CS321: Computer Networks

DNS

Dr. Manas Khatua
Assistant Professor
Dept. of CSE
IIT Jodhpur
E-mail: manaskhatua@iitj.ac.in

DNS - Internet's Directory Service

- Just as humans can be identified in many ways, so too can Internet hosts.
  - Hostname (e.g., gmail.co.in, iitj.ac.in)
    - these are mnemonic, user friendly for Humans
  - IP Address (e.g., 121.7.106.83, 172.17.0.10)
    - these are structured numeric digits, user friendly for Routers
- The Internet needs to have a directory system that can map a name to an address.
- The Internet is so huge today, a central directory system cannot hold all the mapping.
- A better solution - distribute the directory information among many computers in the world.
- The host that needs mapping can contact the closest computer holding the needed information.
- This method is used by the **Domain Name System (DNS)**.

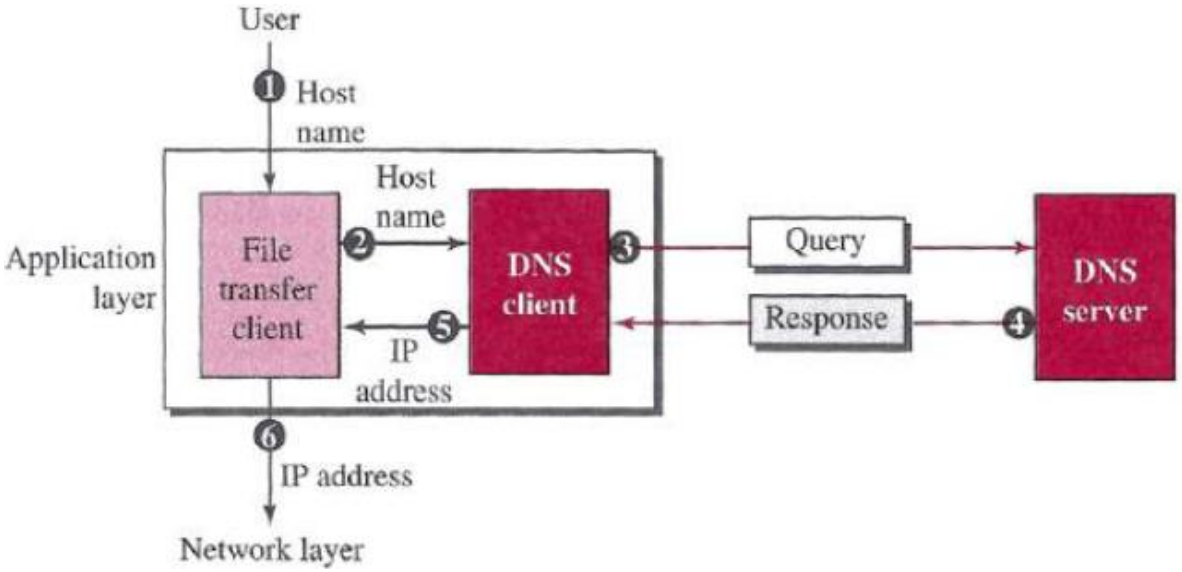
Cont…

- The DNS is a combination of :
  - a distributed database implemented in a hierarchy of **DNS servers**, and
  - an application-layer protocol that allows hosts to query the distributed database

- Let the purpose of accessing the Internet is to make a connection between the file transfer client and server,
- but before this can happen, another connection needs to be made between the DNS client and DNS server

- DNS protocol runs over UDP and uses port 53.

- The DNS servers are running the Berkeley Internet Name Domain (BIND) software



Cont…

- Design for DNS:
  - Centralized
  - Distributed

- The problems with a centralized design include:
  - A single point of failure: DNS server crashes, so does the entire Internet!
  - Traffic volume: A single DNS server would have to handle all DNS queries generated from hundreds of millions of hosts
  - Distant centralized database: A single DNS server cannot be “close to” all the querying clients.
  - Maintenance: The single DNS server would have to keep records for all Internet hosts. Management of it becomes very difficult!

Cont…

- DNS provides a few other important services in addition to translating hostnames to IP addresses:
  - Host aliasing: relay1.west-coast.enterprise.com could have, say, two aliases such as enterprise.com and www.enterprise.com
  - Mail server aliasing: the canonical hostname of the Hotmail server might be something like relay1.west-coast.hotmail.com but the mail server is simply hotmail.com
  - Load distribution: used to perform load distribution among replicated servers. For replicated servers, a set of IP addresses is thus associated with one canonical hostname.

Name Space

- the names must be unique because the addresses are unique.

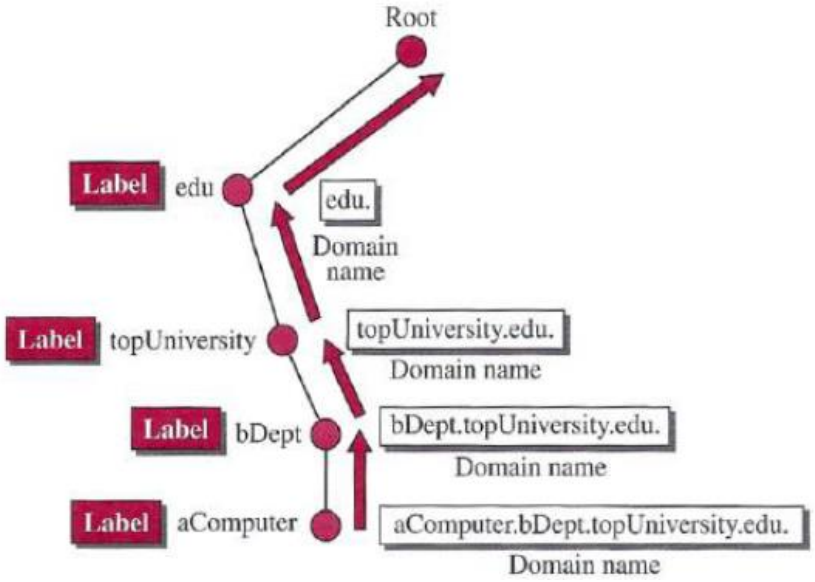
- A name space that maps each address to a unique name can be organized in two ways:
  - flat
  - hierarchical

- *flat name space*
  - a name is assigned to an address
  - a name is a sequence of characters without structure
  - The names may or may not have a common section

  - Disadvantage: it cannot be used in a large system such as the Internet because it must be centrally controlled to avoid ambiguity and duplication

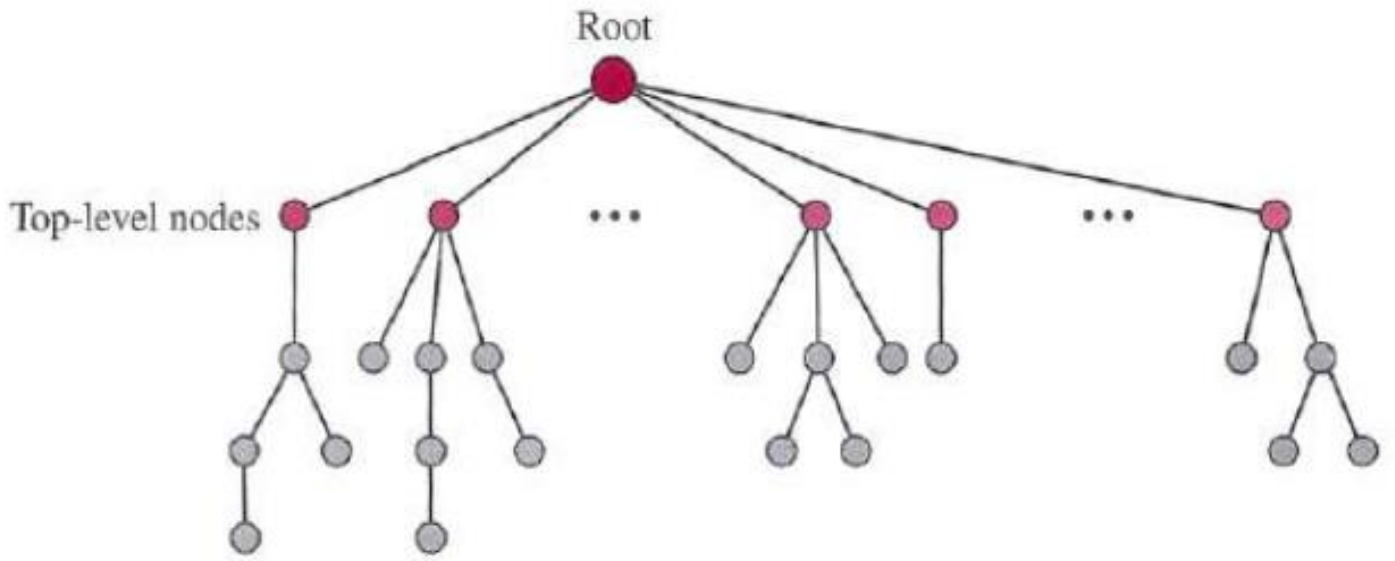
Cont…

- *hierarchical name space:* each name is made of several parts
  - the first part can define the nature of the organization
  - the second part can define the name of an organization
  - the third part can define departments in the organization
- *Advantages*
  - the authority to assign and control the name spaces can be decentralized.
  - A central authority can assign the part of the name. E.g, name & nature of the organization Rest of the name can be assigned by the organization itself



Domain Name Space

- the names are defined in an inverted-tree structure with the root at the top.



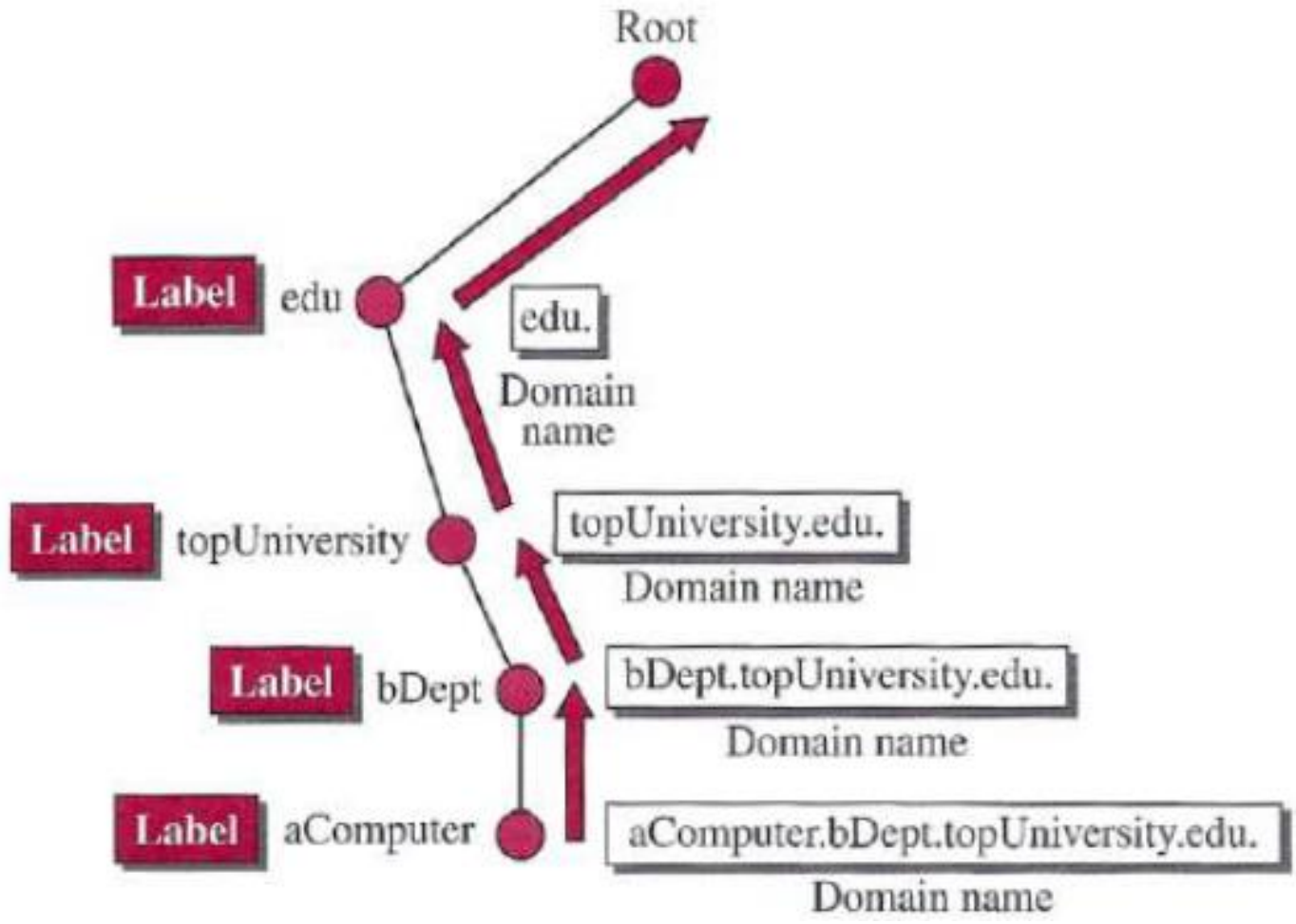
Cont…

- *Label:*
  - Each node in the tree has a label, which is a string with a maximum of 63 characters.
  - The root label is a null string (empty string).

- *Domain Name:*
  - Each node in the tree has a domain name.
  - A full domain name is a sequence of labels separated by dots (.)
  - The domain names are always read from the node up to the root.
  - The last label is the label of the root (null).

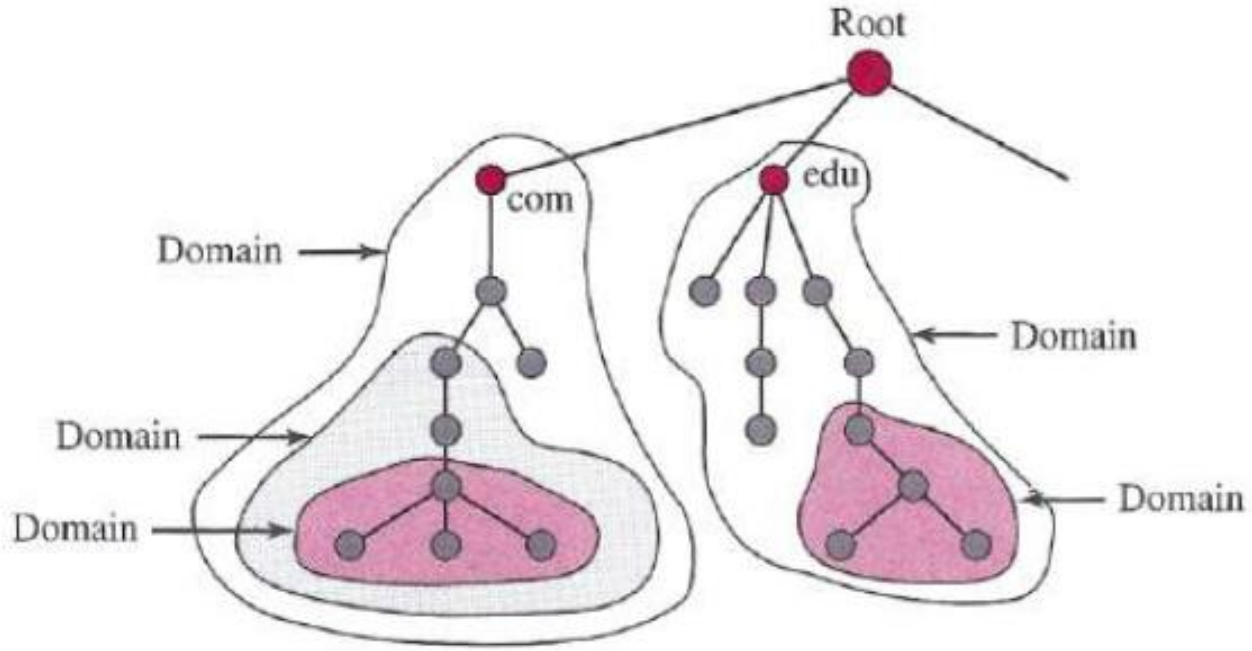
- Fully qualified domain name (FQDN):
  - If a label is terminated by a null string.
  - Else, it is Partially qualified domain name (PQDN)

Cont…


Root
Label
edu
edu.
Domain name
Label
topUniversity
topUniversity.edu.
Domain name
Label
bDept
bDept.topUniversity.edu.
Domain name
Label
aComputer
aComputer.bDept.topUniversity.edu.
Domain name

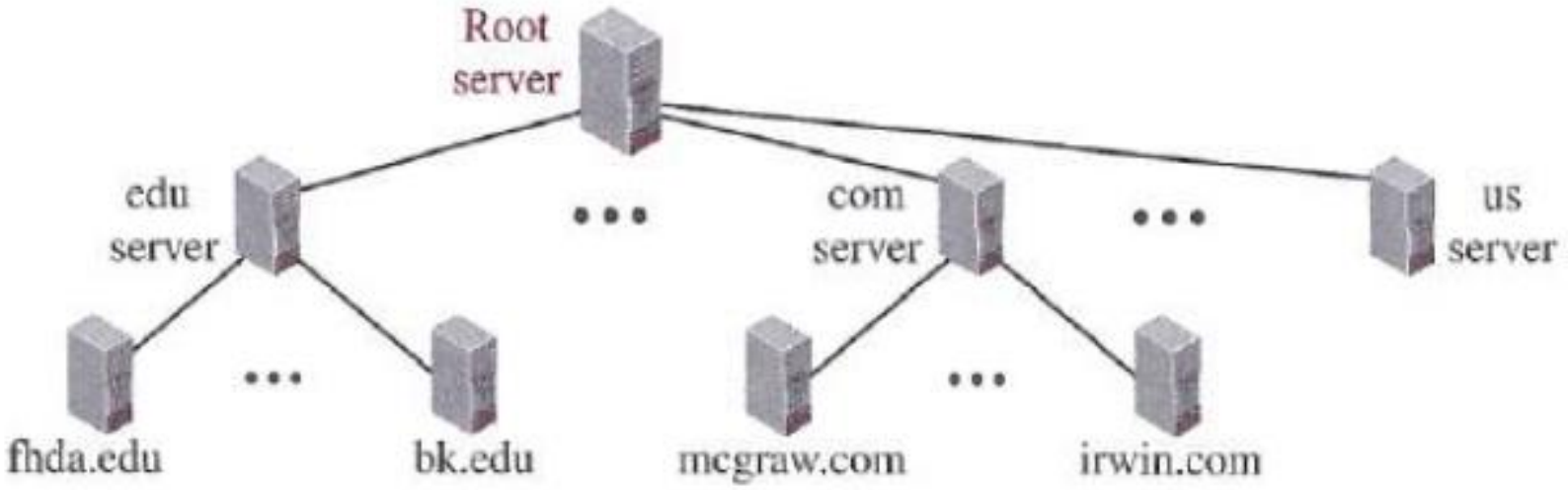
Domain

- A domain is a subtree of the domain name space



Distribution of Name Space

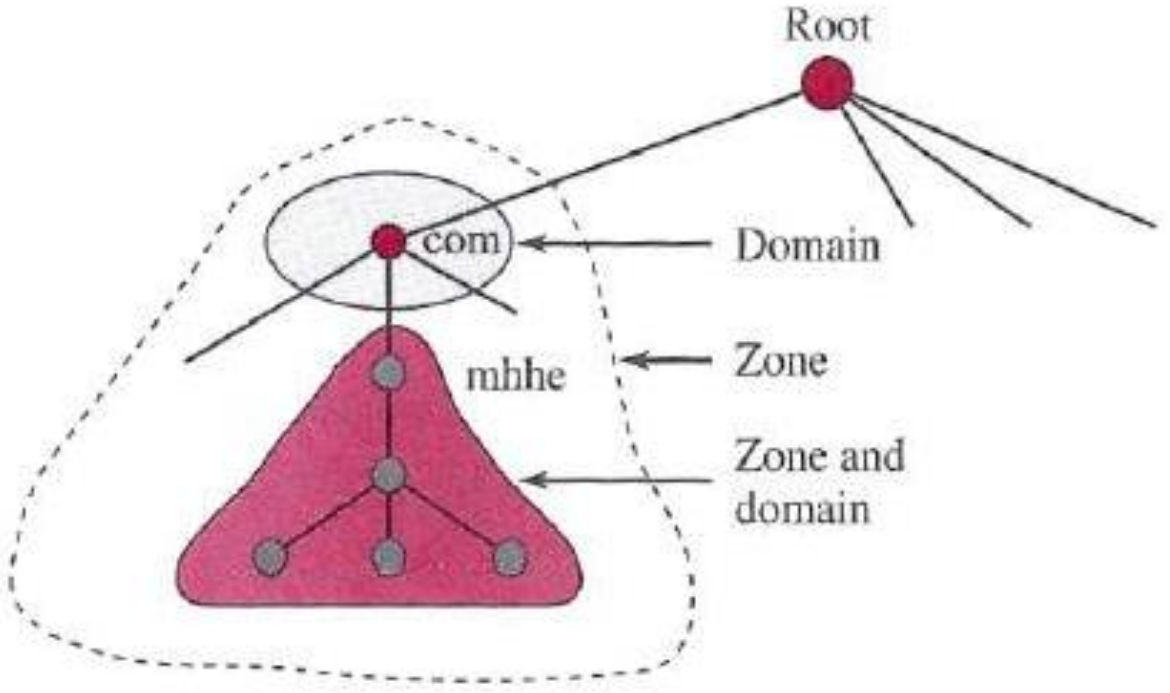
- The information contained in the domain name space must be stored.
- It is very inefficient and also not reliable to have just one computer store such a huge amount of information
- Soln: *Many DNS Servers following a hierarchy*



Cont…

- Zone: What a server is responsible for or has authority over is called a zone.

- A root server is a server whose zone consists of the whole tree.



DNS in the Internet

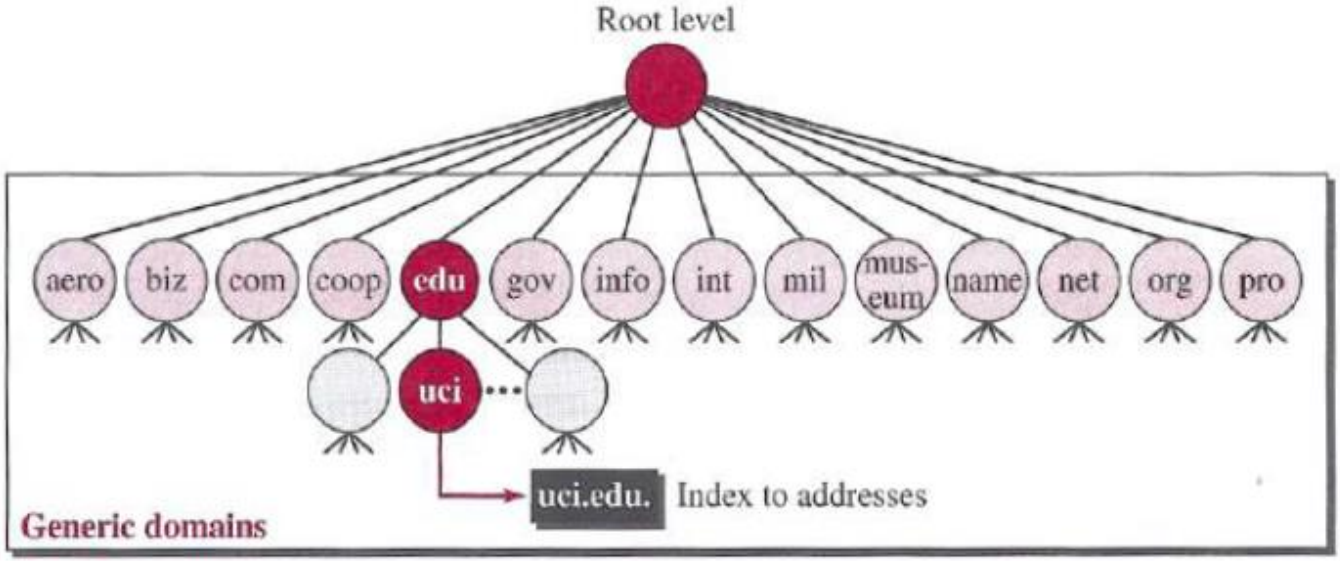
- DNS is a protocol that can be used in different platforms.

- In the Internet, the domain name space (tree) was originally divided into three different sections:
  - generic domains
  - country domains
  - inverse domains

Note: The inverse domains are now deprecated.

Generic Domains

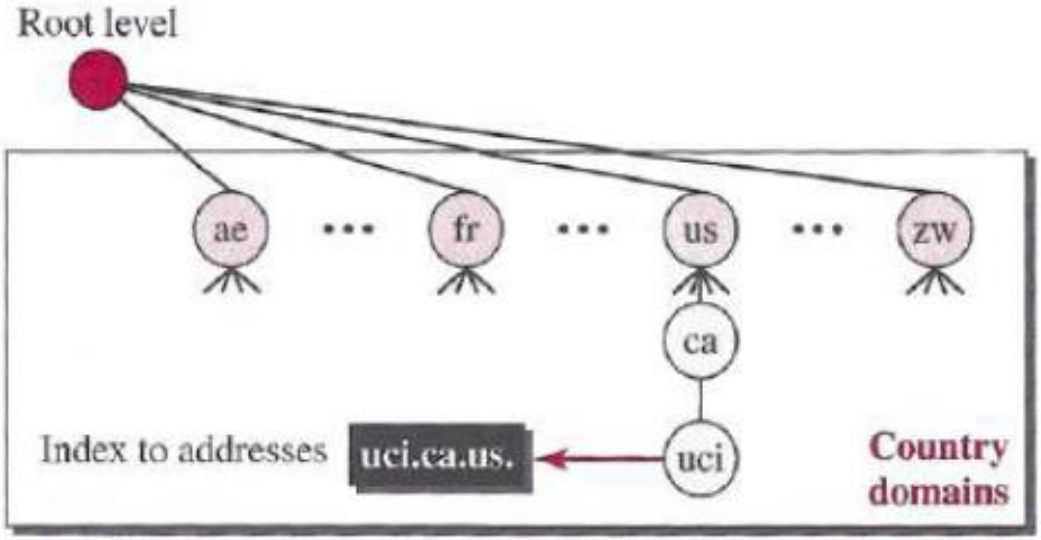
- The generic domains define registered hosts according to their generic behavior.



Label	*Description*	*Label*	*Description*
aero	Airlines and aerospace	**int**	International organizations
biz	Businesses or firms	**mil**	Military groups
com	Commercial organizations	**museum**	Museums
coop	Cooperative organizations	**name**	Personal names (individuals)
edu	Educational institutions	**net**	Network support centers
gov	Government institutions	**org**	Nonprofit organizations
info	Information service providers	**pro**	Professional organizations

Country Domains

- The country domains section uses two-character country abbreviations.
- Second labels can be organizational, or they can be more specific national designations.
- E.g., The address *uci.ca.us.* can be translated to University of California, Irvine, in the state of California in the United States.



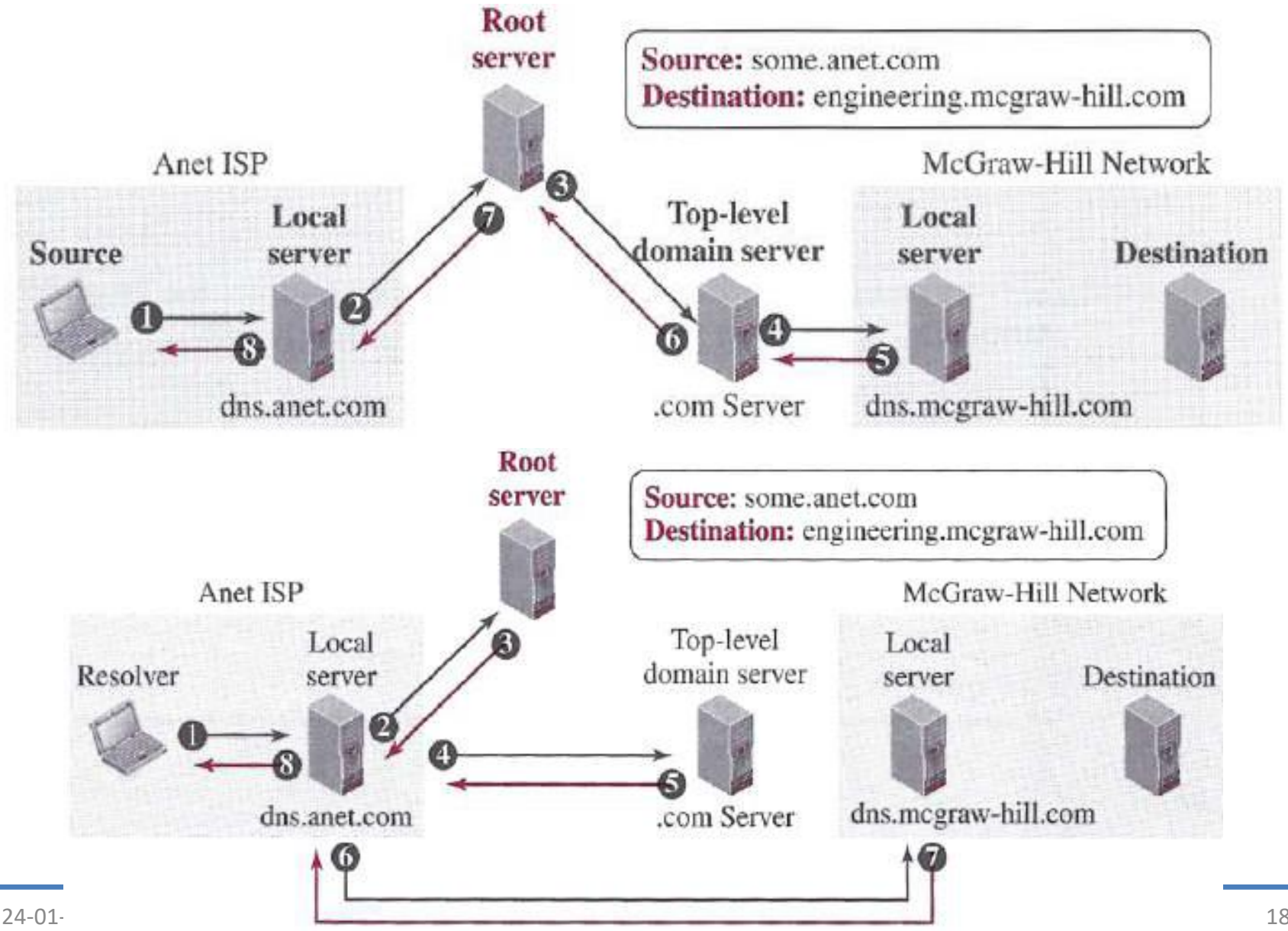
Name-Address Resolution

- Mapping a name to an address is called *name-address resolution*
- DNS is designed as a client-server application.

- The resolver (DNS client) accesses the closest DNS server with a mapping request.
- If the server has the information, it satisfies the resolver;
- otherwise, it either refers the resolver to other servers or asks other servers to provide the information.

- A resolution process can be
  - Recursive
  - Iterative

Recursive vs Iterative Resolution

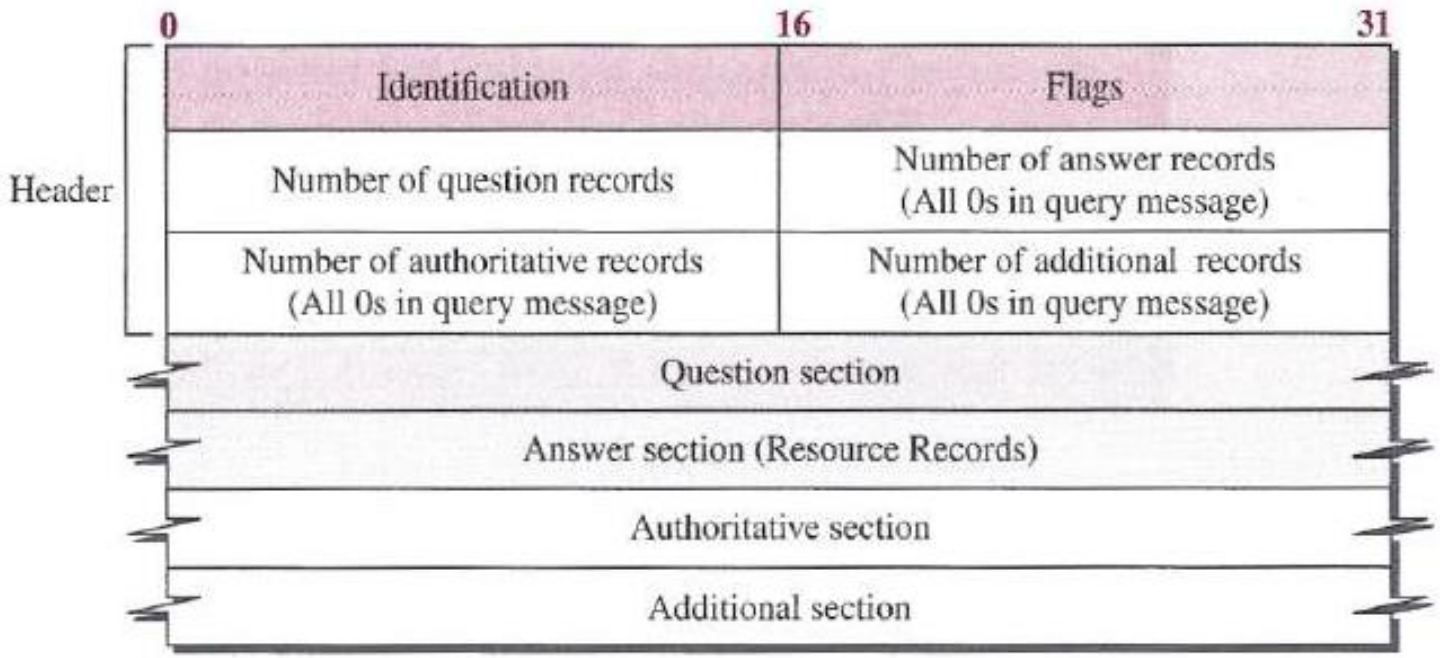


Caching

- Each time a server receives a query for a name that is not in its domain, it needs to search its database for a server IP address.
- Reduction of this search time would increase efficiency.
- DNS handles this with a mechanism called *caching*
- Caching speeds up resolution, but it can also be problematic.
- If a server caches a mapping for a long time, it may send an outdated mapping to the client.
- To counter this, TTL (time-to-live) based technique is used.

DNS Messages

- The identification field is used by the client to match the response with the query.
- The flag field defines whether the message is a query or response.



Note:
The query message contains only the question section.
The response message includes the question section,
the answer section, and possibly two other sections.

Cont…

- DNS can use either UDP or TCP.
- In both cases the well-known port used by the server is port 53.

- Example:
  - In UNIX and Windows, the *nslookup* utility can be used to retrieve address/name mapping.

```
$nslookup www.forouzan.biz
Name:  www.forouzan.biz
Address: 198.170.240.179
```

Thanks!