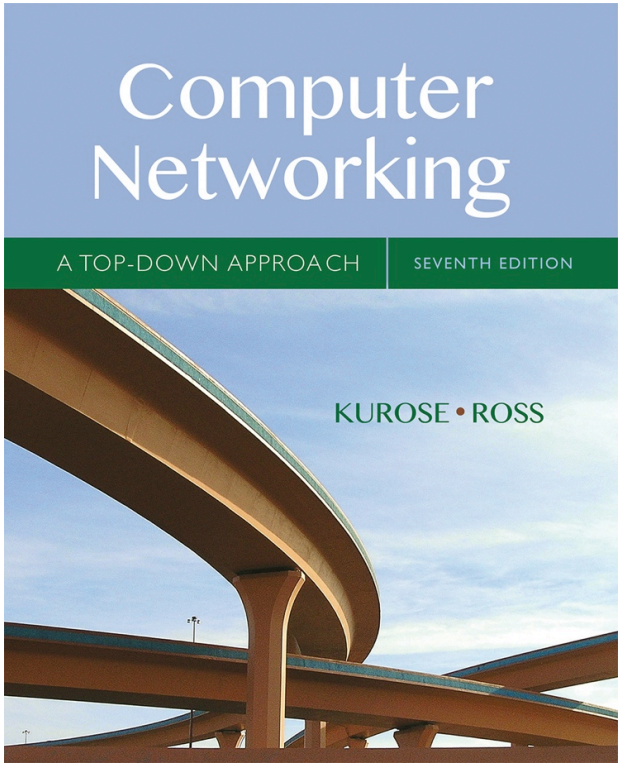
CN-Basic
L16

DNS

Dr. Ram P Rustagi
rprustagi@ksit.edu.in
http://www.rprustagi.com
https://www.youtube.com/rprustagi

Resources Acknowledgement

Chapter 2
Application Layer



Computer Networking: A Top Down Approach

7th edition
Jim Kurose, Keith Ross
Pearson/Addison Wesley
April 2016

A note on the use of these Powerpoint slides:

We're making these slides freely available to all (faculty, students, readers). They're in PowerPoint form so you see the animations; and can add, modify, and delete slides (including this one) and slide content to suit your needs. They obviously represent a *lot* of work on our part. In return for use, we only ask the following:

- If you use these slides (e.g., in a class) that you mention their source (after all, we'd like people to use our book!)
- If you post any slides on a www site, that you note that they are adapted from (or perhaps identical to) our slides, and note our copyright of this material.

Thanks and enjoy! JFK/KWR

Resources

- RFC 1034, 1035
- Dynamic DNS updates: RFC 2136, 3007
- https://danielmiessler.com/study/dns/
- DNS Inventor paper: Mockapetris%202005-Development%20of%20DNS.pdf
- https://www.icann.org/en/system/files/files/presentation-gdd-summit-dns-primer-11may17-en.pdf

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:* how to map between IP address and name, and vice versa ?
- Clients DNS Resolver
  - Unix: /etc/resolv.conf
  - `gethostbyname()`

- *Domain Name System:*
- *distributed database* implemented in hierarchy of many *name servers*
- *application-layer protocol:* hosts, name servers communicate to *resolve* names (address/name translation)
- note: core Internet function, implemented as application-layer protocol
- complexity at network's "edge"

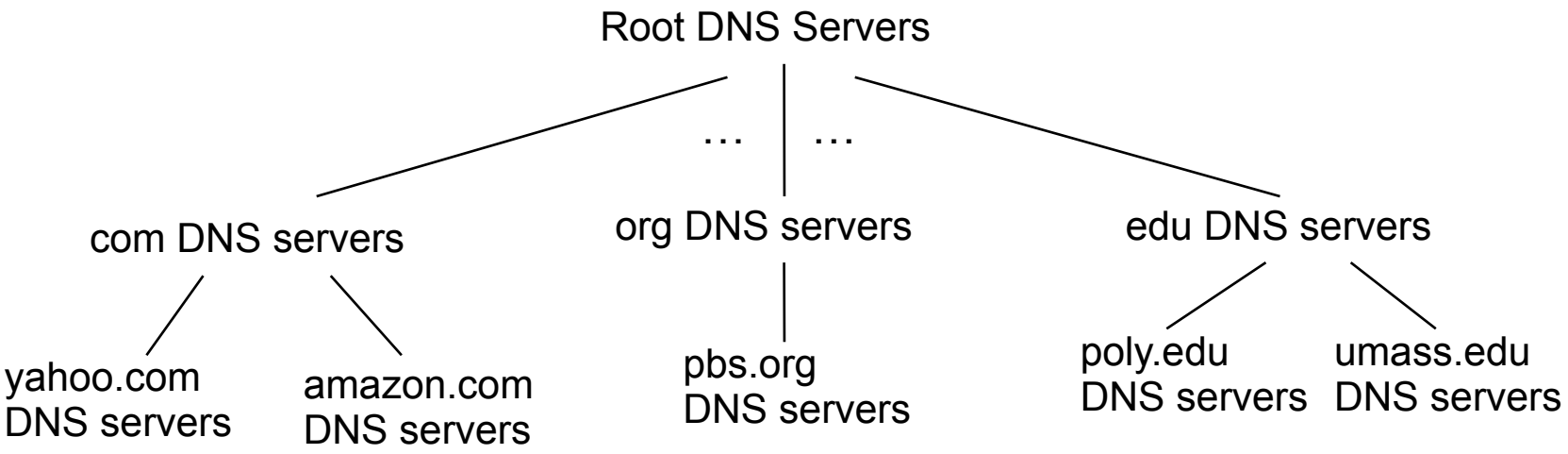
DNS: services, structure

- *why not centralize DNS?*
  - Single point of failure
  - Traffic volume
  - Distant centralized database
  - Update? , delete?
  - Maintenance

A: doesn't scale!

- *DNS services*
- Hostname to IP address translation
- Host aliasing
- Canonical, alias names
- Mail server aliasing
- Load distribution
- Replicated Web servers: many IP addresses correspond to one name, e.g. Google, Yahoo
- Different from other applications
  - End user does not use directly

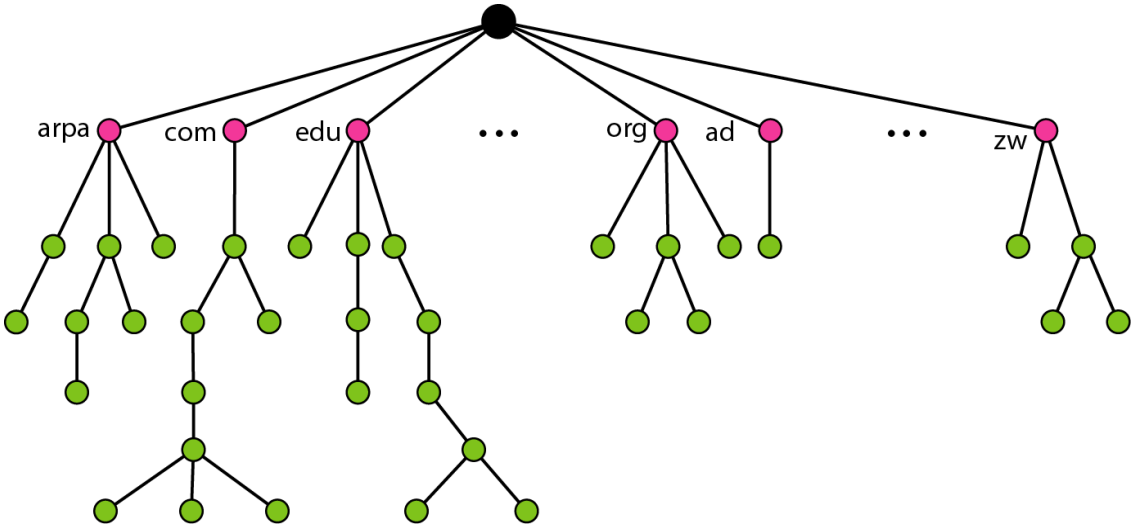
DNS: a distributed, hierarchical database



- *client wants IP for* `www.amazon.com`*; 1st approx:*
- client queries 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`

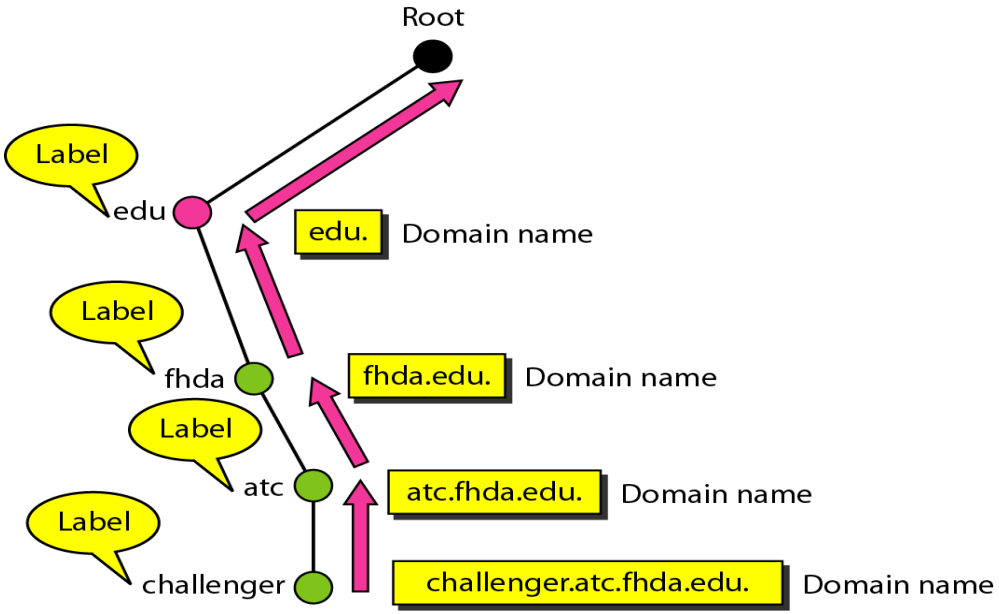
Domain Name Space

- Root (top) level domains
  http://www.iana.org/domains/root/db/



DNS and Labels

- Different from unix file path which starts from root



src: Forouzan - Computer Networking

DNS Node Labels

- Limits
  - Labels
    - 63 octets or less
    - High order 2 bits of length field should be 0
    - Case insensitive
    - Only DNS name, and not URI path
    - Labels must be unique within parent domain
  - Names: 255 octets or less
  - UDP messages: 512 octets or less
- Longest label
- http://thelongestlistofthelongeststuffatthelongestdomainnameatlonglast.com/

Longest Label and URL

thelongestlistofthelongeststuffatthelongestdomainnameatlonglast.com/wearejustdoingthistobestupidnowsincethiscangoonforeverandeverandeverbutitstillllookskindaneatinthebrowsereventhoughitsabigwasteoftimeandenergyandhasnorealpointbutwehadtodoitanyways.html

Longest Label and URL

the longest list of the longest stuff at the longest domain name at long last.com/we are just doing this to be stupid now since this can go on forever and ever and ever but it still looks kind a neat in the browser even though its a big waste of time and energy and has no real point but we had to do it any ways.html

DNS

- **FQDN:** ends with a period(.)
  - also called, absolute domain
- **PQDN:** does not end with a period
  - assumption is name needs to be completed
  - two or more labels may be considered complete
  - general practice usage (browser, email)
- Reserved domain names (RFC 2606)
  Top level
    - .test, .example, .invalid, .localhost

  2nd level domains
  - Example.com (192.0.43.10),
  - Example.net (192.0.43.10),
  - Example.org (192.0.43.10)

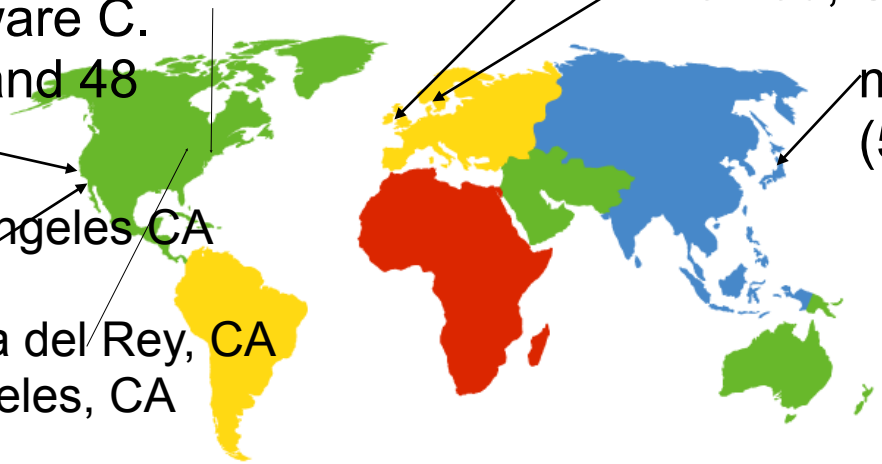
DNS: root name servers

- Contacted by local name server that can not resolve name
- root name server:
  - `http://www.iana.org/domains/root/servers`
  - contacts authoritative name server if name mapping not known
  - gets mapping
  - returns mapping to local name server
- Shortcut (temporary) approach
  - make an entry in DNS local file
    - /etc/hosts in linux
      - e.g. `10.211.55.10  mywww.com`
    - \Windows\System32/drivers\etc\hosts

a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	VeriSign, Inc.
b.root-servers.net	199.9.14.201, 2001:500:200::b	USC (ISI)
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Comm.
d.root-servers.net	199.7.91.13, 2001:500:2d::d	Univ. of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US DoD (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	VeriSign
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

DNS: root name servers

c. Cogent, Herndon, VA (5 other sites)
d. U Maryland College Park, MD
h. ARL Aberdeen, MD
j. Verisign, Dulles VA (69 other sites)
k. RIPE London (17 other sites)
e. NASA Mt View, CA
f. Internet Software C. Palo Alto, CA (and 48 other sites)
i. Netnod, Stockholm (37 other sites)
m. WIDE Tokyo (5 other sites)



a. Verisign, Los Angeles CA (5 other sites)
b. USC-ISI Marina del Rey, CA
l. ICANN Los Angeles, CA (41 other sites)

g. US DoD Columbus, OH (5 other sites)

13 root name "servers" worldwide

TLD, authoritative servers

- *Top-level domain (TLD) servers:*
  - for `.com`, `.org`, `.net`, `.edu` etc.
  - for top-level country domains, e.g.: `uk`, `fr`, `in`
    - Network Solutions maintains servers for .com
    - Educause for `.edu` TLD
  - `https://data.iana.org/TLD/tlds-alpha-by-domain.txt`
- *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

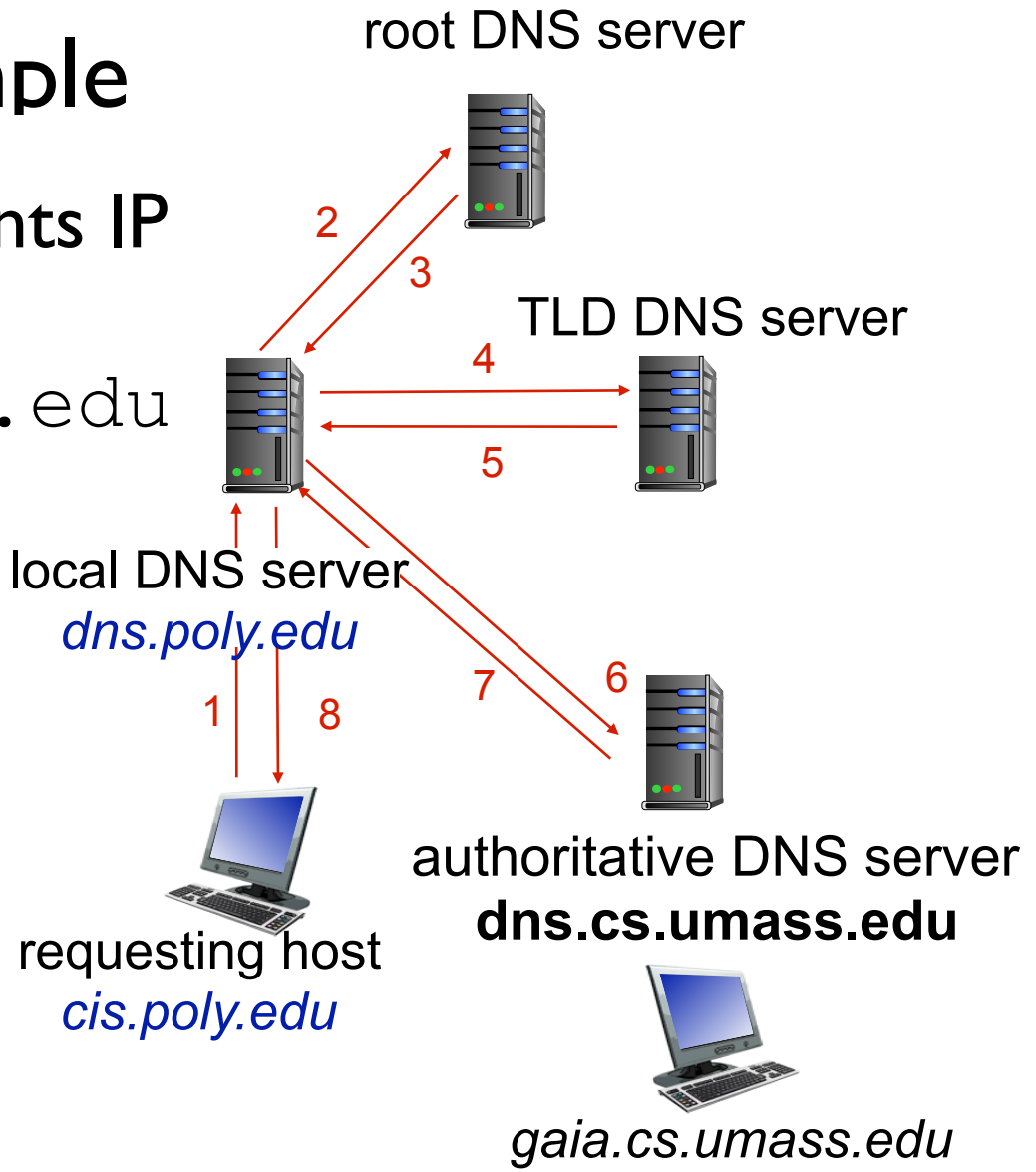
Local DNS name server

- 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

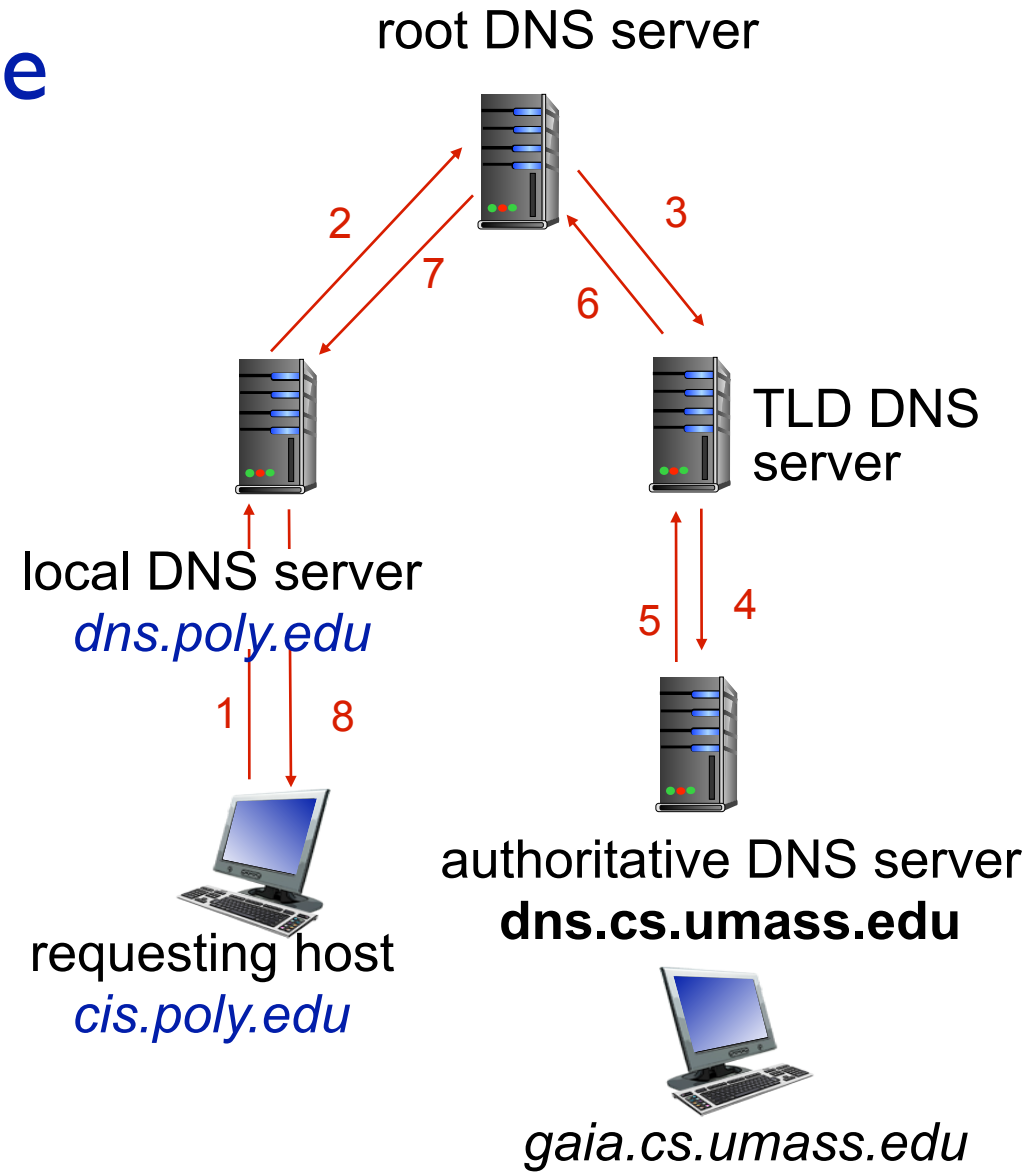
- host at cis.poly.edu wants IP address for
  - `gaia.cs.umass.edu`

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



DNS name resolution example

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



DNS: caching, updating records

- once (any) name server learns mapping, it *caches* mapping
  - cache entries timeout (disappear) after some time (TTL)
  - TLD servers typically cached in local name servers
    - thus root name servers not often visited
- cached entries may be *out-of-date* (best effort name-to-address translation!)
  - if name host changes IP address, may not be known Internet-wide until all TTLs expire
- update/notify mechanisms proposed IETF standard
  - RFC 2136

DNS records

DNS: distributed db storing resource records (RR)

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

type=A (default)

- **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 Examples

- dig -t A rprustagi.com @8.8.8.8

```
;; QUESTION SECTION:
;rprustagi.com.                 IN  NS
;; ANSWER SECTION:
rprustagi.com.          7069    IN  A
69.161.146.196
```

- dig -t ns rprustagi.com @8.8.8.8

```
;; QUESTION SECTION:
;rprustagi.com.                 IN  A
;; ANSWER SECTION:
rprustagi.com.   7199    IN  NS
dns1.doteasy.com.
rprustagi.com.   7199    IN  NS
dns2.doteasy.com.
```

DNS Examples

- dig -t MX rprustagi.com @8.8.8.8

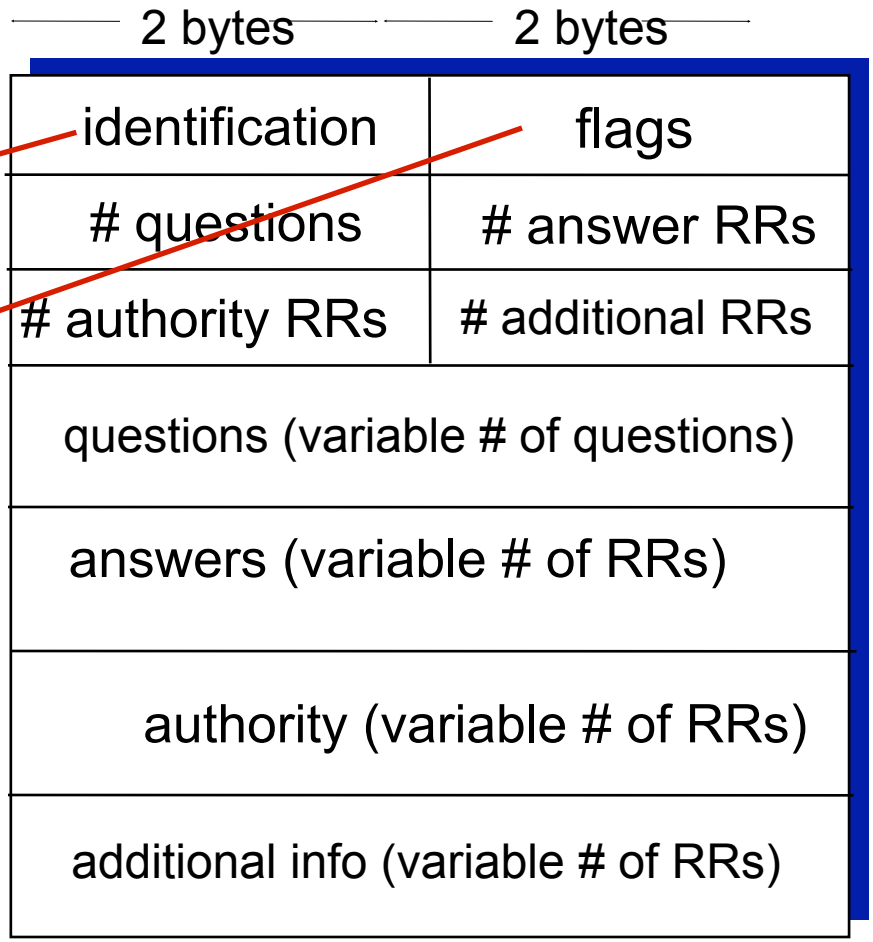
```
;; QUESTION SECTION:
;rprustagi.com.                 IN  MX

;; ANSWER SECTION:
rprustagi.com.          6934    IN  MX
15 dpmailbu.doteasy.com.
rprustagi.com.          6934    IN  MX
10 dpmail06.doteasy.com.
```

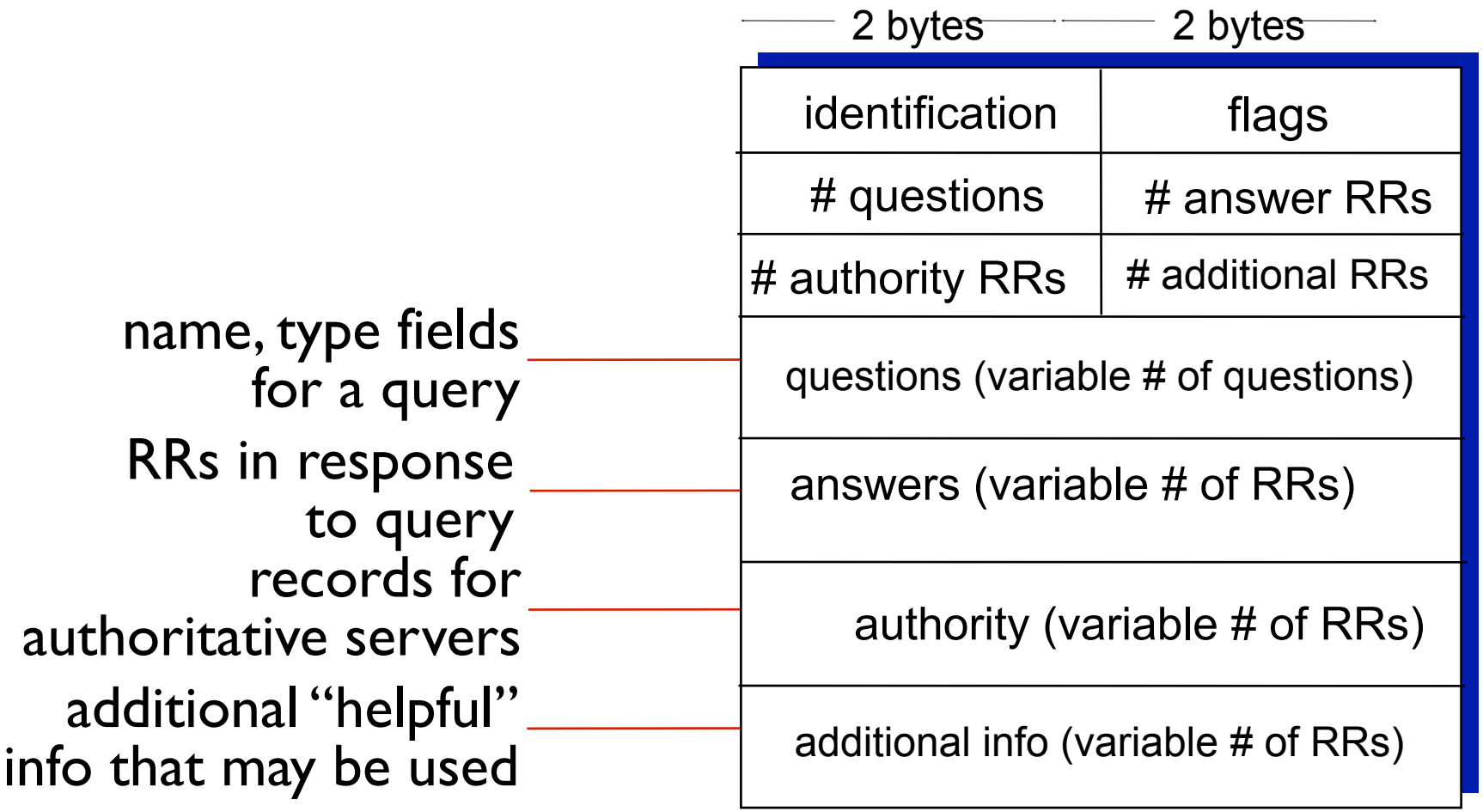
DNS protocol, messages

- *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



DNS query/response example

- Capture file: **ksit-dns-query.pcap (2018-08-14)**

```
$ dig @4.2.2.2 ksit.edu.in ANY

; <<>> DiG 9.10.6 <<>> @4.2.2.2 ksit.edu.in ANY
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46228
;; flags: qr rd ra; QUERY: 1, ANSWER: 12, AUTHORITY: 0,
ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 8192
;; QUESTION SECTION:
;ksit.edu.in.      IN  ANY

;; ANSWER SECTION:
ksit.edu.in.   10471 INA166.62.27.184
```

DNS query/response example…

```
ksit.edu.in.   3406  INNSns21.domaincontrol.com.
ksit.edu.in.   3406  INNSns22.domaincontrol.com.
ksit.edu.in.   3406  INSOAns21.domaincontrol.com.
dns.jomax.net. 2018061700 28800 7200 604800 600
ksit.edu.in.   3406  INMX5 alt1.aspmx.l.google.com.
ksit.edu.in.   3406  INMX5 alt2.aspmx.l.google.com.
ksit.edu.in.   3406  INMX1 aspmx.l.google.com.
ksit.edu.in.   3406  INMX10 aspmx2.googlemail.com.
ksit.edu.in.   3406  INMX10 aspmx3.googlemail.com.
ksit.edu.in.   3406  INTXT"google-site-
verification=NyjmOua0GXrP8rj27-a6zlABkSmXMGyBaoQ0hTstGwc"
ksit.edu.in.   3406  INTXT"MS=ms69244281"
ksit.edu.in.   3406  INTXT"v=spf1 include:_spf.google.com
~all"

;; Query time: 524 msec
;; SERVER: 4.2.2.2#53(4.2.2.2)
;; WHEN: Tue Aug 14 16:18:59 IST 2018
;; MSG SIZE  rcvd: 445
```

Inserting records into DNS

- example: new startup "Network Utopia"
- register name networkuptopia.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:
    (networkutopia.com, dns1.networkutopia.com, NS)
    - **(dns1.networkutopia.com, 212.212.212.1, A)**

Attacking DNS

- DDoS attacks
- Bombard root servers with traffic
  - Not successful to date
  - Traffic Filtering
  - Local DNS servers cache IPs of TLD servers, allowing root server bypass
- Bombard TLD servers
  - Potentially more dangerous

- Redirect attacks
  - Man-in-middle
  - Intercept queries
  - DNS poisoning
  - Send bogus relies to DNS server, which caches
- Exploit DNS for DDoS
  - Send queries with spoofed source address: target IP
  - Requires amplification

Summary

- DNS protocol
  - Top level domains
- Query type
  - Iterative
  - Recursive
- DNS record structure
  - Query and Answer
- DNS Servers