DNS – Domain Name System

Peter Sjödin
KTH School of ICT

Acknowledgements

- The presentation builds upon material from
  - Previous slides by Olof Hagsand, Markus Hidell, Peter Sjödin and Björn Knutsson
  - *Computer Networking: A Top Down Approach*, 6th ed. Jim Kurose, Keith Ross. Addison-Wesley.
  - *TCP/IP Protocol Suite*, 4th ed, Behrouz Foruzan. McGraw-Hill.

Course Material

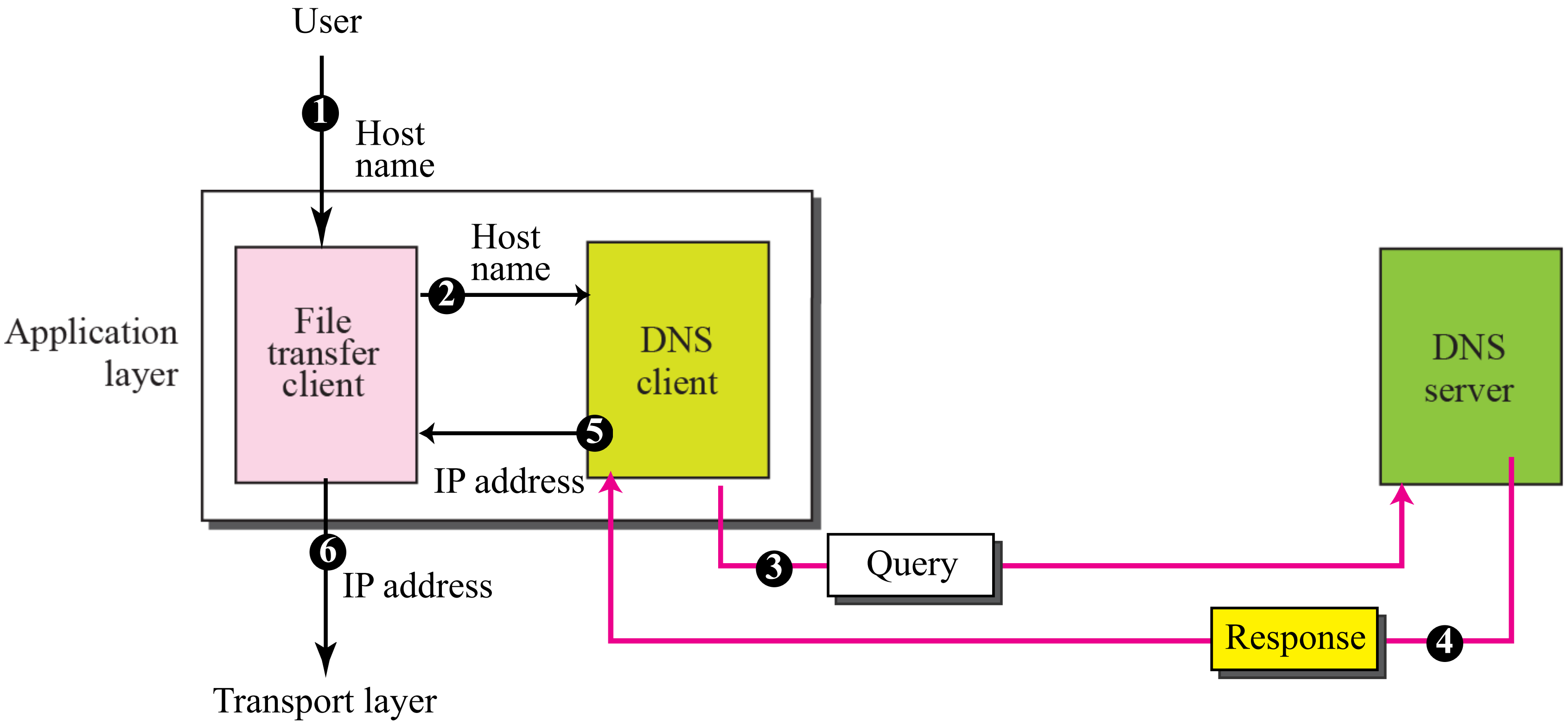
- Forouzan Chapter 19
- Lab: Domain Name System
  - BIND 9 reference manual
    - http://www.bind9.net/manuals
    - Intro – Chapter 1
    - Zone files – Chapter 3
- RFC 1034 and RFC 1035 (Reference)
- Liu and Albitz, DNS and BIND, O'Reilly (Reference)
- IANA
  - http://www.iana.org/assignments/dns-parameters

Outline

- Name Systems
- Internet Domains
- Distributed system of name servers
- Application layer protocol
- DNS servers and zone files

DNS – The Domain Name System

- Main purpose: Translate hostnames to IP addresses
  - "www.kth.se" and "www.google.se" are easier than "130.237.32.143" and "2a00:1450:400f:801::101f"

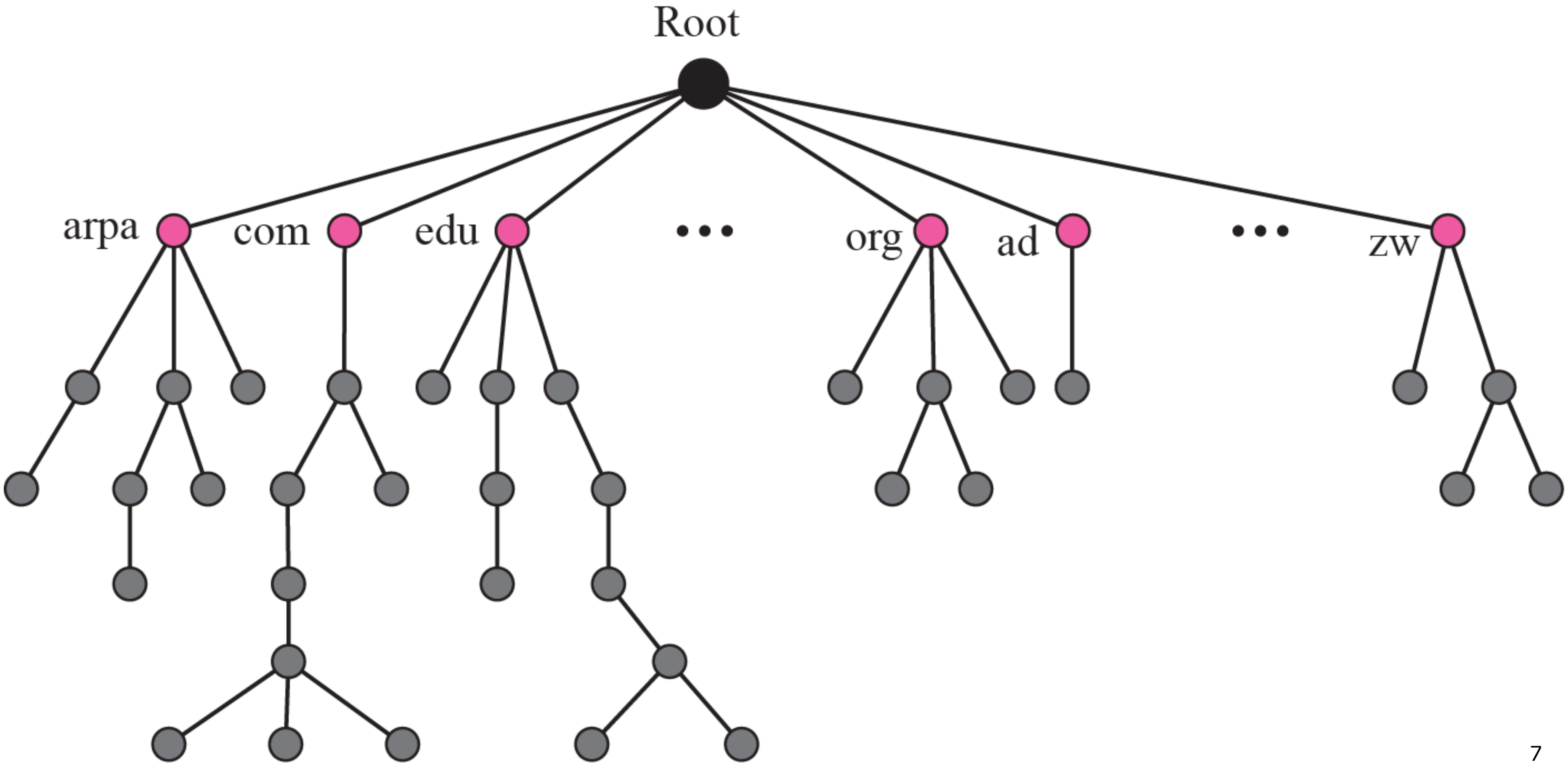


Why Names

- Easier to use and remember
- Names add a layer of abstraction
  - Decoupling between names and hosts/addresses
  - One name can map to several addresses
  - One address can map to several names
- Names can be used for other purposes
  - Load balancing
  - Redundancy
  - Service location and aliasing
  - Mail direction and redirection

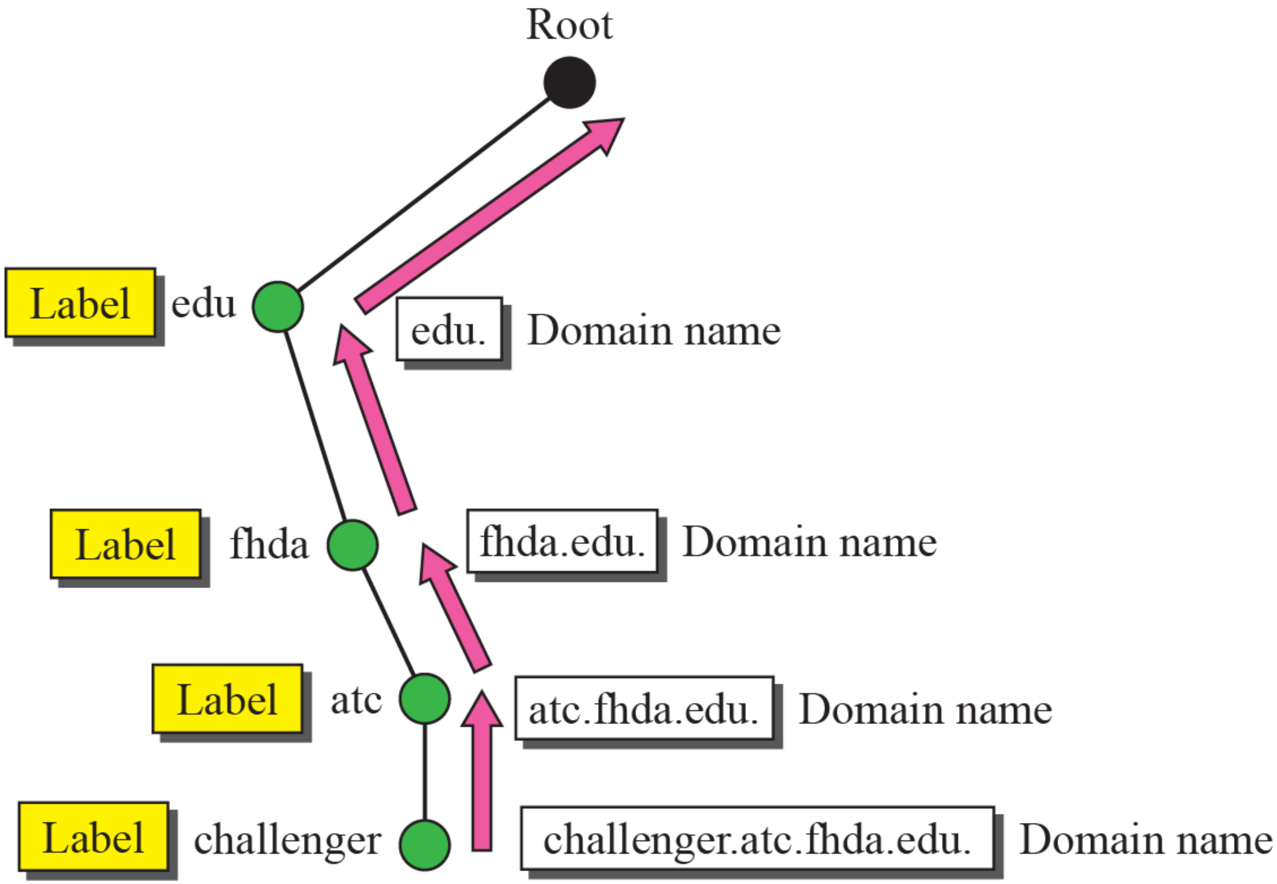
Domain Name Space

- Hierarchical name space organized as an inverted-tree structure



Domain Names and Labels

- Nodes have labels (root’s label is empty string)
- Each node represents a domain name



Domain Names

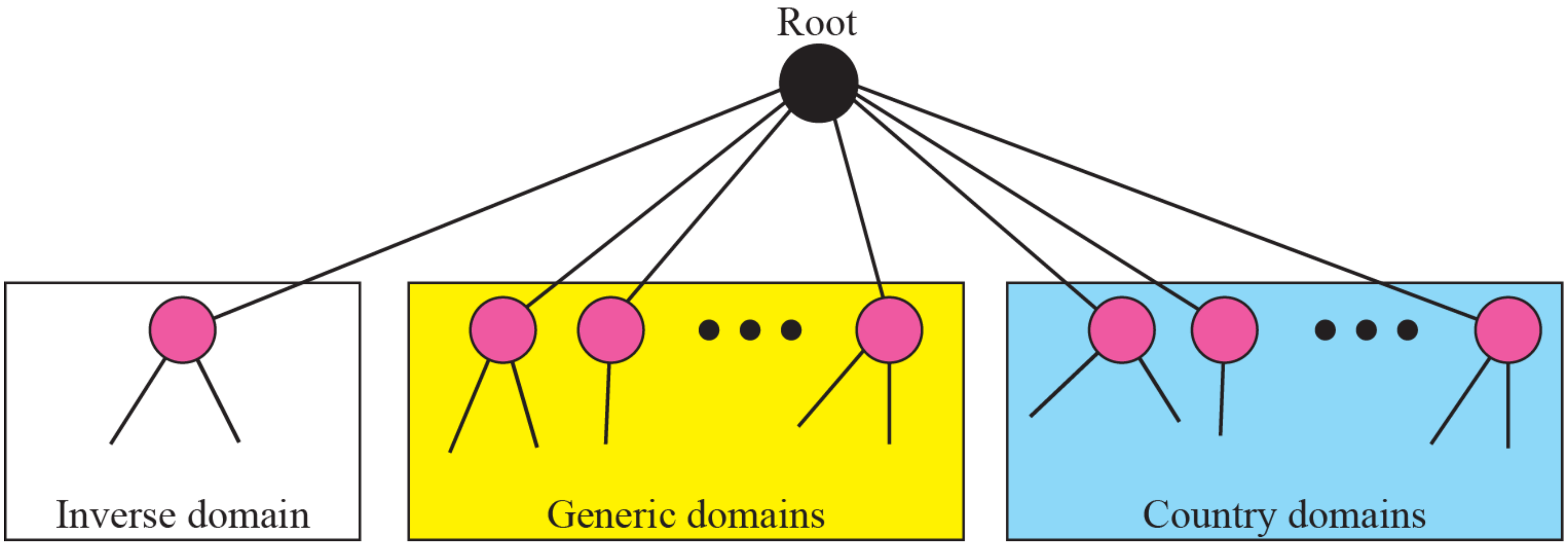
- Domain name is sequence of labels separated by dots "."
- A full domain name is a sequence from bottom to top
  - Root's label is empty string, so a full domain name ends with a dot "."
  - Fully Qualified Domain Name (FQDN)
- Otherwise partial name
  - Partially Qualified Domain Name (PQDN)
  - Relative to a node in the tree
  - The term "PQDN" is seldom used in practice though

FQDN	PQDN
challenger.atc.fhda.edu.	challenger.atc.fhda.edu
cs.hmme.com.	cs.hmme
www.funny.int.	www

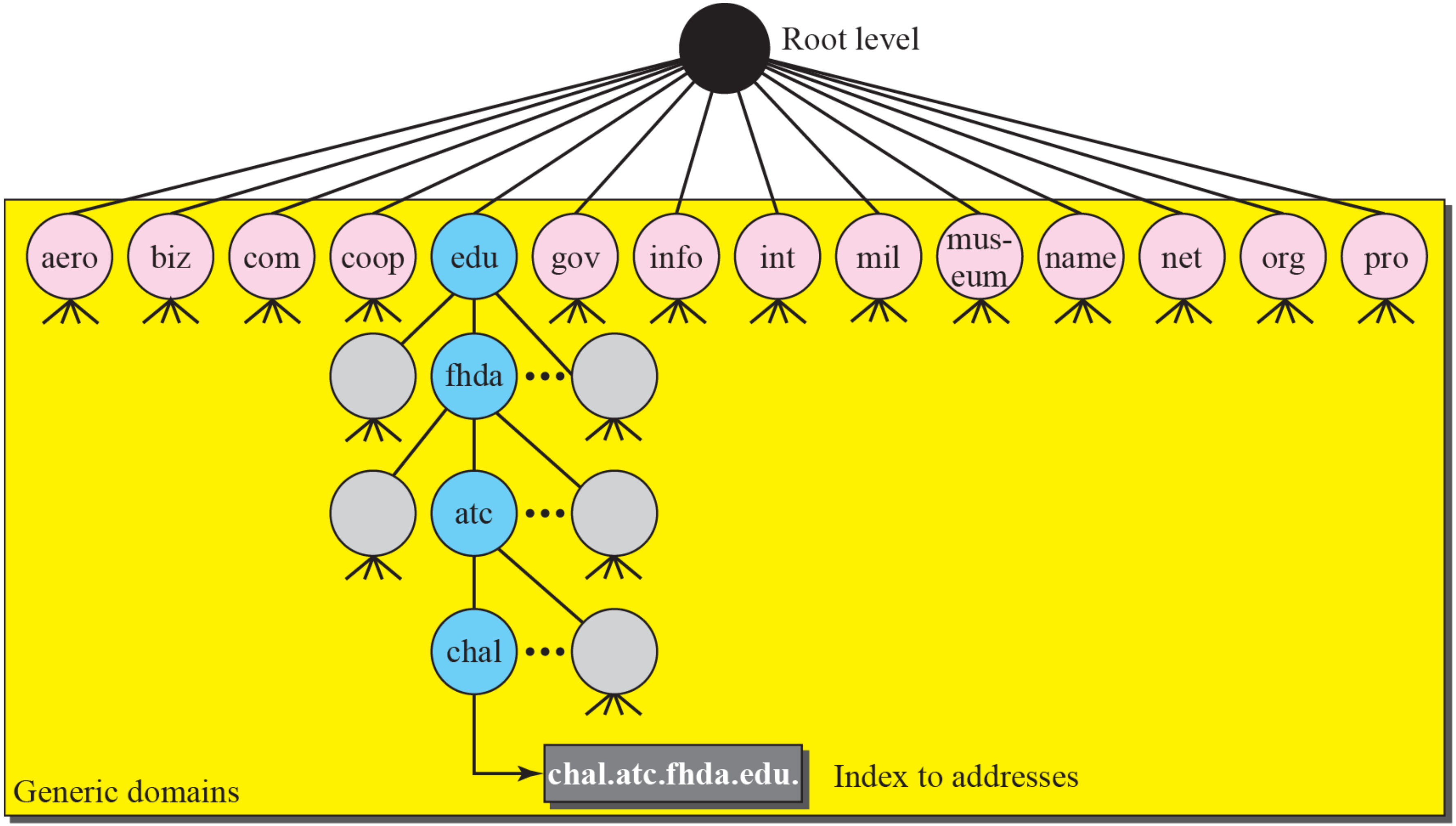
Outline

- Name Systems
- Internet Domains
- Distributed system of name servers
- Application layer protocol
- DNS servers and zone files

Domains in the Internet



Generic Domains



Generic Domain Labels

Domain	Intended use
aero	the air transport industry.
asia	companies, organizations and individuals in the Asia-Pacific region
biz	business use
cat	Catalan language/culture
com	commercial organizations, but unrestricted
coop	cooperatives
edu	U.S. post-secondary educational establishments
gov	U.S. government entities at the federal, state, and local levels
info	informational sites, but unrestricted
int	international organizations established by treaty
jobs	employment-related sites
mil	the U.S. military
mobi	sites catering to mobile devices
museum	museums
name	families and individuals
net	originally for network infrastructures, now unrestricted
org	originally for organizations not clearly falling within the other gTLDs, now unrestricted
post	postal services
pro	certain professions
tel	services involving connections between the telephone network and the Internet
travel	travel agents, airlines, hoteliers, tourism bureaus, etc.
xxx	pornography

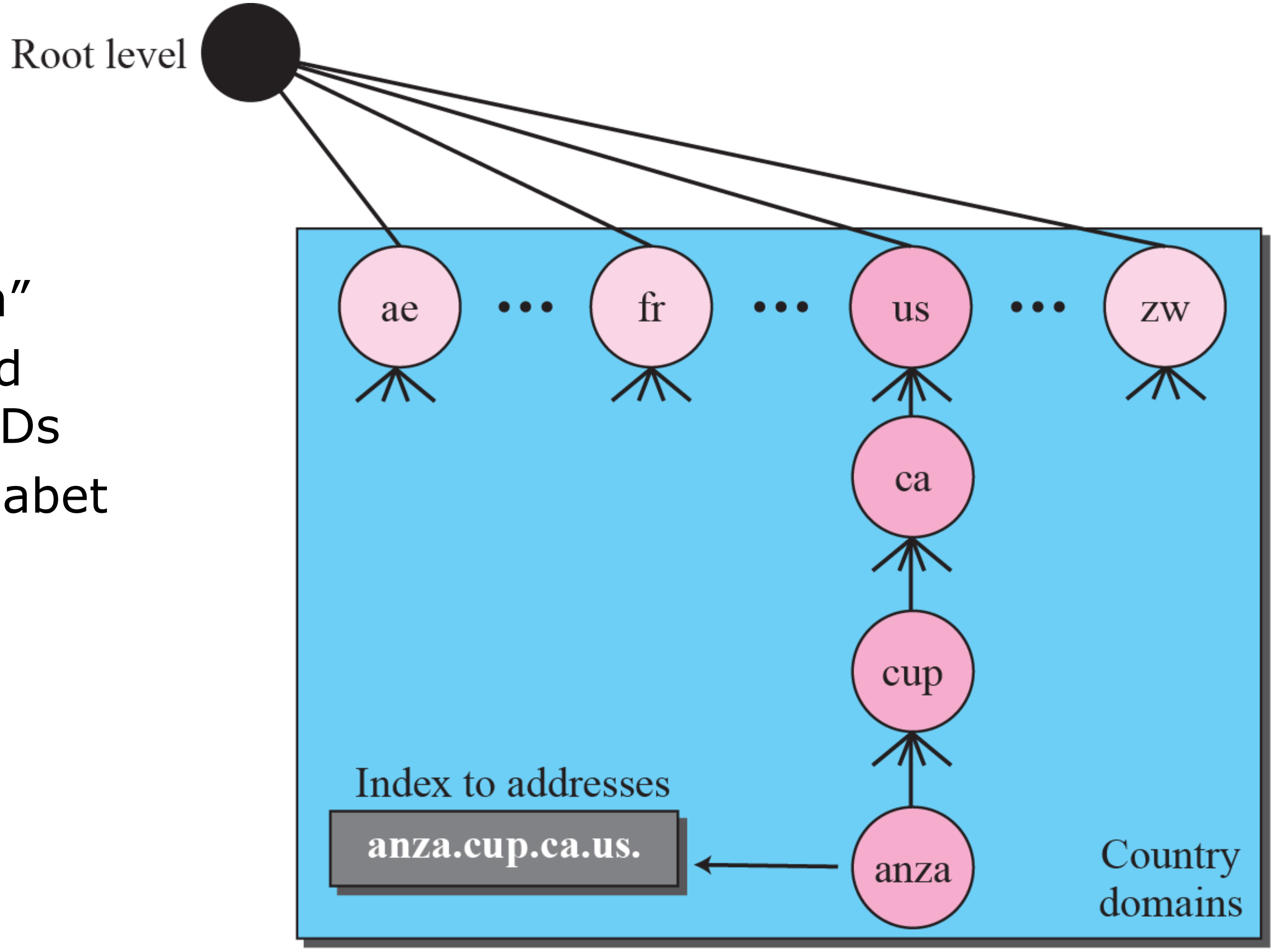
From: Wikipedia, 2013-09-30

ICANN New gTLD Program

- Internet Corporation for Assigned Names and Numbers
  - http://newgtlds.icann.org
  - "Largest-ever expansion of the Domain Name System"
  - ICANN accepting applications for new gTLDs since 2012
  - 1192 "Registry Agreements" signed for new gTLDs as of Sept 25, 2015
    - Still more in process
- Examples
  - Commonly used words – .CULTURE, .MUSICAL, .TRUSTED, .PIZZA
  - Geographic – .WALES, .BUDAPEST
  - Community – .CLEANWATER, .LITERACY
  - Brand – .BMW, .YOUTUBE
  - Internationalized Domain Names – онлайн, 游戏

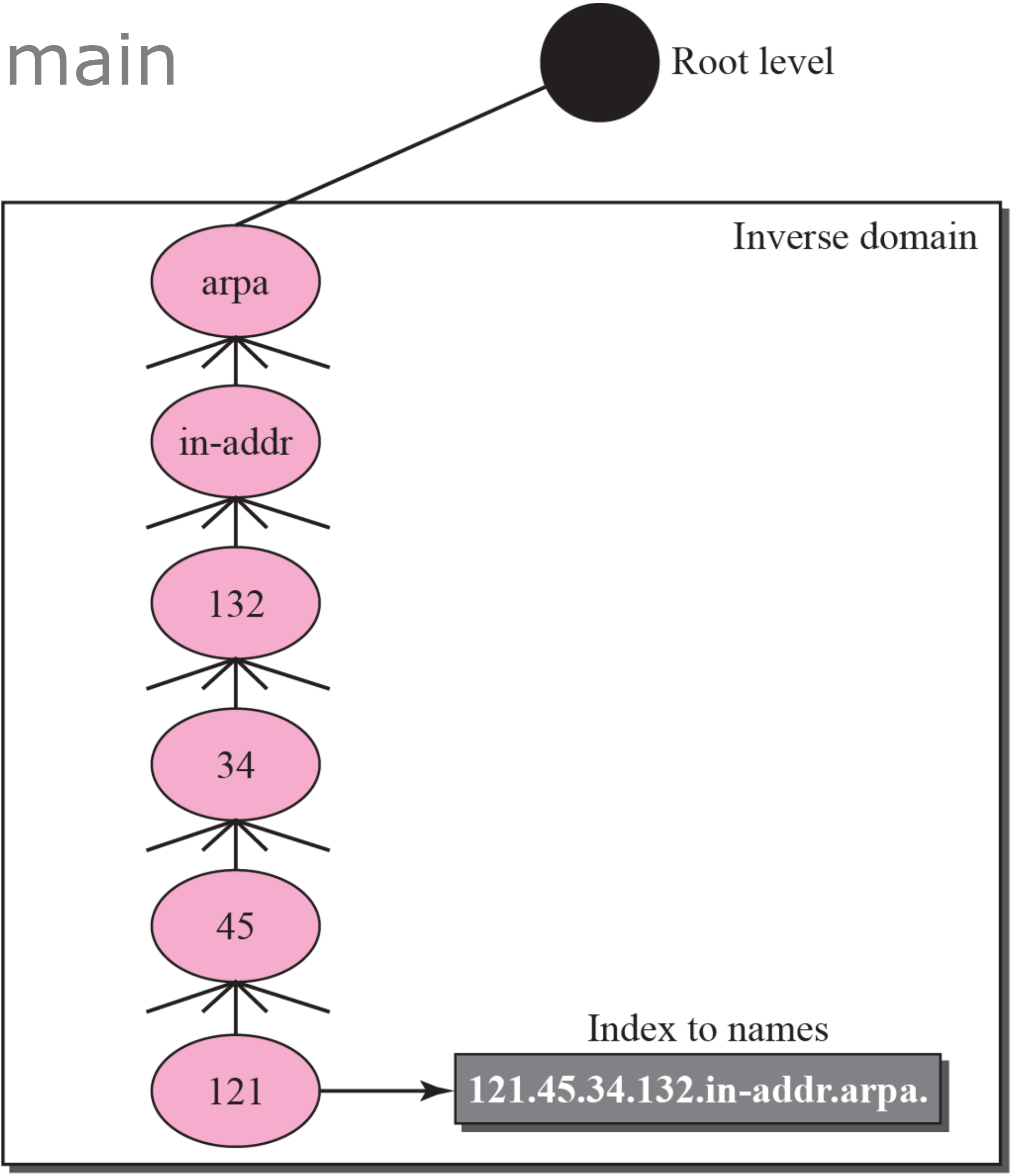
Country Domains

- Country code
  - Two-letter ISO codes
    - "se", "uk", "cn"
  - Internationalized country code TLDs
    - Non-latin alphabet



Inverse Domain

- Infrastructure domain
- For mapping addresses to names
  - in-addr.arpa.
    - IPv4
  - ip6.arpa.
    - IPv6
  - ...



Outline

- Name Systems
- Internet Domains
- Distributed system of name servers
- Application layer protocol
- DNS servers and zone files

The DNS System

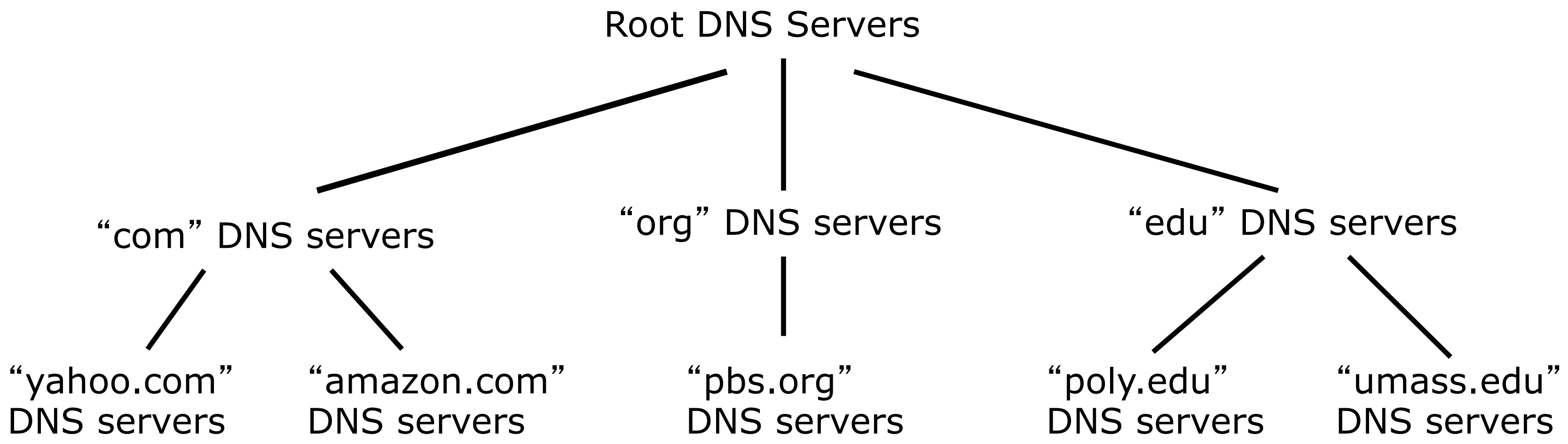
- A distributed database
- An application-layer protocol
  - For querying the database

Core Internet function, implemented as application-layer protocol—complexity at network's edge

Distributed Database

- Consistency
  - All parts of the database are up to date and synchronized
- Management
  - Responsibility for database updates
- Service location
  - What server to use, and where to find it
- …

Hierarchy of Name Servers



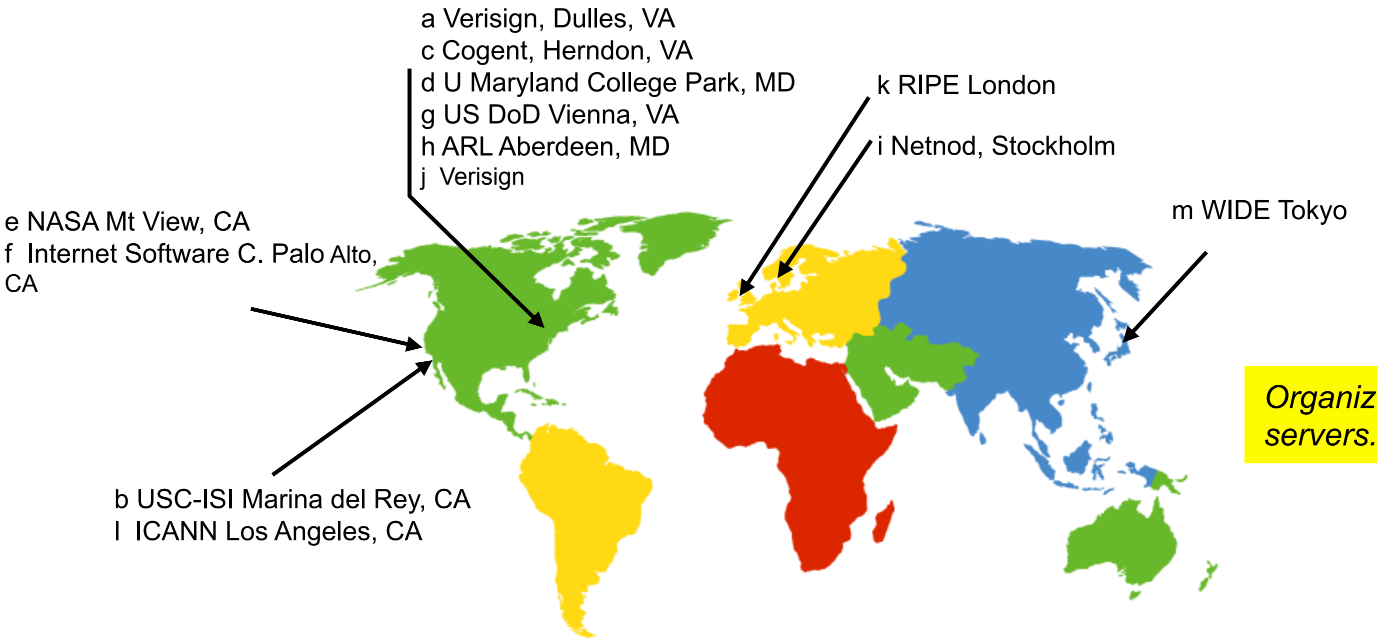
- Distributed database organized as a tree of name servers

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”

Root Name Servers

- Registry of name servers for top-level domains
- “Root Zone” and “Root Hints” files
  - http://www.iana.org/domains/root/files
- 13 root name servers worldwide
  - Replicated, with anycast addressing/routing
- http://www.root-servers.org



Organizations responsible for root servers.

Root Servers

From Wikipedia, 2015-09-28

Hostname	IPv4/IPv6 Addresses	Operator	No of Sites Global/Local
a.root-servers.net	198.41.0.4 2001:503:ba3e::2:30	Verisign	5/0
b.root-servers.net	192.228.79.201 2001:500:84::b	USC-ISI	0/1
c.root-servers.net	192.33.4.12 2001:500:2::c	Cogent Communications	8/0
d.root-servers.net	199.7.91.13 2001:500:2d::d	University of Maryland	50/67
e.root-servers.net	192.203.230.10 N/A	NASA	1/11
f.root-servers.net	192.5.5.241 2001:500:2f::f	Internet Systems Consortium	57/0
g.root-servers.net	192.112.36.4 N/A	Defense Information Systems Agency	6/0
h.root-servers.net	128.63.2.53 2001:500:1::803f:235	U.S. Army Research Lab	2/0
i.root-servers.net	192.36.148.17 2001:7fe::53	Netnod	41/0
j.root-servers.net	192.58.128.30 2001:503:c27::2:30	Verisign	61/13
k.root-servers.net	193.0.14.129 2001:7fd::1	RIPE NCC	5/23
l.root-servers.net	199.7.83.42 2001:500:3::42	ICANN	157/0
m.root-servers.net	202.12.27.33 2001:dc3::35	WIDE Project	6/1

Top-Level DNS Servers

- Top-level domain (TLD) DNS servers:
  - responsible for top-level domains
    - Generic domains: com, org, net, edu, etc,
    - Country domains: se, uk, fr, ca, jp, etc.
- ICANN/IANA delegates to each TLD
  - VeriSign operates “com” TLD
  - Educause (through VeriSign) for “edu” TLD
  - Stiftelsen för Internetinfrastruktur (.SE) maintains “se” TLD
  - Foggy Moon LLC operates “pizza” TLD

Authoritative DNS Servers

- Authoritative DNS servers:
  - organization’s name servers, providing authoritative hostname to IP mappings for organization’s servers (e.g., Web, mail).
    - Authoritative – server has been configured with the mapping for the domain in question
      - Provides firsthand information
  - can be maintained by organization or a service provider

```
$ dig +short kth.se ns
nic.lth.se.
ns2.chalmers.se.
b.ns.kth.se.
a.ns.kth.se.
```

"According to many customers, sites hosted by major web host and domain registrar GoDaddy are down. […]

A tipster tells us that the technical reason for the failure is being caused by the inaccessibility of GoDaddy's DNS servers — specifically CNS1.SECURESERVER.NET, CNS2.SECURESERVER.NET, and CNS3.SECURESERVER.NET are failing to resolve."

http://techcrunch.com/2012/09/10/godaddy-outage-takes-down-millions-of-sites/, 2012-09-11

- "On October 21, 2002 an attack lasting for approximately one hour was targeted at all 13 DNS root name server. This was the second significant failure of the root nameservers."
- "On February 6, 2007 an attack began at 10 AM UTC and lasted twenty-four hours. At least two of the root servers (G-ROOT and L-ROOT) reportedly suffered badly […]"

http://en.wikipedia.org/wiki/Distributed_denial_of_service_attacks_on_root_nameservers, *2012-09-11*

Making Queries – Local Name Server

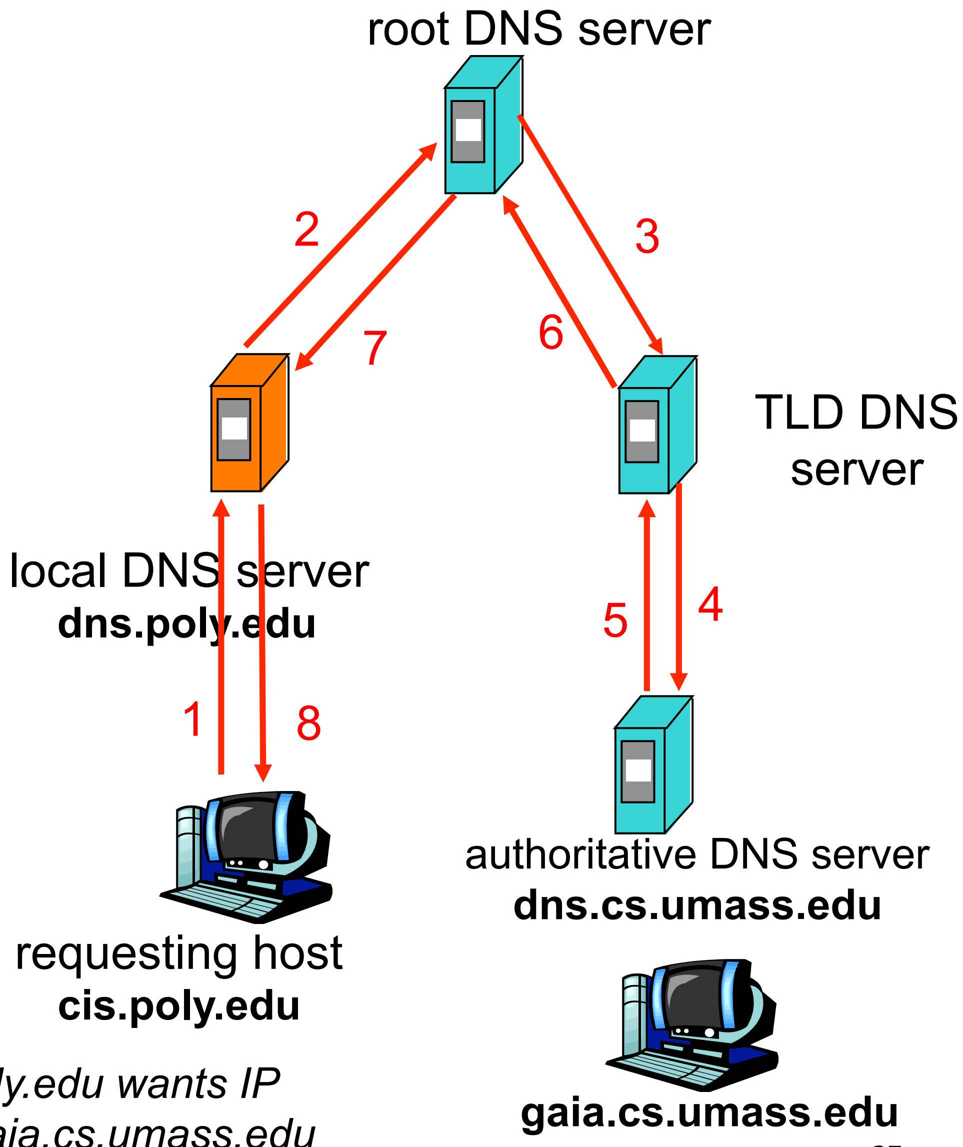
- “Default name server”
- “Resolving name server”
- Does not belong to the hierarchy of name servers
- Each ISP (residential ISP, company, university) has one.
  - Part of IP configuration of a host
    - Which is your name server?
- Responsible for making queries into the distributed database
  - On behalf of its clients
    - When host makes DNS query, query is sent to its local name server
- Maintains a cache of recent responses

Recursive Resolution

- ❒ Server should respond with the requested address
- ❒ If a server does not have the address, the server passes the query to another server

Not how it is done in practice:

- ❒ puts burden of name resolution on contacted name server
- ❒ high-level servers (root, TLD, etc) do not accept recursive queries
- ❒ (So figure does not reflect real scenario)



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

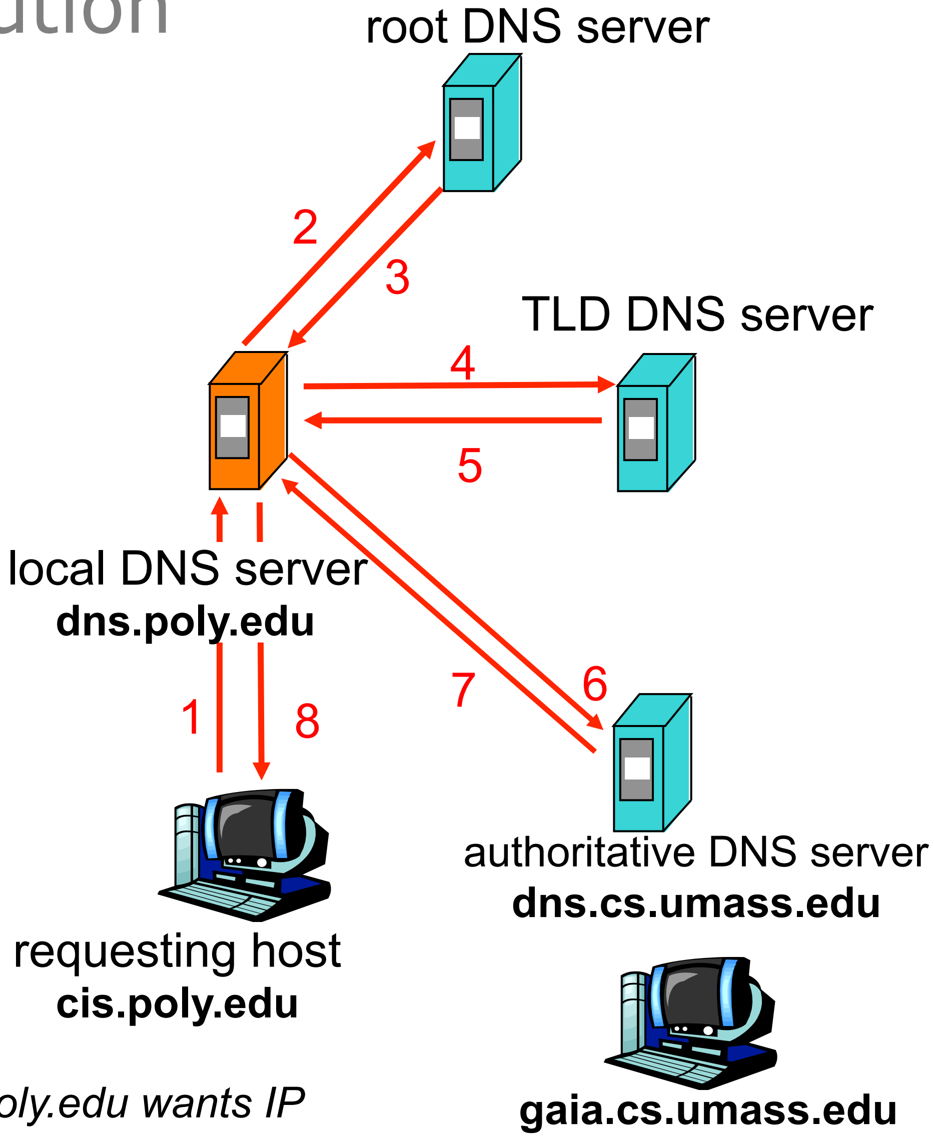
Iterative Resolution

iterated query:

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

In practice:

- ❒ Local DNS server performs iterated query on behalf of client
- ❒ Local DNS server stores results of previous lookups in a cache



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

Delegation

- Authority is delegated from the root downwards
- Delegation is the primary way to distribute the DNS database

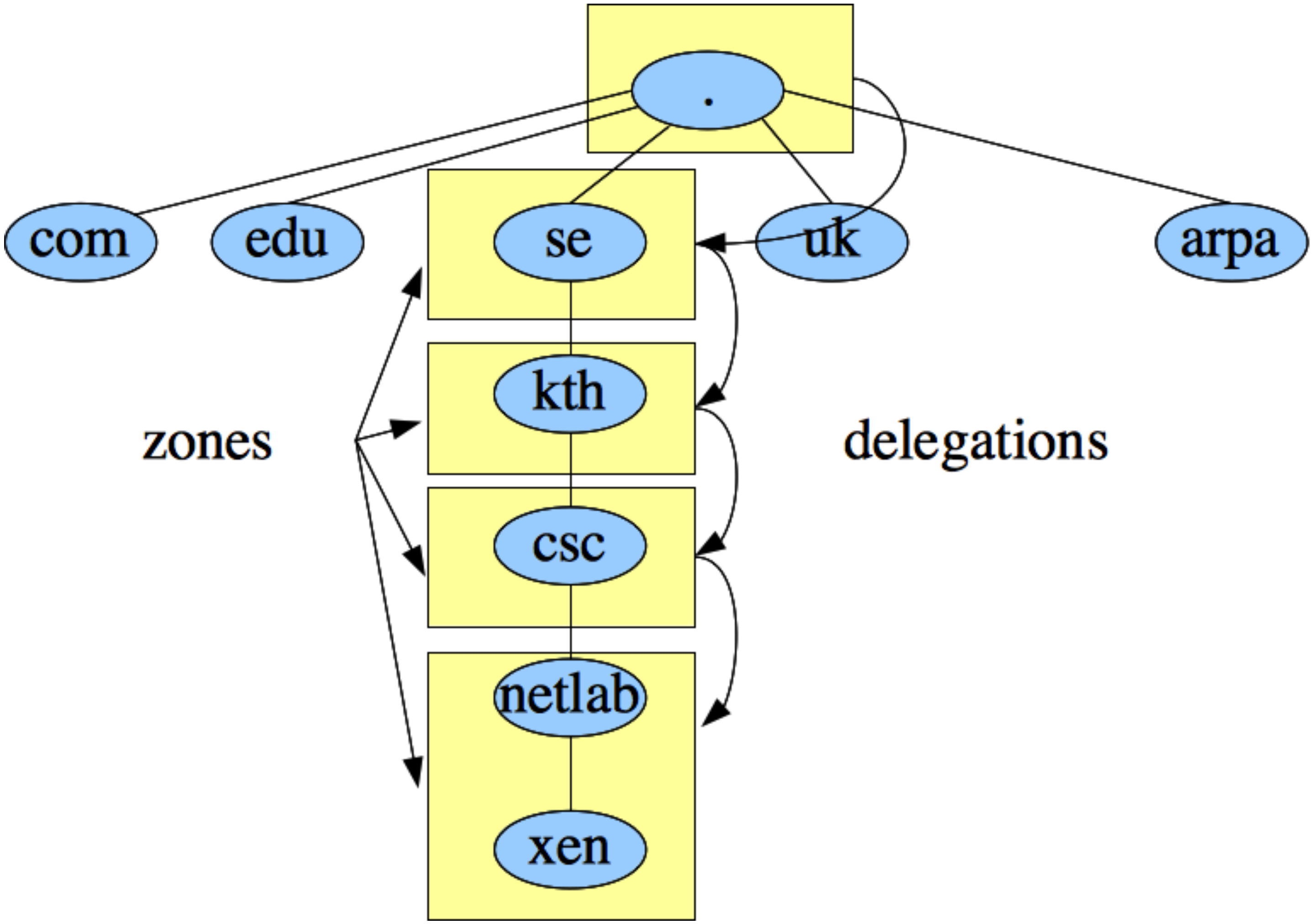
- *In the labs, we use "xen.netlab.csc.kth.se"*
  - ICANN handles the root
  - ICANN delegates "se" to IIS
  - IIS delegates "kth" to KTH Royal Institute of Technology
  - KTH delegates "csc" to the school of computer science (KTH CSC)
  - KTH CSC delegates "netlab" to us
  - We delegate to you (when you do the lab)

- You can delegate at every point in the tree
  - But you don't have to
  - Example: "xen" is not delegated from "netlab"

Zones

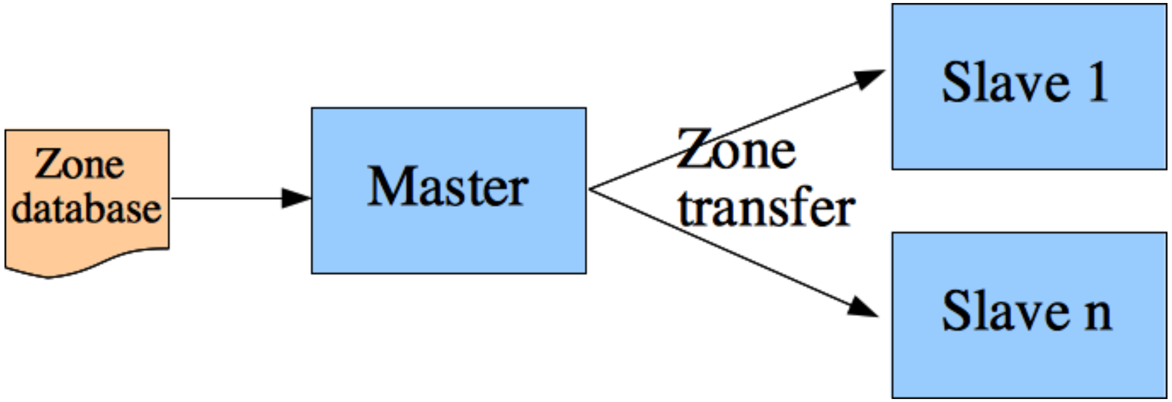
- Delegation requires administrative units
  - “Zones”
  - Similar to autonomous systems in routing
- A zone is a domain minus everything that has been delegated
- *The parent zone refers to a name server of the delegated zone*
- There should be more than one name server per zone
  - Currently four for “kth.se”
- The distribution of the DNS database is thus made by sequences of delegations from parent zone to child

Zones and Delegations



Master and Slaves

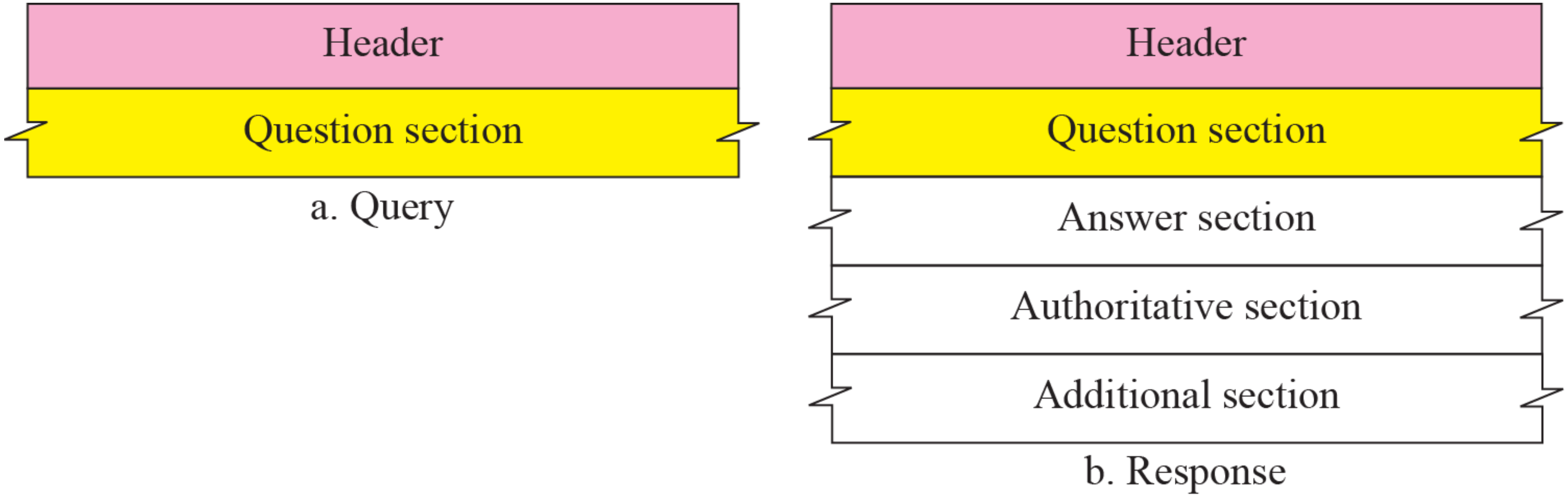
- One or several name servers are *authoritative* for a zone
  - Responsible for that part of the namespace
- One server is master (primary server)
  - Other servers are slaves (secondary servers)
  - Redundancy
- Changes are distributed to slaves
  - “Zone transfer” over TCP



Outline

- Name Systems
- Internet Domains
- Distributed system of name servers
- Application layer protocol
- DNS servers and zone files

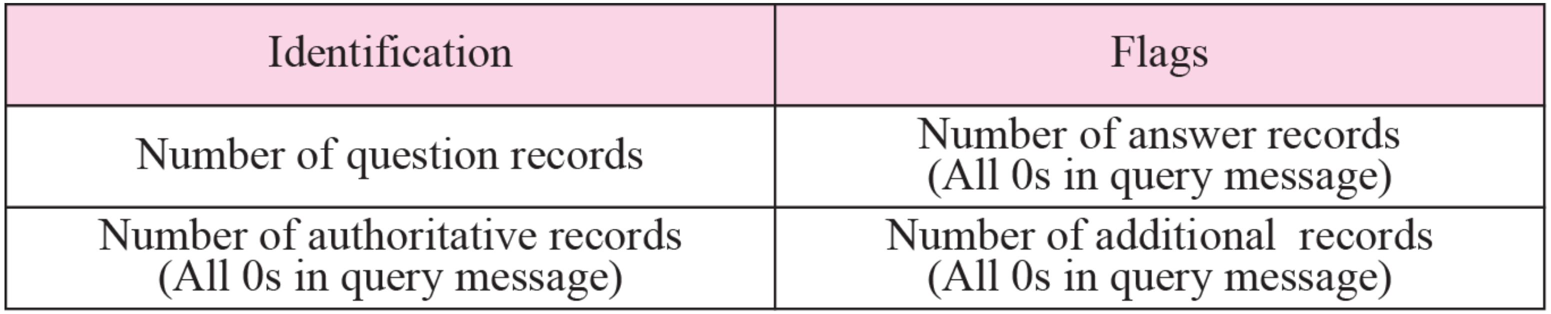
DNS Query and Response



- UDP and TCP port 53 (by default)

Side note: DNS primarily uses UDP. The trend is that messages are getting larger due to new functionality being introduced, such as security, so a DNS message may not fit in a single IP datagram. Then TCP might be a better choice, compared to IP fragmentation. Zone transfers always use TCP.

Header format

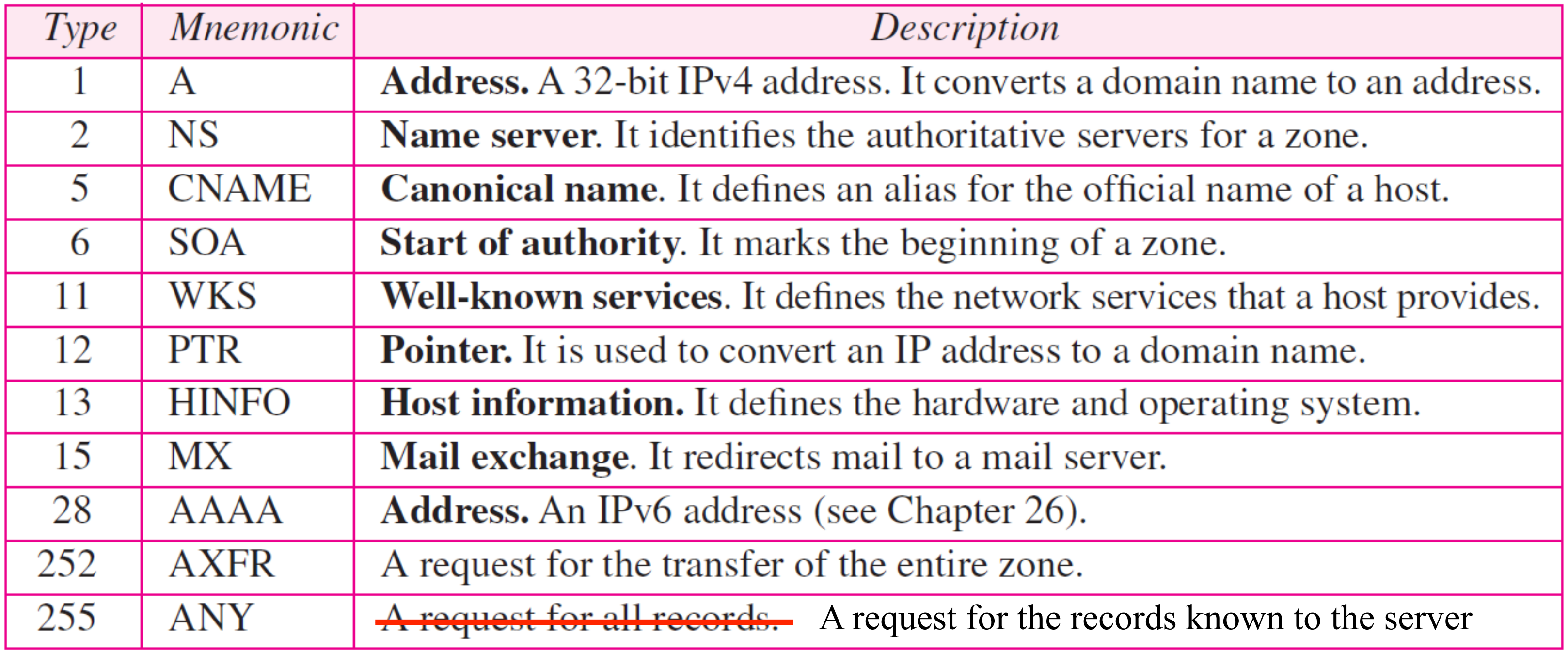


Identification	Flags
Number of question records	Number of answer records (All 0s in query message)
Number of authoritative records (All 0s in query message)	Number of additional records (All 0s in query message)

- Identification
  - Match response with query (16-bit number)
- Flags, various purposes including
  - Recursion
  - Indicating whether server is authoritative
  - Return code (error status)
- Answer records
  - Results of query
- Authoritative records
  - Domain names for authoritative name servers for domain in question
- Additional records
  - For instance, IP addresses for authoritative name servers

Examples of Record Types

Table 19.3 *Types*



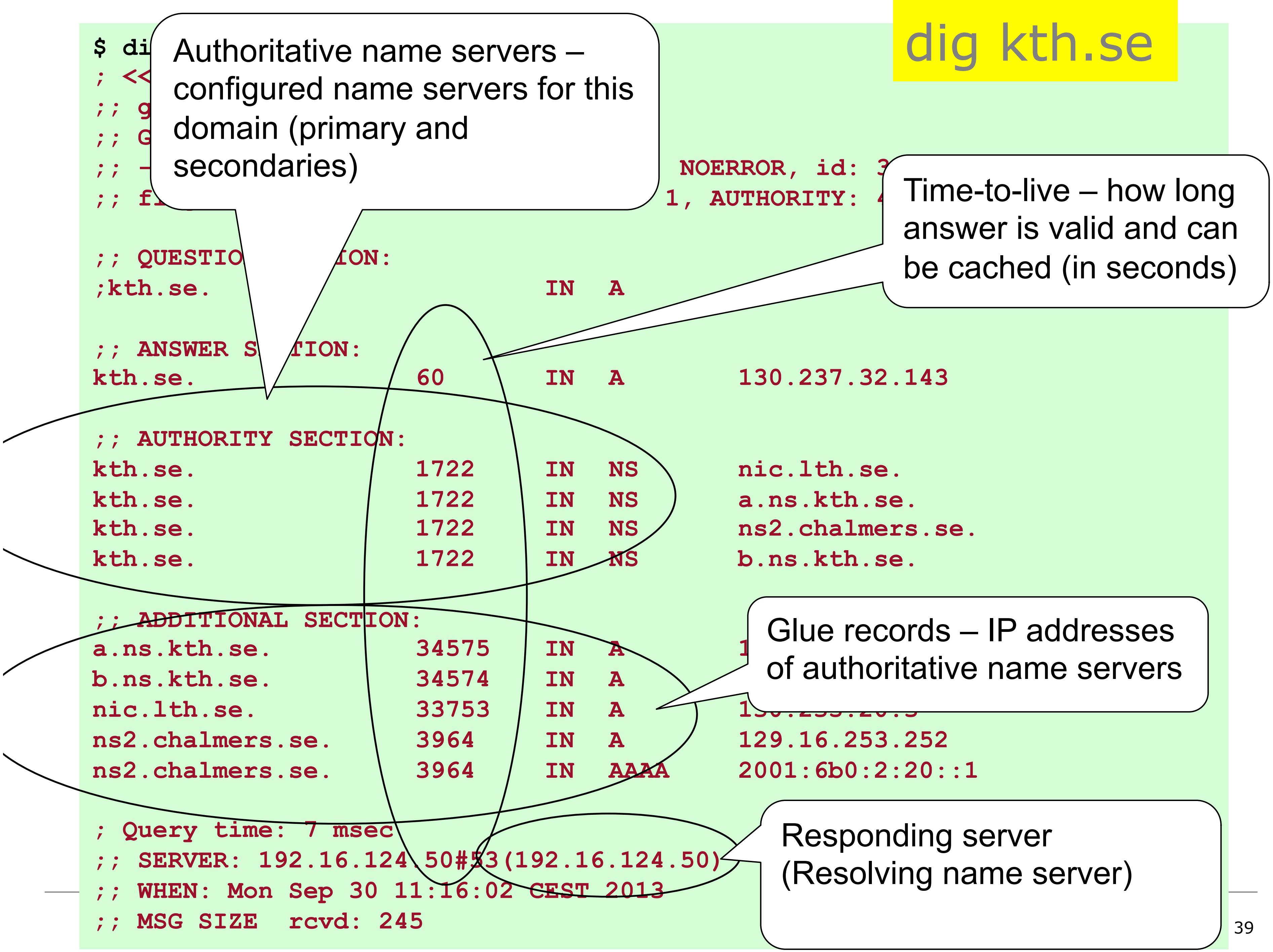
Type	*Mnemonic*	*Description*
1	A	**Address.** A 32-bit IPv4 address. It converts a domain name to an address.
2	NS	**Name server**. It identifies the authoritative servers for a zone.
5	CNAME	**Canonical name**. It defines an alias for the official name of a host.
6	SOA	**Start of authority**. It marks 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.~~ A request for the records known to the server

Querying Tools

- Make DNS queries from command line
- dig (domain information groper)
  - BIND DNS software
    - http://www.isc.org/software/bind
  - Preinstalled in most Linux distros and Mac OS X
  - Preferred tool
- Older tools
  - Nslookup
    - In Windows
  - host
    - Simple interface

dig kth.se

```
$ dig kth.se
; <<>> DiG 9.8.5-P1 <<>> kth.se
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32320
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 6

;; QUESTION SECTION:
;kth.se.                      IN  A

;; ANSWER SECTION:
kth.se.              60       IN  A        130.237.32.143

;; AUTHORITY SECTION:
kth.se.              1722     IN  NS       nic.lth.se.
kth.se.              1722     IN  NS       a.ns.kth.se.
kth.se.              1722     IN  NS       ns2.chalmers.se.
kth.se.              1722     IN  NS       b.ns.kth.se.

;; ADDITIONAL SECTION:
a.ns.kth.se.         34575    IN  A        130.237.72.246
b.ns.kth.se.         34574    IN  A        130.237.72.250
nic.lth.se.          33753    IN  A        130.235.20.3
ns2.chalmers.se.     3964     IN  A        129.16.253.252
ns2.chalmers.se.     3964     IN  AAAA     2001:6b0:2:20::1

; Query time: 7 msec
;; SERVER: 192.16.124.50#53(192.16.124.50)
;; WHEN: Mon Sep 30 11:16:02 CEST 2013
;; MSG SIZE  rcvd: 245
```



dig kth.se

```
$ di
; <<
;; g
;; G
;; -                                      NOERROR, id: 3
;; fl                                   1, AUTHORITY: 4

;; QUESTIO        ION:
;kth.se.                      IN   A

;; ANSWER S    TION:
kth.se.               60      IN   A        130.237.32.143

;; AUTHORITY SECTION:
kth.se.               1722    IN   NS       nic.lth.se.
kth.se.               1722    IN   NS       a.ns.kth.se.
kth.se.               1722    IN   NS       ns2.chalmers.se.
kth.se.               1722    IN   NS       b.ns.kth.se.

;; ADDITIONAL SECTION:
a.ns.kth.se.          34575   IN   A        1
b.ns.kth.se.          34574   IN   A
nic.lth.se.           33753   IN   A        130.235.20.3
ns2.chalmers.se.      3964    IN   A        129.16.253.252
ns2.chalmers.se.      3964    IN   AAAA     2001:6b0:2:20::1

; Query time: 7 msec
;; SERVER: 192.16.124.50#53(192.16.124.50)
;; WHEN: Mon Sep 30 11:16:02 CEST 2013
;; MSG SIZE  rcvd: 245
```

Authoritative name servers – configured name servers for this domain (primary and secondaries)

Time-to-live – how long answer is valid and can be cached (in seconds)

Glue records – IP addresses of authoritative name servers

Responding server (Resolving name server)

Query Specified Type

```
dig +short <domain> <query> (“+short” for brief output)
```

```
 $ dig +short kth.se a
130.237.32.143

$ dig +short kth.se aaaa

$ dig +short kth.se ns
nic.lth.se.
a.ns.kth.se.
b.ns.kth.se.
ns2.chalmers.se.

$ dig +short kth.se soa
a.ns.kth.se. hostmaster.kth.se. 2012090601 14400 3600 604800 86400

$ dig +short kth.se mx
10 mx.kth.se.
```

Reverse Lookups

```
dig -x <ip address>
```

```
$ dig +short mx.kth.se
130.237.48.98
130.237.32.140
130.237.48.97

$ dig +short -x 130.237.48.98
mx2.kth.se.

$ dig +short google.com aaaa
2a00:1450:400f:801::1008

$ dig +short -x 2a00:1450:400f:801::1008
arn06s02-in-x08.1e100.net.
```

Outline

- Name Systems
- Internet Domains
- Distributed system of name servers
- Application layer protocol
- DNS servers and zone files

Setting up a DNS Server

- BIND DNS software (Berkeley Internet Name Daemon)
  - Most common DNS software
    - DNS server
    - DNS resolver library (for client applications)
    - Testing tools (such as dig)
  - https://www.isc.org/software/bind
  - This is what you use in the DNS lab

Zone File

- DNS zone described in a zone file
  - Plain text format

```
Name        TTL     Class   Type    Rdata
```

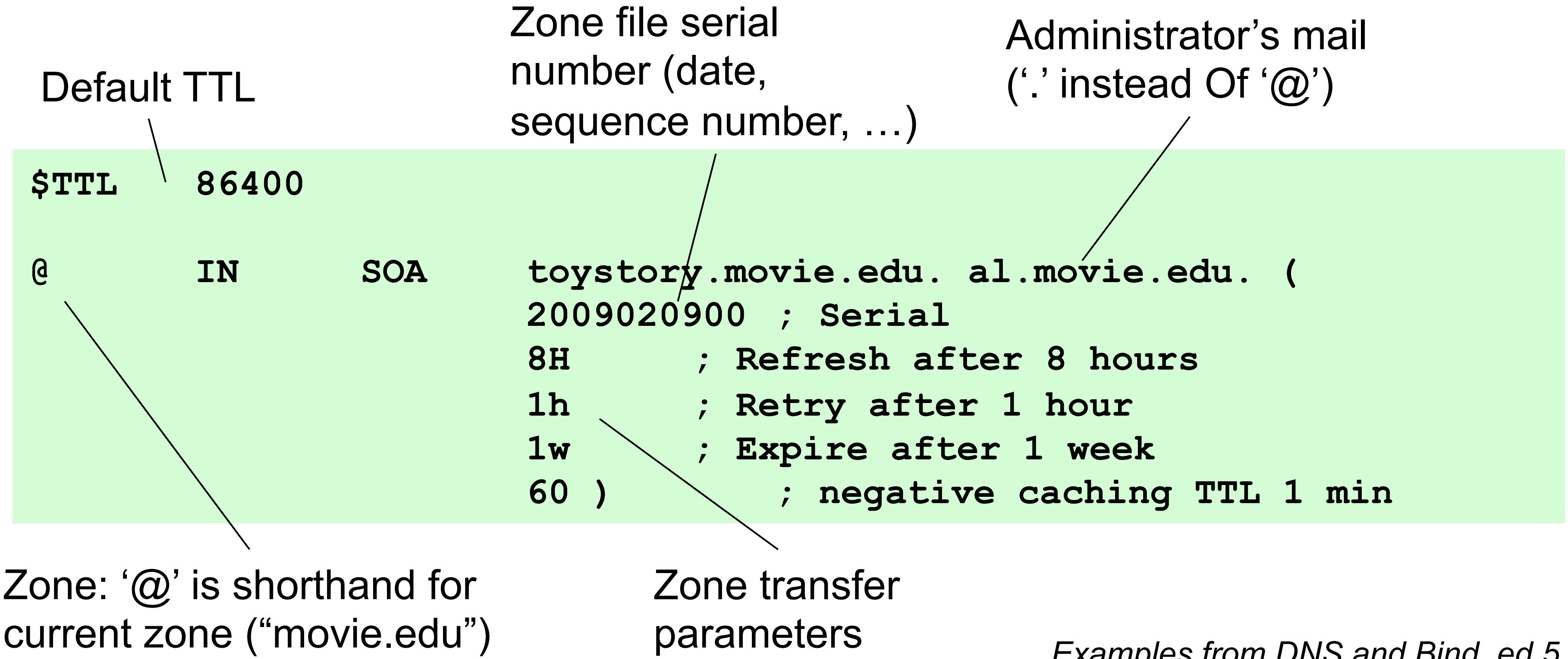
- Name – Owner name (or label) to which record belongs
- TTL – How long entries are valid (for cache)
  - Often skipped (use default)
- Class – IN (Internet class)
- Type – Resource record type
- Rdata – Type specific data

- Example (IPv4 address – A record):

```
www         60      IN      A       130.237.32.143
```

Start of Authority – SOA

- Defines a zone
- Always first record in a zone file



Default TTL

Zone file serial number (date, sequence number, …)

Administrator’s mail (‘.’ instead Of ‘@’)

```
$TTL     86400

@        IN      SOA     toystory.movie.edu. al.movie.edu. (
                         2009020900  ; Serial
                         8H      ; Refresh after 8 hours
                         1h      ; Retry after 1 hour
                         1w      ; Expire after 1 week
                         60 )        ; negative caching TTL 1 min
```

Zone: ‘@’ is shorthand for current zone (“movie.edu”)

Zone transfer parameters

Examples from DNS and Bind, ed 5

Address Records – A and AAAA

- A – IPv4, AAAA – IPv6

- Same name can translate to multiple addresses
  - E.g. harp
- Several names can translate to same address
  - E.g. guitar and violin

```
violin  IN  A       192.249.249.2
guitar  IN  A       192.249.249.2
harp    IN  A       192.249.249.1
        IN  A       192.253.253.1
piano   IN  A       192.253.253.2
        IN  AAAA    2001:db80:1:2:3:4:567:891b
```

Blank means repeat

Canonical Name – CNAME

- Alias
- Several names for same address

```
piano   IN  CNAME      guitar
guitar  IN  A          192.249.249.3
flute   IN  CNAME      oboe
oboe    IN  A          192.249.249.1
        IN  A          192.253.253.1
```

Nameserver – NS

- At least one nameserver per zone
- Parent zone file includes NS entries for child zones
  - This is how delegation works

```
kth.se.              1722    IN  NS      nic.lth.se.
kth.se.              1722    IN  NS      a.ns.kth.se.
kth.se.              1722    IN  NS      ns2.chalmers.se.
kth.se.              1722    IN  NS      b.ns.kth.se.
```

Delegation

- Parent zone file includes NS entries for child zone
- Also contains IP address for child subdomain nameserver
  - *Glue record*
  - Might be needed in order to reach the subdomain’s nameserver

Delegation of “child.example.net” In the zone file for “example.net”:

```
child.example.net.     IN  NS      ns.child.example.net.
ns.child.example.net.  IN  A       11.2.3.4
```

Mail Exchange – MX

- Mail server for a domain
  - Where to send email for recipients within that domain

Preference (cost, distance, ...) – lower value means higher preference

```
google.com.    600 IN  MX  30 alt2.aspmx.l.google.com.
google.com.    600 IN  MX  40 alt3.aspmx.l.google.com.
google.com.    600 IN  MX  50 alt4.aspmx.l.google.com.
google.com.    600 IN  MX  10 aspmx.l.google.com.
google.com.    600 IN  MX  20 alt1.aspmx.l.google.com.
```

MX Records

- Not how it is currently done at KTH

```
$ dig +short kth.se mx
10 mx.kth.se.

$ dig +short mx.kth.se
130.237.48.97
130.237.48.98
130.237.32.140
```

Pointer – PTR

- Appears in arpa top-level zones
- Maps address to names

```
5.24.71.192.in-addr.arpa.   IN PTR  xen.netlab.csc.kth.se.
a.0.4.c.3.4.e.f.f.f.0.e.0.6.2.0.1.1.0.1.3.0.0.0.0.4.0.2.1.0.0.2.ip6.arpa. \
                            IN PTR  xen.netlab.csc.kth.se.
```

Root Hints File

- How does a resolving name server (such as the local DNS server) know where to start?
- Pre-configured with Root Hints file
  - Contains the root servers
  - Published by IANA
    - http://www.iana.org/domains/root/files

```
; FORMERLY AOS.ARL.ARMY.MIL
;
.                        3600000      NS    H.ROOT-SERVERS.NET.
H.ROOT-SERVERS.NET.      3600000      A     128.63.2.53
H.ROOT-SERVERS.NET.      3600000      AAAA  2001:500:1::803F:235
;
; FORMERLY NIC.NORDU.NET
;
.                        3600000      NS    I.ROOT-SERVERS.NET.
I.ROOT-SERVERS.NET.      3600000      A     192.36.148.17
I.ROOT-SERVERS.NET.      3600000      AAAA  2001:7FE::53
;
; OPERATED BY VERISIGN, INC.
;
.                        3600000      NS    J.ROOT-SERVERS.NET.
J.ROOT-SERVERS.NET.      3600000      A     192.58.128.30
J.ROOT-SERVERS.NET.      3600000      AAAA  2001:503:C27::2:30
```

Summary

- Domain name space organized in hierarchy
  - Generic domains, country domains, inverse domain
- Database distributed over name servers
  - Root server, TLD servers, authoritative servers
- Local DNS server performs (iterative) resolution on behalf of clients
- Name servers are responsible for zones
  - Responsibilities are distributed through delegations
- Supports different kinds of queries
  - A, AAAA, NS, PTR, MX, …
- BIND DNS software
  - Zone file definitions

Not Covered

- Compression
- Header details
- Dynamic DNS
  - Enables hosts to automatically update zone file when addresses changes
- DNSSEC, DNS security
  - Authentication