Domain Name System (or Service) (DNS)

Computer Networks

A15

DNS Outline

- Infrastructure Services
- DNS Hierarchical Structure
- Root Name Servers
- Top-Level Domain Servers
- Authoritative Name Servers
- Local Name Server
- Caching and Updating DNS Records
- DNS Protocols and Messages

Infrastructure Services

- There are protocols *essential* for the Internet to run smoothly that do not fit neatly into the strictly layered model.
- Two of these infrastructure services, a name service and network management are provided by DNS and SNMP (Simple Network Management Protocol) respectively.
- name server :: an implementation of a resolution mechanism available on a network and queried via a message.

Name Service Terminology

name space :: defines the set of possible names.

- A name space can be either flat (names are not divisible into components), or it can be hierarchical (Unix file names are an obvious example).

naming system :: maintains a collection of bindings of names to values.

- The value can be anything we want the naming system to return when presented with a name; in many cases it is an address.

resolution mechanism :: a procedure that returns the corresponding value when invoked with a name.

Name Service email Example

- Name Service (DNS)

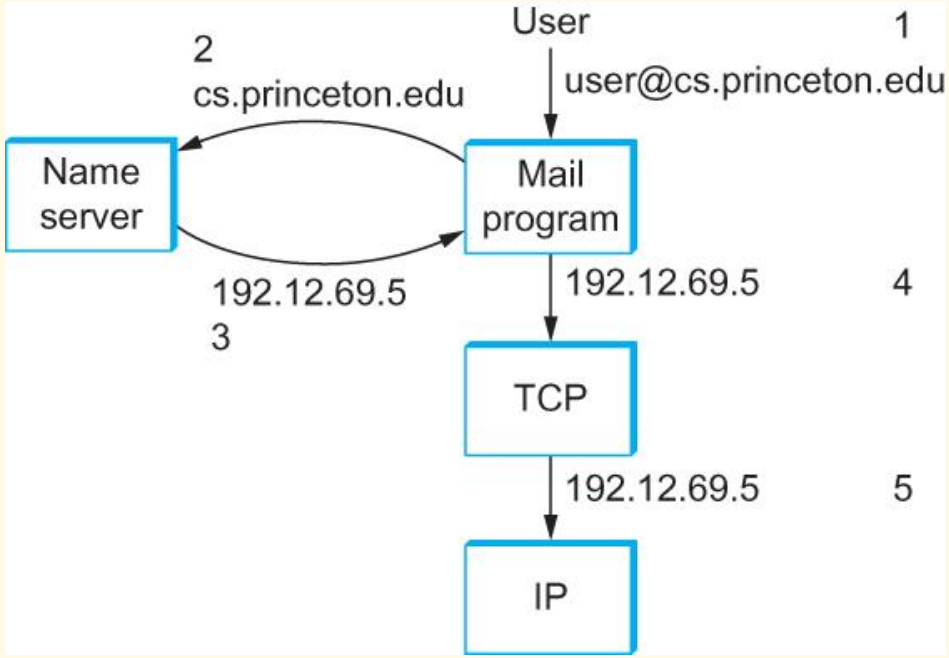


Figure 9.14 Names translated into addresses, where the numbers 1–5 show the sequence of steps in the process.

DNS: Domain Name System

People: many identifiers:

- SSN, name, passport #

Internet hosts, routers:

- IPv4 address (32 bit) - used for addressing datagrams.
- "name", e.g., `www.cnn.com` - used by humans.

Q: map between IP addresses and name?

Domain Name System::

1. distributed database implemented in hierarchy of many DNS name servers.
2. application-layer protocol that enables hosts, routers, name servers to communicate to resolve names (address/name translation).
   - note: This core Internet function, implemented as application-layer protocol.
   - complexity is at network's "edge".

K&R

DNS Details

- DNS servers often run on Unix machines running BIND (Berkeley Internet Name Domain software).
- DNS runs over UDP.
- Uses port 53.
- DNS is commonly employed by other application layer protocols (HTTP, SMTP and FTP) to determine IP addresses.

DNS Design

DNS provides four services:

1. hostname to IP address translation
2. host aliasing
   - Aliases, where canonical name is "real" name
3. mail server aliasing
4. load distribution
   - replicated Web servers: set of IP addresses for one host name.

Why not centralize DNS?

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

→ doesn't *scale!*

- DNS is distributed by design!

K&R

Distributed Domain Hierarchy

- DNS implements a hierarchical name space for Internet objects.
  - Unlike Unix file names, DNS names are processed from right to left and use periods as the separator.
  - Like Unix files, the DNS hierarchy is a tree abstraction (i.e., each node in the tree corresponds to a domain and the leaves correspond to the hosts being named).

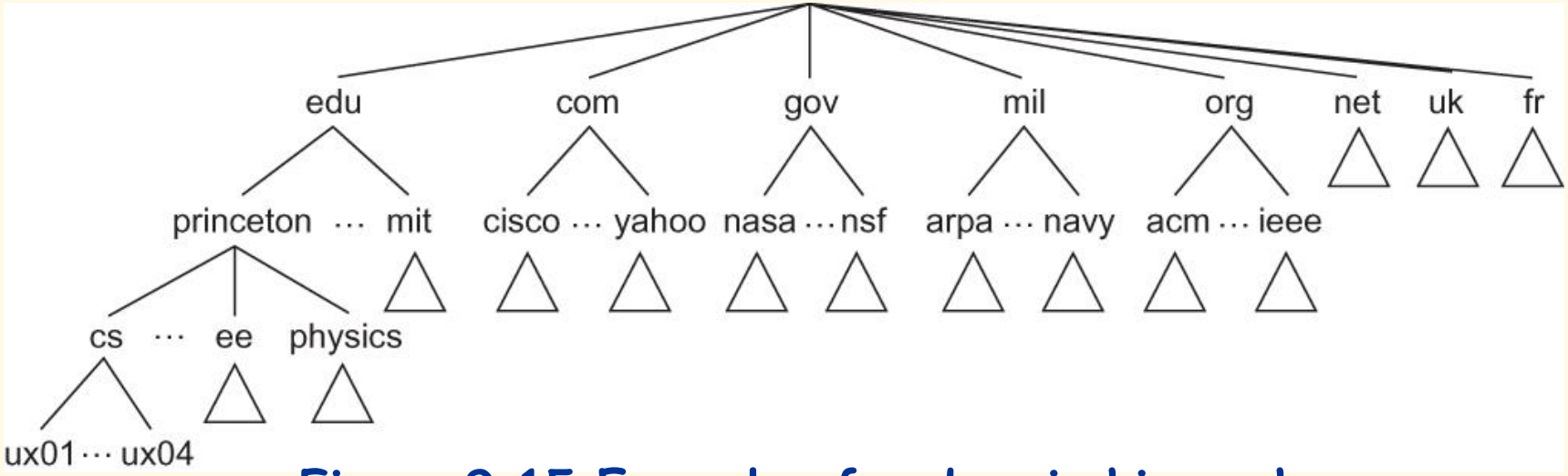
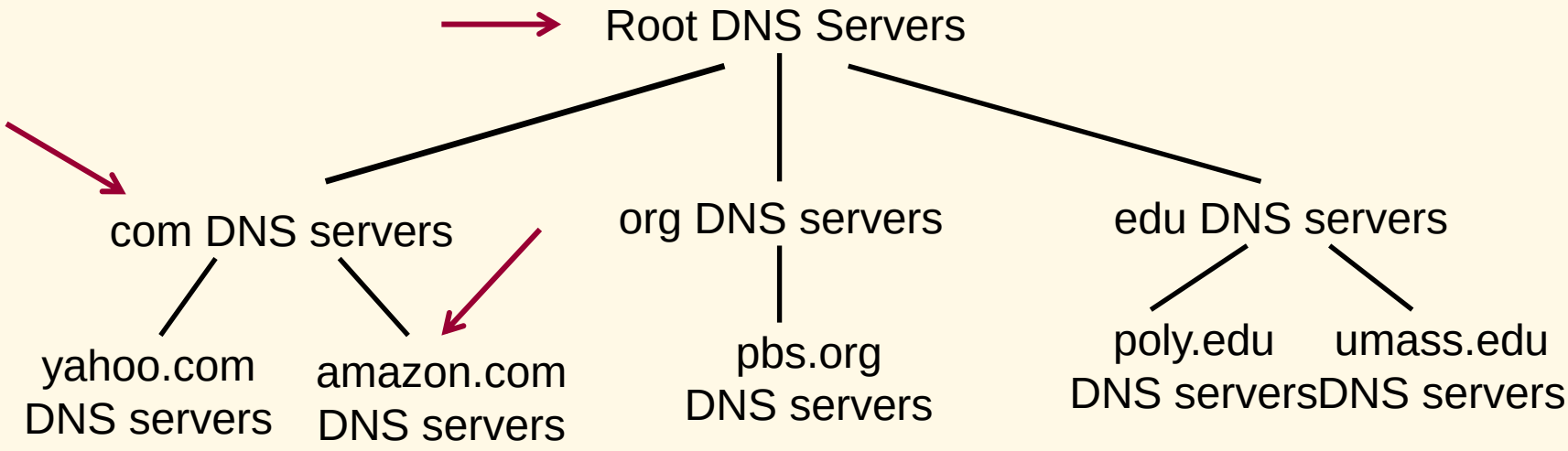


Figure 9.15 Example of a domain hierarchy

DNS Server Classes

- Three classes of servers (approximation):
  - Root DNS servers
  - Top-level domain (TLD) servers
  - Authoritative DNS servers
- Additionally, the resolution includes
  - Local name servers

Distributed, Hierarchical Database

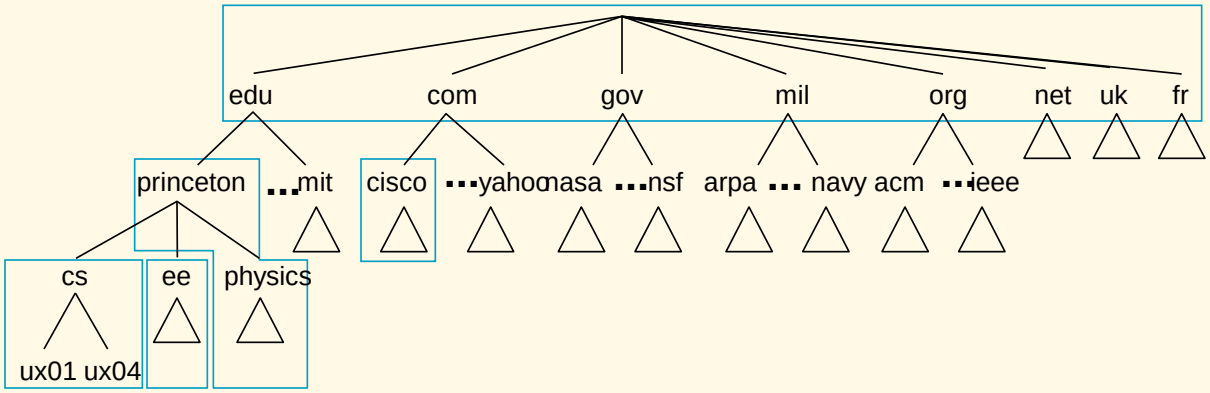


Example: Client wants IP for `www.amazon.com` {1st approx}

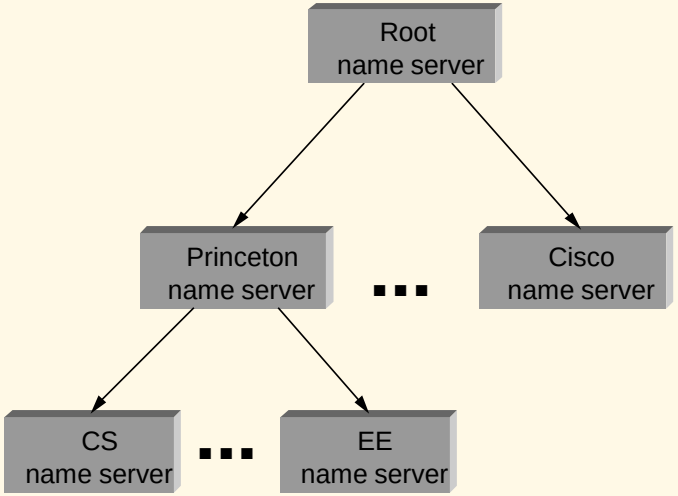
- client queries a root server to find `.com` DNS server
- client queries `.com` DNS server to get `amazon.com` DNS server
- client queries `amazon.com` DNS server to get IP address for `www.amazon.com`

Name Servers

- Partition hierarchy into *zones*



- Each zone implemented by two or more *name servers*.
- Each zone corresponds to some administrative authority that is responsible for that portion of the hierarchy.



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 (a-m) in 2012

K&R

Top-Level Domain (TLD)

- Top-level domain (TLD) servers:
  - Responsible for `com`, `org`, `net`, `edu`, etc, and all top-level country domains such as `uk`, `fr`, `ca` and `jp`.
  - Verisign Global Registry Services maintains servers for `com` and `net` TLD.
  - Educause for `edu` TLD.

Authoritative Servers

Authoritative DNS servers:

- Organization's DNS servers, providing authoritative hostname to IP mappings for organization's servers (e.g., Web, mail).

- Can be maintained by organization or service provider.

Local Name Server

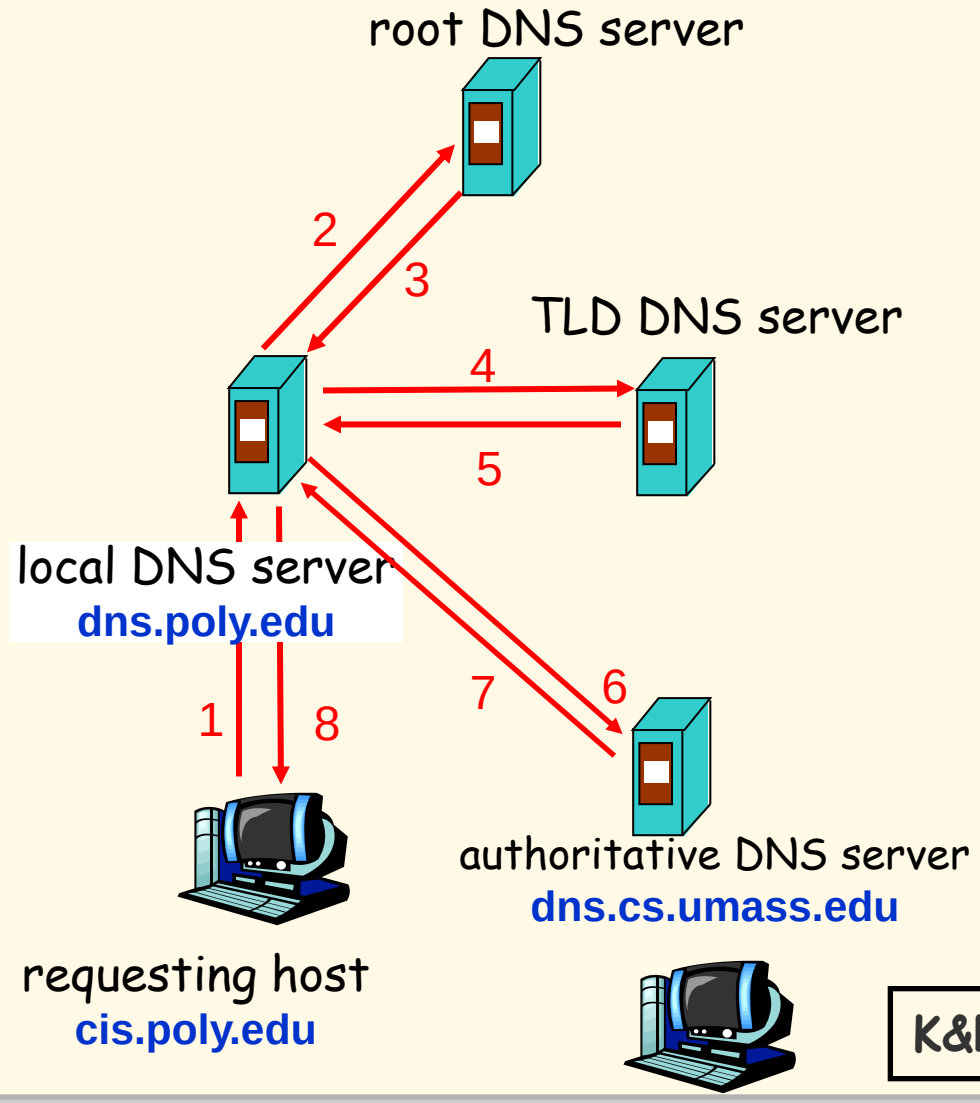
- Does not strictly belong to hierarchy.
- Each ISP (residential ISP, company, university) has one
  - Also called "default name server".
  - You can run one in your home/dorm!
- When a host makes a DNS query, the query is sent to its local DNS server.
  - ISP provides IP address of local DNS server using DHCP.
  - Acts as proxy, forwards query into the name server 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."



K&R

Name Resolution Example

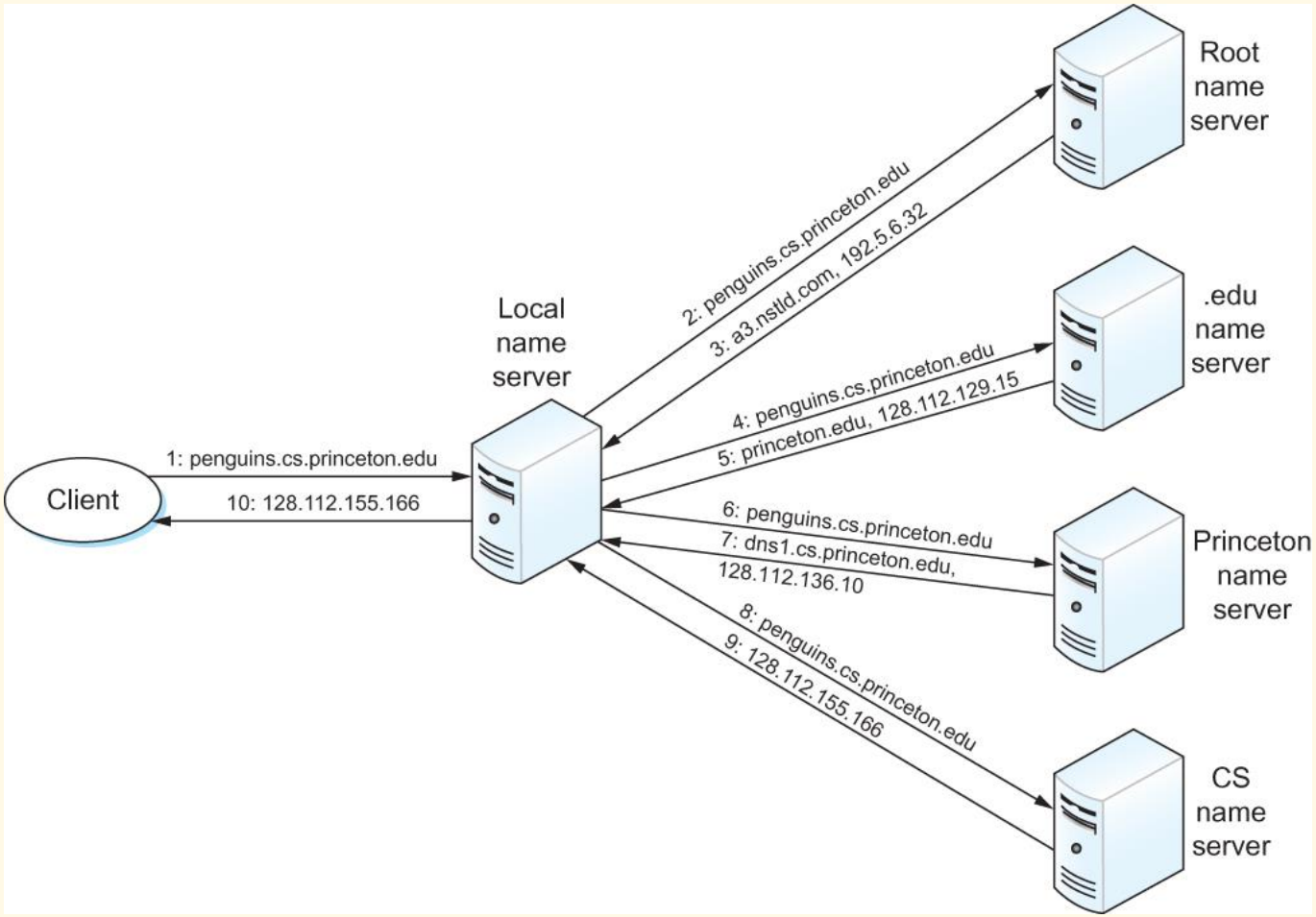
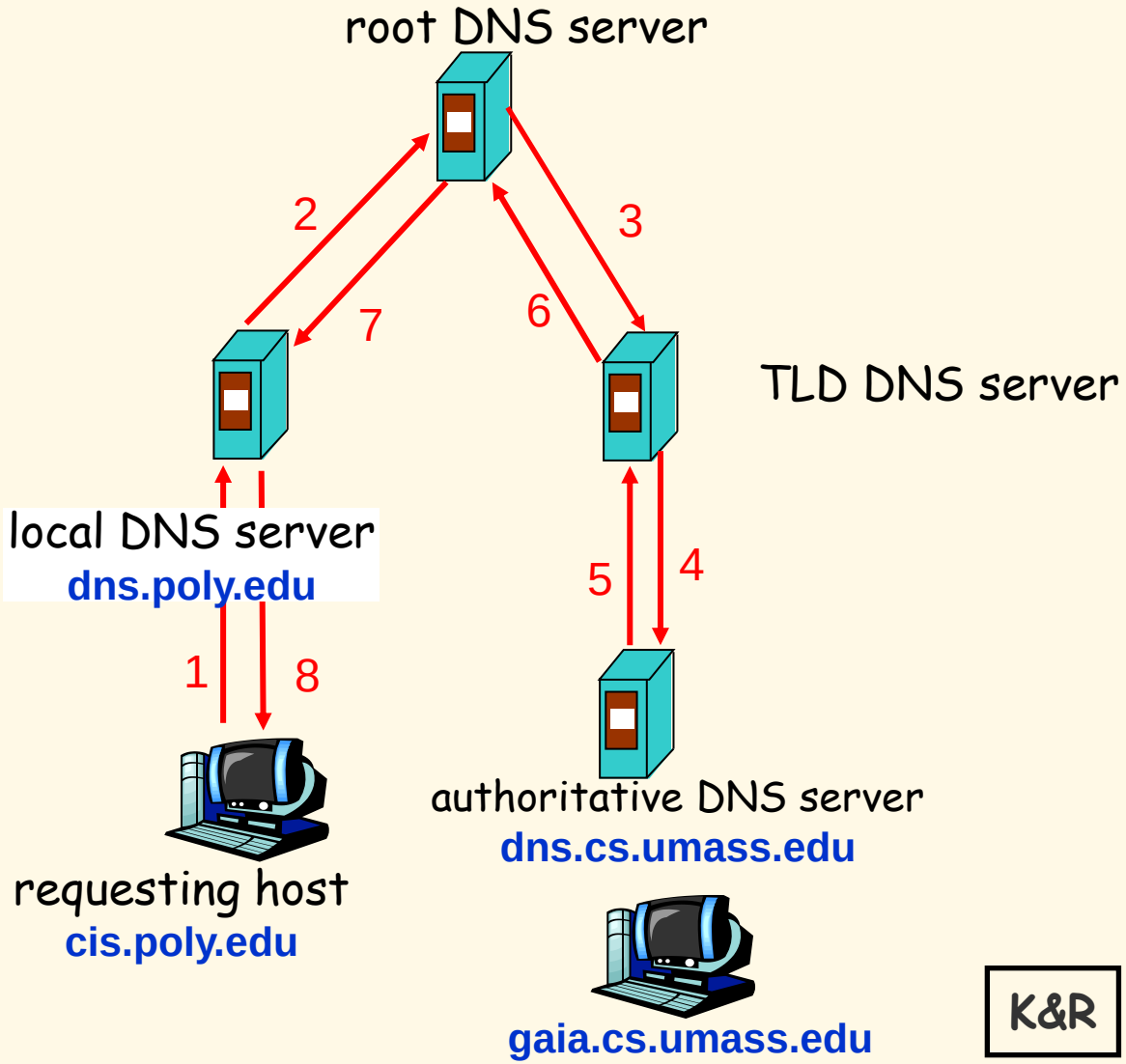


Figure 9.18 Name resolution in practice, where the numbers 1–10 show the sequence of steps in the process.

DNS Name Resolution (example)

Recursive query

- Puts burden of name resolution on contacted name server.
- Heavy load?



K&R

DNS: Caching and Updating Records

- Each name server implements the zone information as a collection of *resource records*.
- Once (any) name server learns mapping, it *caches* mapping.
  - Cache entries timeout (disappear) after some time (e.g two days) {specified as TTL ==Time-To-Live}.
  - IP addresses of TLD servers are typically cached in local name servers.
    - Thus root name servers are not visited frequently.
- Originally thought DNS names quite static, but increasingly not so → update/notify mechanisms under design by IETF.
  - RFC 2136: http://www.ietf.org/rfc/rfc2136.txt

DNS Resource Records

DNS: distributed database 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**

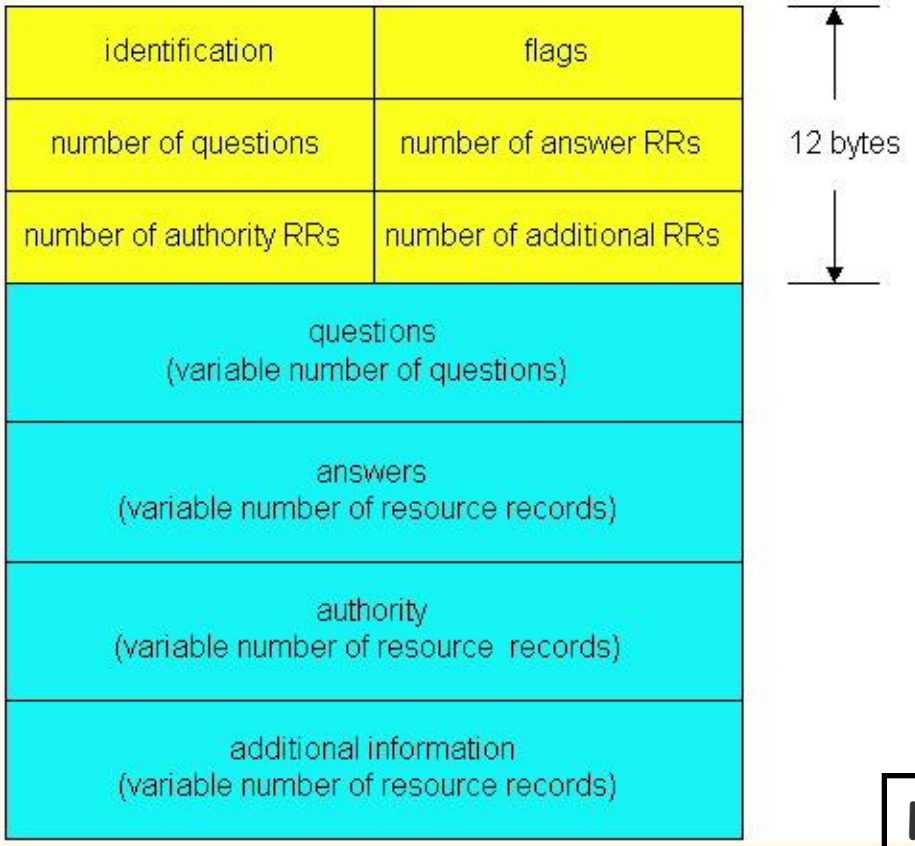
K&R

DNS Protocol and Messages

DNS protocol: *query* and *reply* messages, both with the 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



K&R

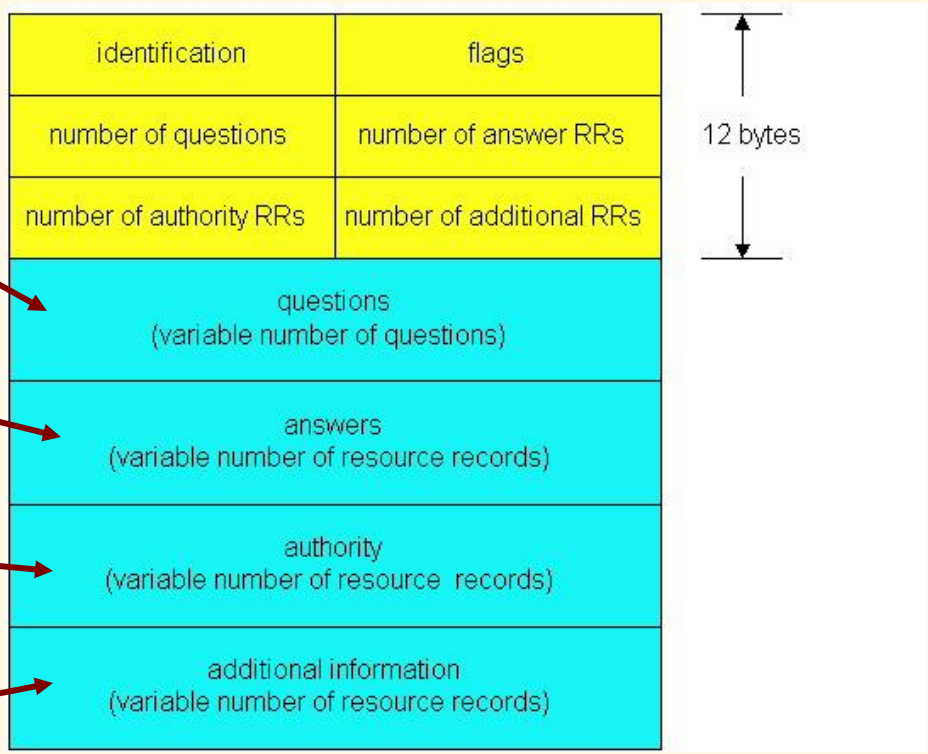
DNS Protocol and Messages

Name, type fields for a query

Resource records in response to query

Records for authoritative servers

Additional "helpful" info that may be used



K&R

Inserting records into DNS

- Example: new startup "Network Utopia"
  - How do people get IP address of your Web site?
  - How do they send you email?

1. Register domain name `networkutopia.com` at DNS registrar (e.g., Verisign)
   - provide names, IP addresses of authoritative name server (primary and secondary).
   - registrar inserts two RRs per server into `.com` TLD server:

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

2. Create Type A record `www.networkuptopia.com` for web server and Type MX record for `mail.networkutopia.com` for mail server in authoritative DNS server.

K&R

DNS Summary

- DNS Hierarchial Structure
- Root Name Servers
- Top-Level Domain Servers
- Authoritative Name Servers
- Local Name Server
- Caching and Updating DNS Records
- DNS Protocols and Messages