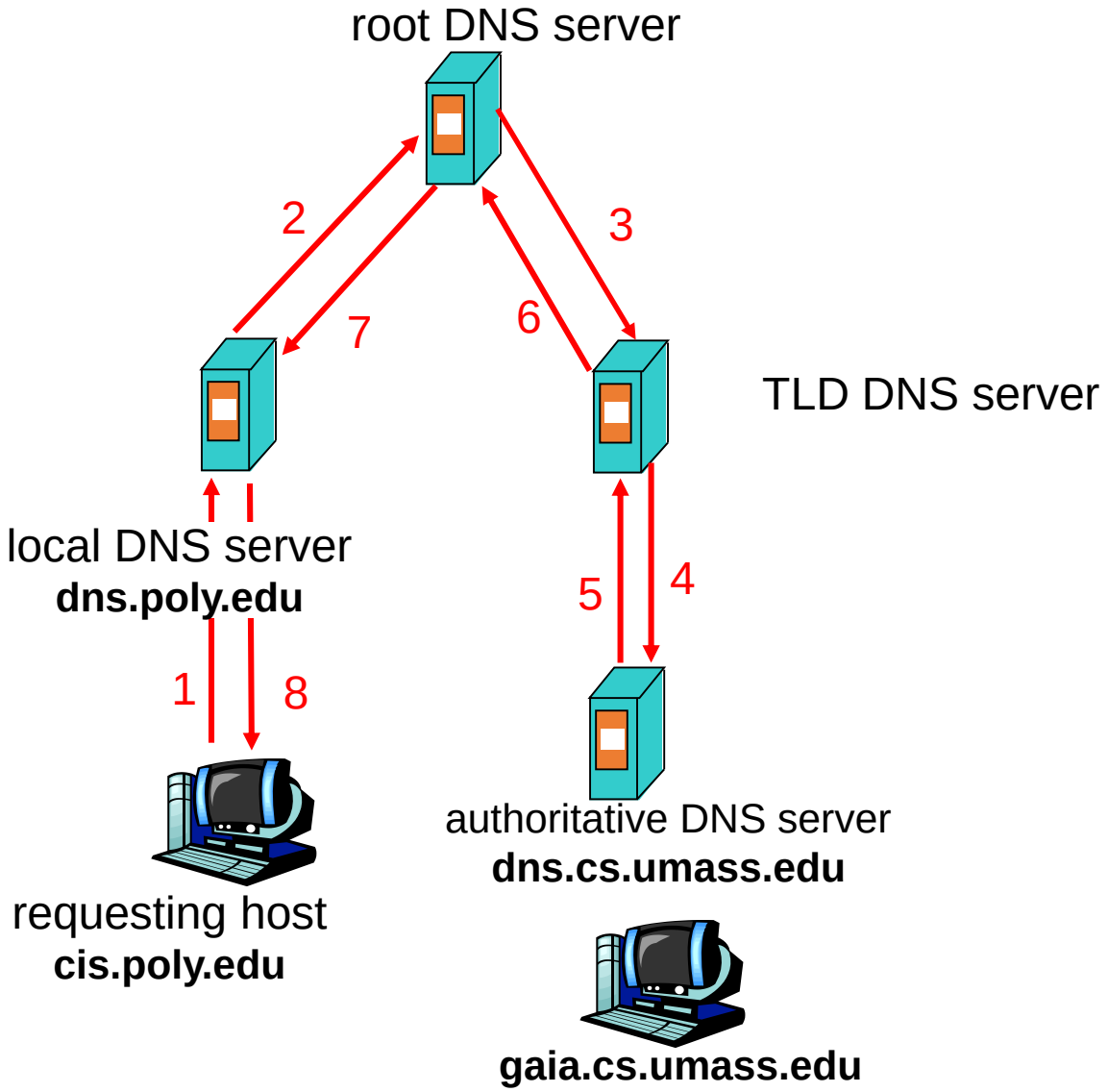
- Contacted server replies with name of server to contact
- "I don't know this name, but ask this server"



DNS name resolution example

Recursive query:

- It resolves any query that it receives even if they are not authoritative for the question being asked , by consulting server or servers that are authoritative for the question
- If a name server cannot answer a query because it does not contain an entry for the host in its database, it may recursively query name servers higher up in the hierarchy. This is known as a recursive query or recursive lookup.



DNS: Updating records and Caching

- An Authoritative name server can be either primary or secondary.
- Primary servers store the definitive versions of the record in that zone and the secondary server maintains an identical copy of the primary server's database
- The update/notify mechanisms proposed IETF standard

  RFC 2136 known as Dynamic DNS .
- Caching :
- 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 and improves efficiency.

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

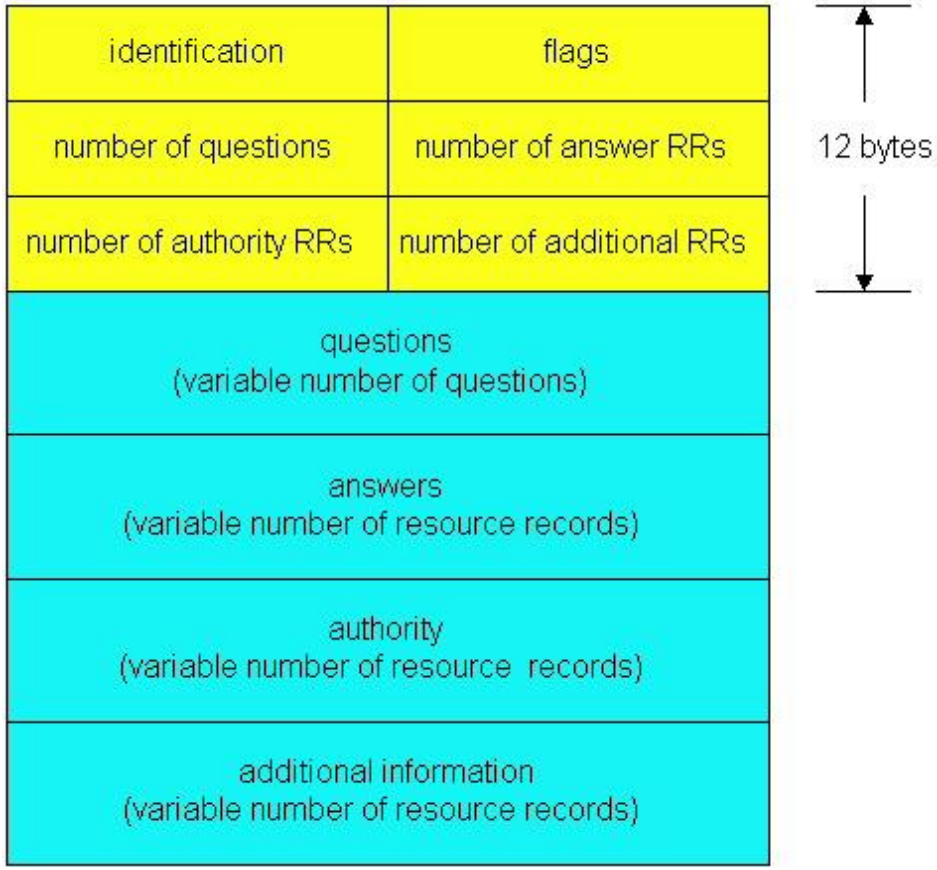
- **value** is name of mail server associated with **name**

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



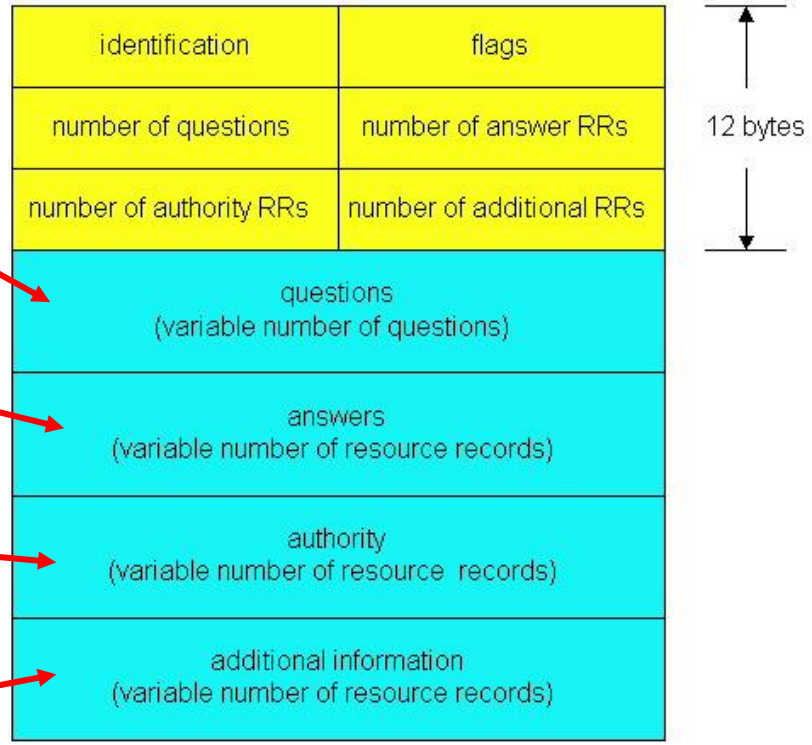
DNS protocol, messages

Name, type fields for a query

RRs in response to query

records for authoritative servers

additional "helpful" info that may be used



Inserting records into DNS

- example: new startup “Network dz”
- register name networkdz.com at *DNS registrar* (e.g., Network Solutions)
  - provide names, IP addresses of authoritative name server (primary and secondary)
  - registrar inserts two RRs into com TLD server:

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

- create authoritative server Type A record for www.networkuptopia.com; Type MX record for networkdz.com
- How do people get IP address of your Web site?