DNS Domain Name System

Domain names and IP addresses

- People prefer to use easy-to-remember names instead of IP addresses

- Domain names are alphanumeric names for IP addresses e.g., neon.ece.utoronto.ca, www.google.com, ietf.org
- The domain name system (DNS) is an Internet-wide distributed database that translates between domain names and IP addresses

- **How important is DNS?**

  Imagine what happens when the local DNS server is down.

Before there was DNS ….

…. there was the HOSTS.TXT file

- Before DNS (until 1985), the name-to-IP address was done by downloading a single file (hosts.txt) from a central server with FTP.
  - Names in hosts.txt are not structured.
  - The hosts.txt file still works on most operating systems. It can be used to define local names.

Domain Name System

Problems of centralized DNS -

- Single point of failure
- Traffic volume
- Distant centralized database
- Maintenance
- Does not scale

Domain Name System

Distributed database implemented in hierarchy of many name servers

Application-layer protocol

Runs over UDP and uses port 53

DNS Services

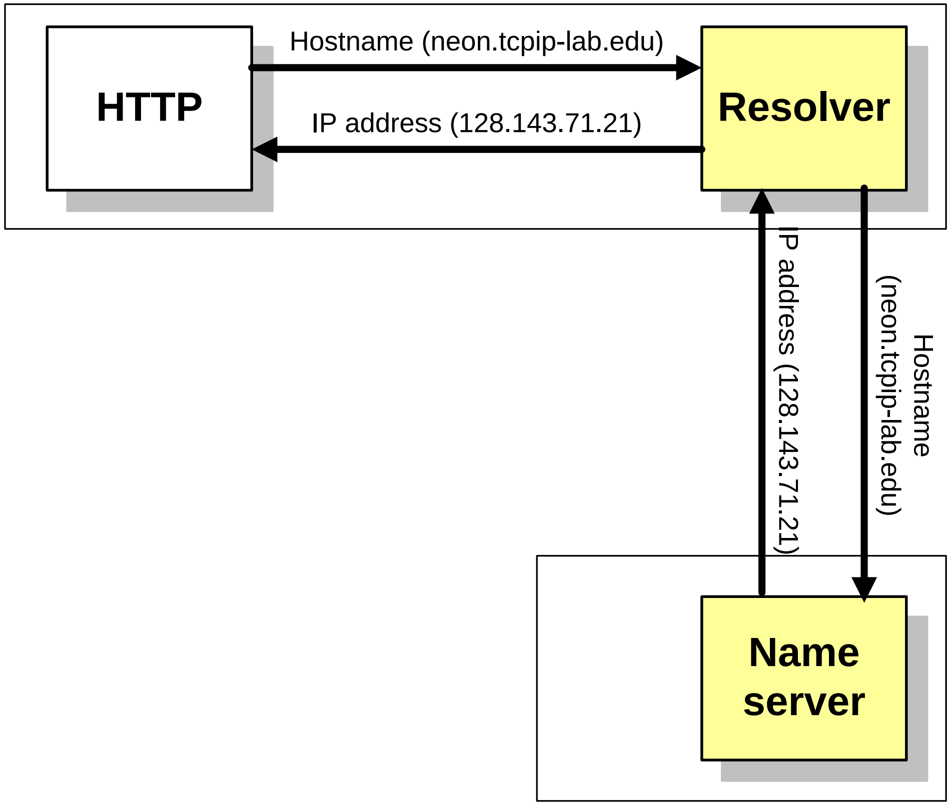
- Hostname to IP address translation
- Host aliasing
  - Canonical, alias names
- Mail server aliasing
- Load distribution
  - Replicated Web servers: set of IP addresses for one canonical name

Major Components

- Domain Name Space and Resource Records
    - specifications for a tree structured name space and data associated with the names
- Name Servers
    - Contains complete information about a subset of the domain space, and pointers to other name servers that can be used to lead to information from any part of the domain tree
    - An Authority for these parts of the name space
- Resolvers
    - extract information from name servers in response to client requests
    - typically a system routine that is directly accessible to user programs

Resolver and name server

1. An application program on a host accesses the domain system through a DNS client, called the **resolver**
2. Resolver contacts DNS server, called name server
3. DNS server returns IP address to resolver which passes the IP address to application


HTTP
Hostname (neon.tcpip-lab.edu)
IP address (128.143.71.21)
Resolver
IP address (128.143.71.21)
Hostname (neon.tcpip-lab.edu)
Name server

- Reverse lookups are also possible, i.e., find the hostname given an IP address

Design principle of DNS

Flat Name Space

A name is assigned to an address

A name in this space is a sequence of characters without structure

The names may or may not have a common section

Must be centrally controlled to avoid ambiguity and duplication

Hierarchical Name Space

Each name is made of several parts

Authority to assign and control the name spaces can be decentralized

Design principle of DNS

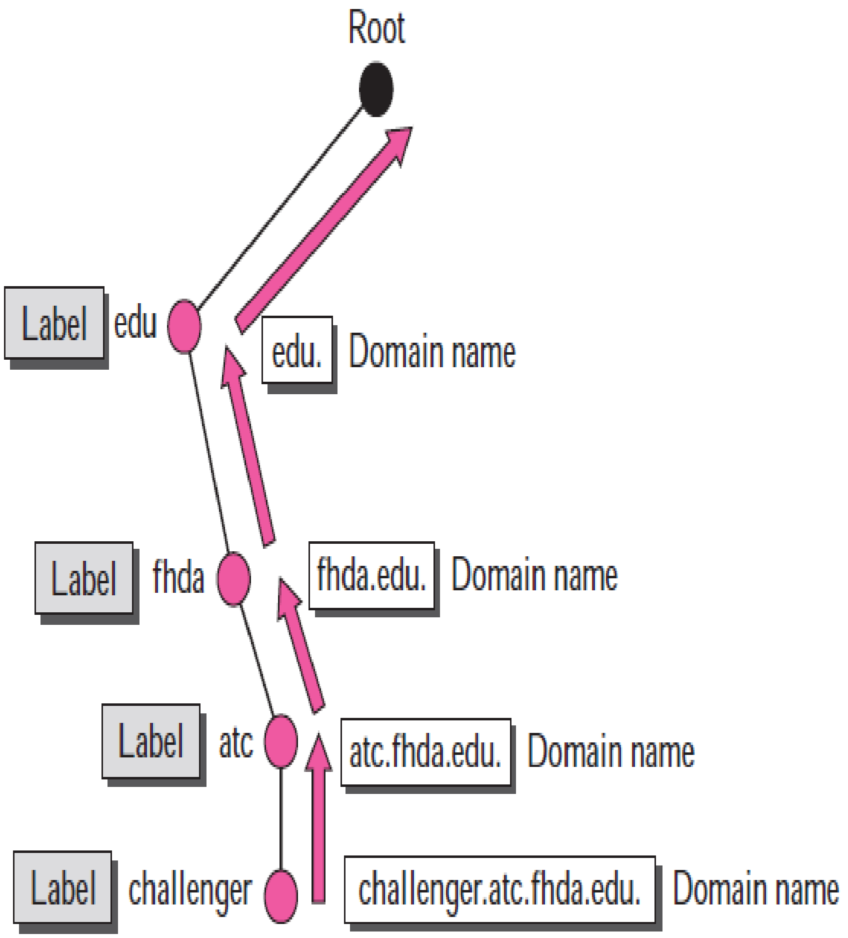
- The naming system on which DNS is based is a hierarchical and logical tree structure called the *domain namespace*.
- An organization obtains authority for parts of the name space, and can add additional layers of the hierarchy
- Names of hosts can be assigned without regard of location on a link layer network, IP network or autonomous system
- In practice, allocation of the domain names generally follows the allocation of IP address, e.g.,
  - All hosts with network prefix 128.143/16 may have domain name suffix jadavpur.edu.in
  - All hosts on network 128.143.136/24 are in the Computer Science and Engineering Department of Jadavpur University

Design principle of DNS

128 levels: level 0 (root) to level 127

Each node in the tree has a **label** (max. 63 characters)

The root label is a null string (empty string)



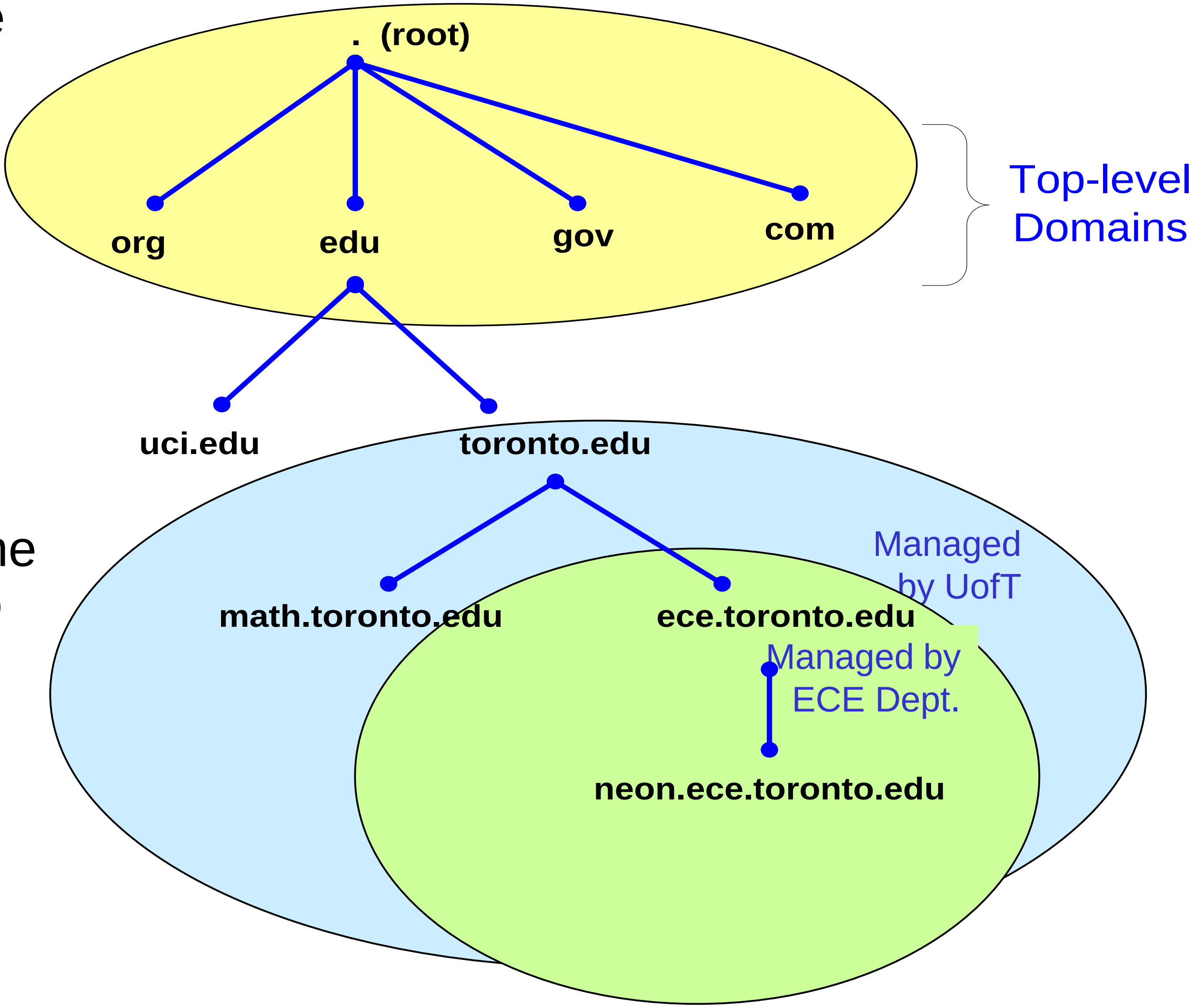
DNS Name hierarchy

DNS hierarchy can be represented by a tree

Root and top-level domains are administered by an Internet central name registration authority (ICANN)

Below top-level domain, administration of name space is delegated to organizations

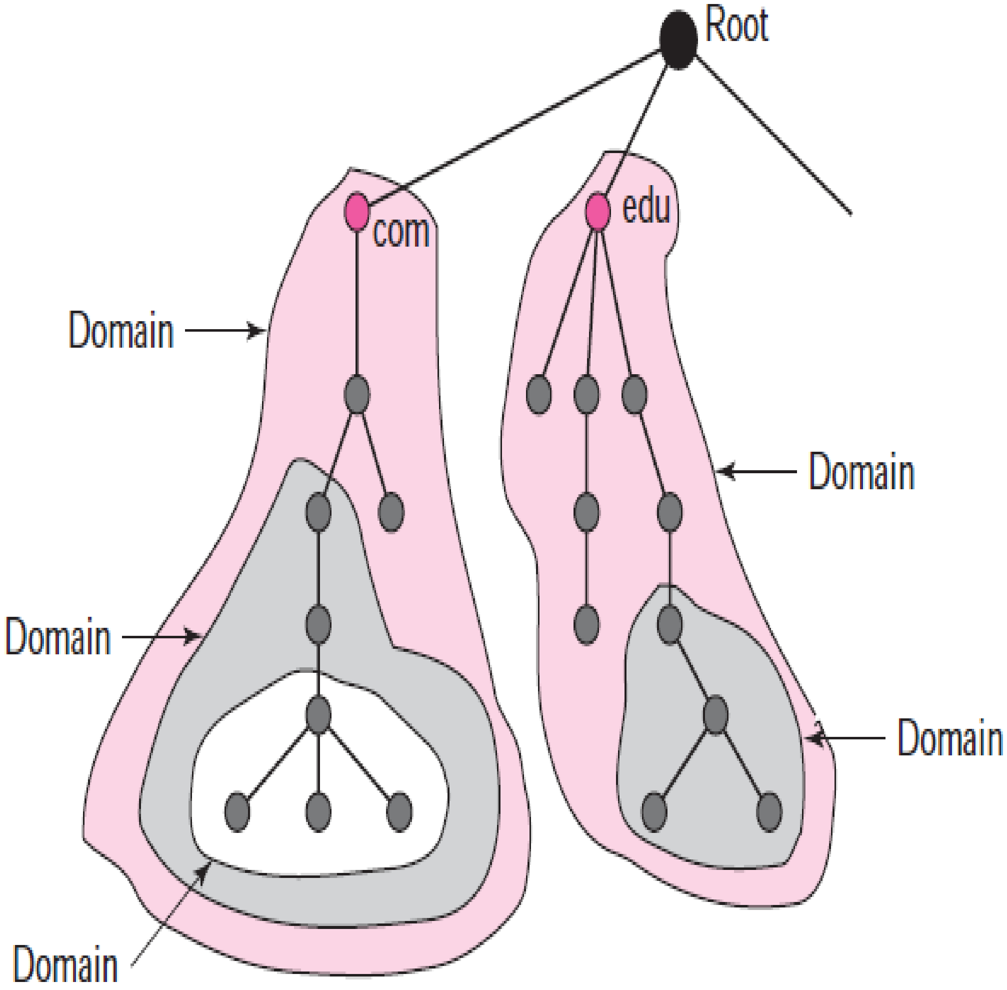
Each organization can delegate further



Domain name system

- Each node in the DNS tree represents a DNS name
- Each branch below a node is a DNS domain.
  - DNS domain can contain hosts or other domains (subdomains)

- Example:
  DNS domains are
  ., edu, virginia.edu, cs.virginia.edu



Domain names

- Hosts and DNS domains are named based on their position in the domain tree
- Every node in the DNS domain tree can be identified by a unique Fully Qualified Domain Name (FQDN). The FQDN gives the position in the DNS tree.

cs.virginia.edu or cs.virginia.edu.

- A FQDN consists of labels (“cs”,“virginia”,”edu”) separated by a period (“.”)
- There can be a period (“.”) at the end.
- Each label can be up to 63 characters long
- FQDN contains characters, numerals, and dash character (“-”)
- FQDNs are not case-sensitive

Domain names

- Fully Qualified Domain Name (FQDN) (or absolute domain name)
  - If a label is terminated by a null string
  - the full domain name for “C” is “C.B.A.” where “A” is a top-level domain.
- Partially Qualified Domain Name (PQDN)
  - If a label is not terminated by a null string
  - the name only partially specifies the location of the device. By definition, a PQDN is ambiguous.
  - one can only use a PQDN within the context of a particular parent domain, whose absolute domain name is known.
    - For example, if we have the PQDN “Z” within the context of the FQDN “Y.X.”, we know the FQDN for “Z” is “Z.Y.X.”

Top-level domains

- Three types of top-level domains:
  - Organizational: 3-character code indicates the function of the organization
    - Used primarily within the US
    - Examples: gov, mil, edu, org, com, net
  - Geographical: 2-character country or region code
    - Examples: in, us, jp, de
  - Reverse domains: A special domain (in-addr.arpa) used for IP address-to-name mapping

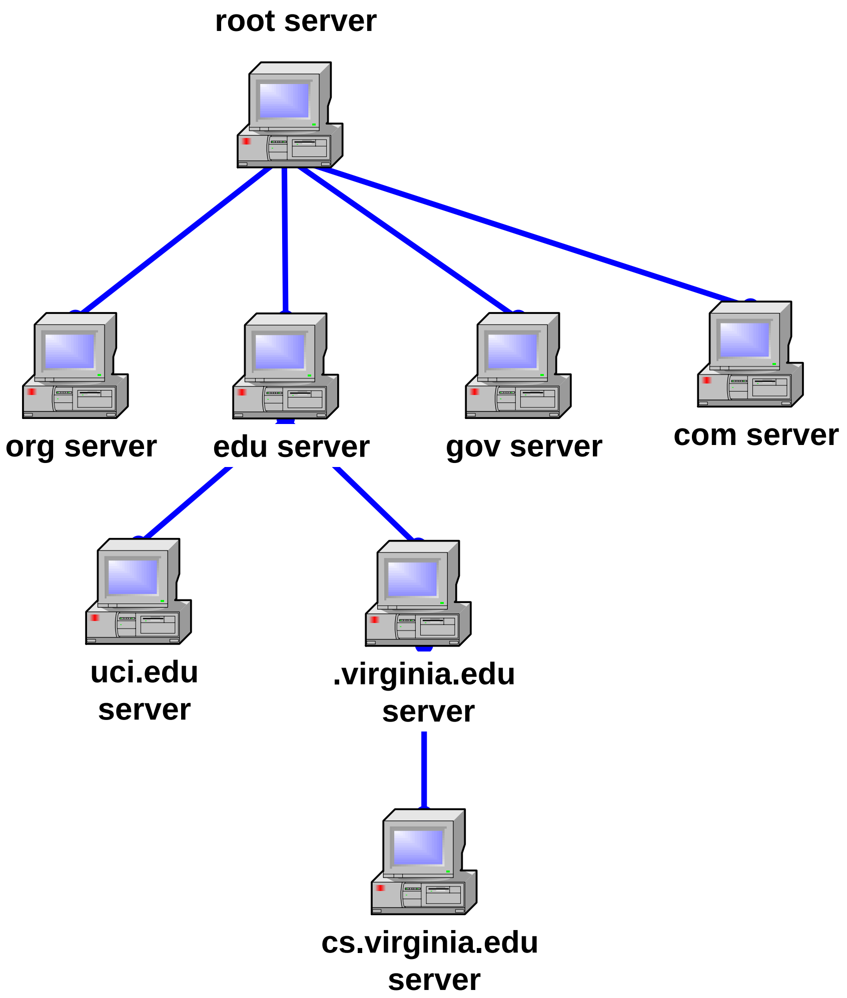
There are more than 200 top-level domains.

Organizational top-level domains

com	Commercial organizations
edu	Educational institutions
gov	Government institutions
int	International organizations
mil	U.S. military institutions
net	Networking organizations
org	Non-profit organizations

Hierarchy of name servers

- The resolution of the hierarchical name space is done by a hierarchy of name servers
- Each server is responsible (authoritative) for a contiguous portion of the DNS namespace, called a zone.
- Zone is a part of the subtree
- DNS server answers queries about hosts in its zone



Hierarchy of name servers

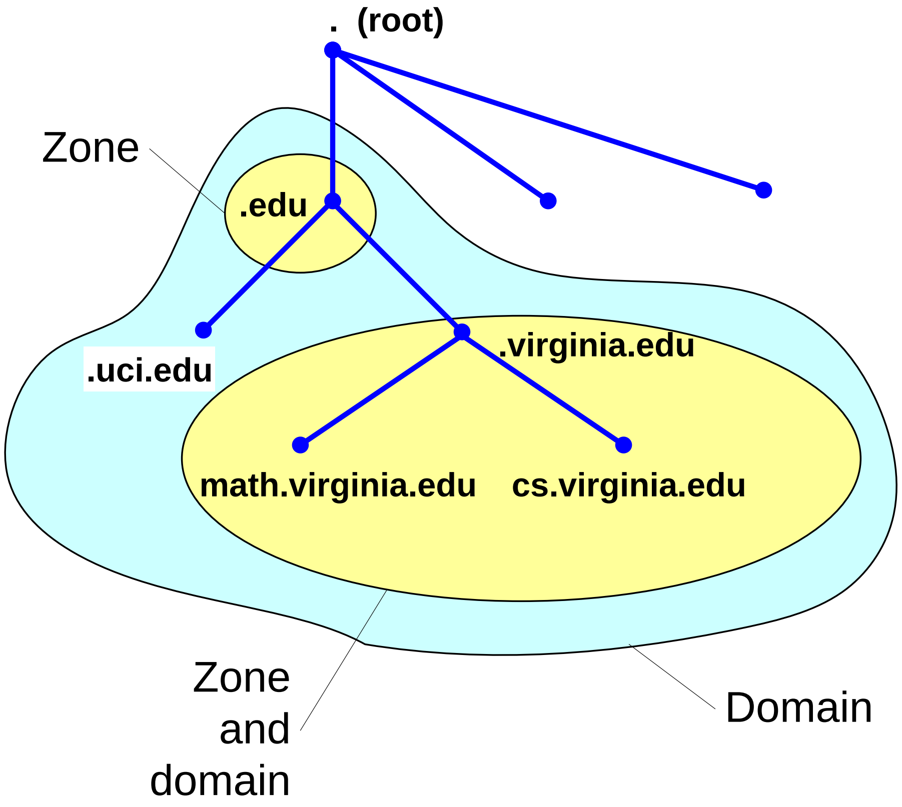
- Root Name Server
  - Its zone consists of the whole tree
- Primary Name Server
  - Stores a file about the zone for which it is an authority
  - It is responsible for creating, maintaining, and updating the zone file
  - It stores the zone file on a local disk
- Secondary Server
  - Transfers the complete information about a zone from another server (primary or secondary)
- Primary and secondary servers are both authoritative for the zones they serve

DNS domain and zones

- Each zone is anchored at a specific domain node, but zones are not domains.

- *A DNS domain* is a branch of the namespace
- A zone is a portion of the DNS namespace generally stored in a file (It could consist of multiple nodes)

- A server can divide its zone into parts and delegate it to other servers



Primary and secondary name servers

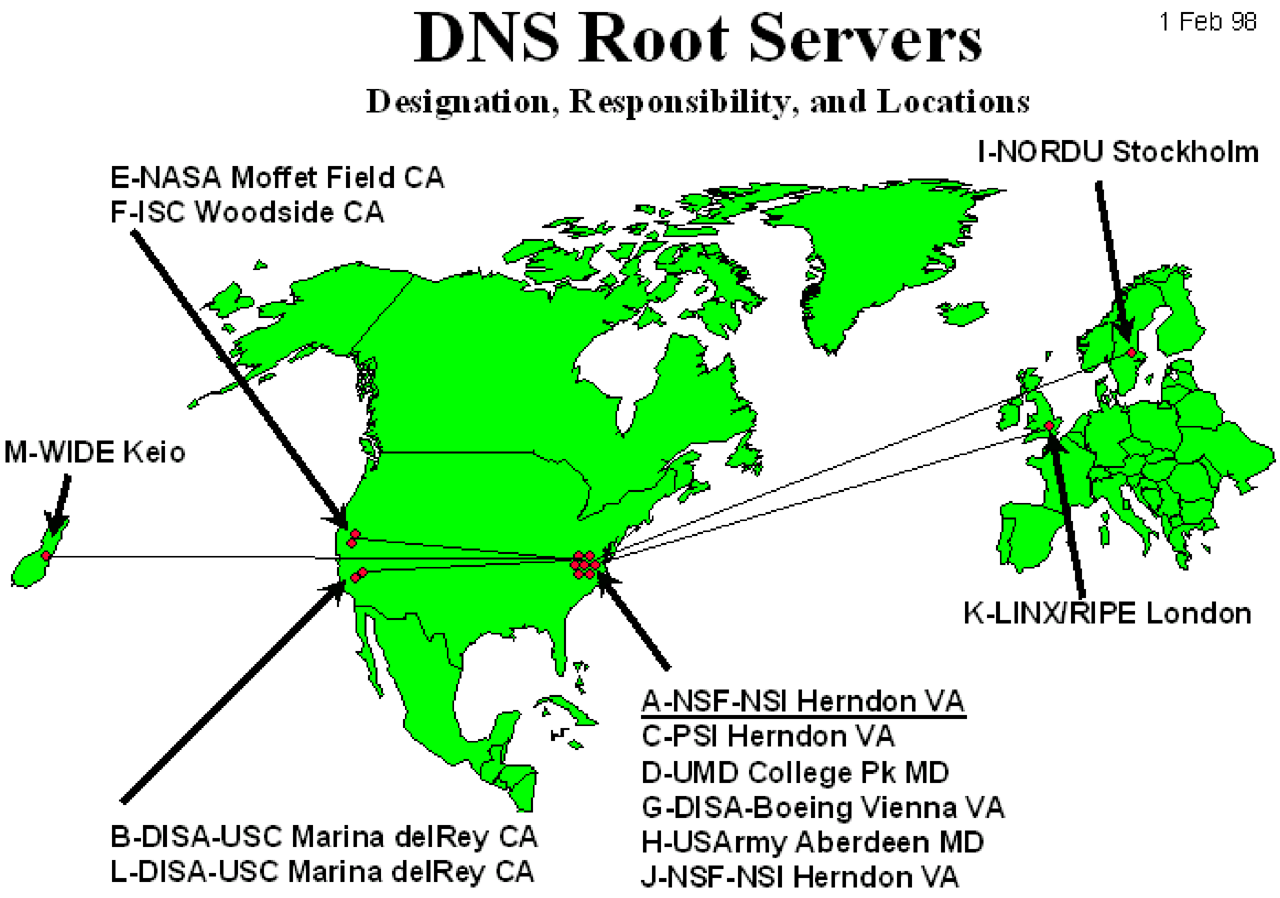
- For each zone, there must be a primary name server and a secondary name server
  - The primary server (master server) maintains a zone file which has information about the zone. Updates are made to the primary server
  - The secondary server copies data stored at the primary server.

Adding a host:

- When a new host is added (“alpha.cs.jaduniv.edu.in”) to a zone, the administrator adds the IP information on the host (IP address and name) to a configuration file on the primary server

Root name servers

- The root name servers know how to find the authoritative name servers for all top-level zones.
- There are only 13 root name servers
- Root servers are critical for the proper functioning of name resolution



Addresses of root servers

A.ROOT-SERVERS.EDU.	(formerly NS.INTERNIC.NET)	10.0.2.32
A.ROOT-SERVERS.NET.	(formerly NS1.ISI.EDU)	198.41.0.4
B.ROOT-SERVERS.NET.	(formerly C.PSI.NET)	128.9.0.107
C.ROOT-SERVERS.NET.	(TERP.UMD.EDU)	192.33.4.12
D.ROOT-SERVERS.NET.	(NS.NASA.GOV)	128.8.10.90
E.ROOT-SERVERS.NET.	(NS.ISC.ORG)	192.203.23
F.ROOT-SERVERS.NET.	(NS.NIC.DDN.MIL)	192.5.5.241
G.ROOT-SERVERS.NET.	(AOS.ARL.ARMY.MIL)	192.112.36.4
H.ROOT-SERVERS.NET.	(NIC.NORDU.NET)	128.63.2.53
I.ROOT-SERVERS.NET.	(at NSI (InterNIC))	192.36.148.17
J.ROOT-SERVERS.NET.	(operated by RIPE NCC)	198.41.0.10
K.ROOT-SERVERS.NET.	(at ISI (IANA))	193.0.14.129
L.ROOT-SERVERS.NET.	(operated by WIDE, Japan)	198.32.64
M.ROOT-SERVERS.NET.		202.12.27.33

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

Client wants IP for www.amazon.com

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

TLD and Authoritative Servers

- Top-level domain (TLD) servers:
  - Responsible for com, org, net, edu etc., and all top-level country domains uk, fr, ca, jp, in
  - Network Solutions maintains servers for .com TLD
  - Educause for .edu TLD
- 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”
- When host makes DNS query, query is sent to its local DNS server
  - Acts as proxy, forwards query into hierarchy

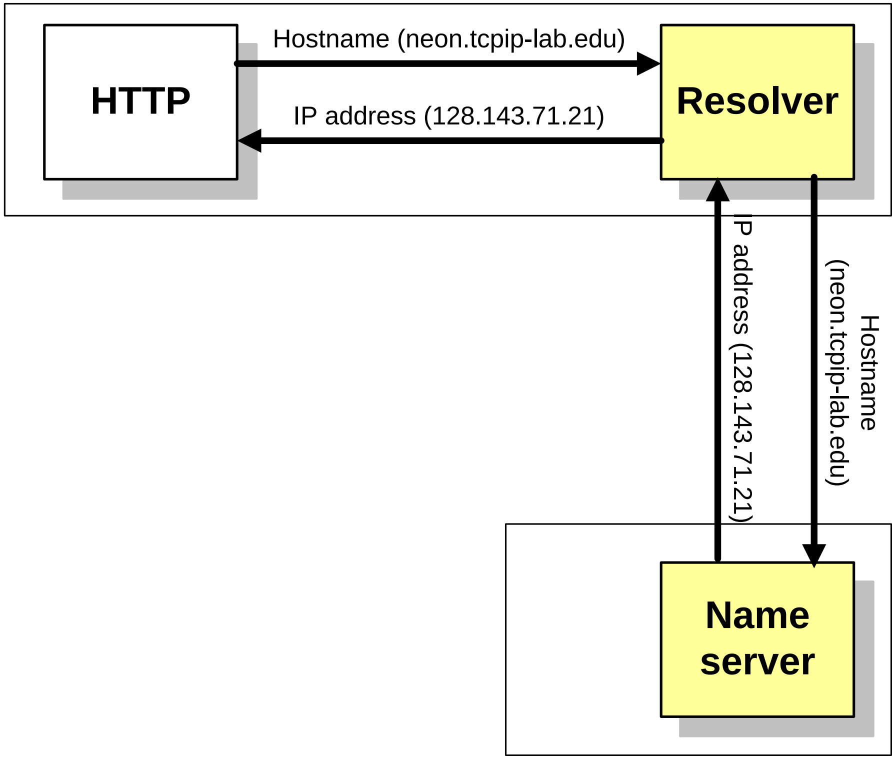
Authority and delegation

- Authority for the root domain is with the Internet Corporation for Assigned Numbers and Names (ICANN)
- ICANN delegates to accredited registrars (for gTLDs) and countries for country code top level domains (ccTLDs)
- Authority can be delegated further

- Chain of delegation can be obtained by reading domain name from right to left.
- Unit of delegation is a “zone”.

Domain name resolution

1. User program issues a request for the IP address of a hostname
2. Local resolver formulates a DNS query to the name server of the host
3. Name server checks if it is authorized to answer the query.
   a) If yes, it responds.
   b) Otherwise, it will query other name servers, starting at the root tree
4. When the name server has the answer it sends it to the resolver.


HTTP
Hostname (neon.tcpip-lab.edu)
IP address (128.143.71.21)
Resolver
IP address (128.143.71.21)
Hostname (neon.tcpip-lab.edu)
Name server

```
             Local Host                        |  Foreign
                                               |
+---------+               +----------+         |  +--------+
|         | user queries  |          |queries  |  |        |
|  User   |-------------->|          |---------|->|Foreign |
| Program |               | Resolver |         |  |  Name  |
|         |<--------------|          |<--------|--| Server |
|         | user responses|          |responses|  |        |
+---------+               +----------+         |  +--------+
                            |     A            |
            cache additions |     | references |
                            V     |            |
                          +----------+         |
                          |  cache   |         |
                          +----------+         |
```

A Simple Configuration of Query and Responses

```
             Local Host                        |  Foreign
                                               |
  +---------+                                  |
 /         /|                                  |
+---------+ |             +----------+         |  +--------+
|         | |             |          |responses|  |        |
|         | |             |   Name   |---------|->|Foreign |
|  Master |-------------->|  Server  |         |  |Resolver|
|  files  | |             |          |<--------|--|        |
|         |/              |          | queries |  +--------+
+---------+               +----------+         |
```

A primary name server acquires information about one or more zones by reading master files from its local file system, and answers queries about those zones that arrive from foreign resolvers.

```
                 Local Host                        |  Foreign
                                                   |
      +---------+                                  |
     /         /|                                  |
    +---------+ |             +----------+         |  +--------+
    |         | |             |          |responses|  |        |
    |         | |             |   Name   |---------|->|Foreign |
    |  Master |-------------->|  Server  |         |  |Resolver|
    |  files  | |             |          |<--------|--|        |
    |         |/              |          | queries |  +--------+
    +---------+               +----------+         |
                                A     |maintenance |  +--------+
                                |     +------------|->|        |
                                |      queries     |  |Foreign |
                                |                  |  |  Name  |
                                +------------------|--| Server |
                             maintenance responses |  +--------+
```

The name server periodically establishes a virtual connection to a foreign name server to acquire a copy of a zone file or to check that an existing copy has not changed.

```
             Local Host                        |  Foreign
                                               |
+---------+               +----------+         |  +--------+
|         | user queries  |          |queries  |  |        |
|  User   |-------------->|          |---------|->|Foreign |
| Program |               | Resolver |         |  |  Name  |
|         |<--------------|          |<--------|--| Server |
|         | user responses|          |responses|  |        |
+---------+               +----------+         |  +--------+
                            |     A            |
            cache additions |     | references |
                            V     |            |
                          +----------+         |
                          |  Shared  |         |
                          | database |         |
                          +----------+         |
                            A     |            |
  +---------+     refreshes |     | references |
 /         /|               |     V            |
+---------+ |             +----------+         |  +--------+
|         | |             |          |responses|  |        |
|         | |             |   Name   |---------|->|Foreign |
|  Master |-------------->|  Server  |         |  |Resolver|
|  files  | |             |          |<--------|--|        |
|         |/              |          | queries |  +--------+
+---------+               +----------+         |
                            A     |maintenance |  +--------+
                            |     +------------|->|        |
                            |      queries     |  |Foreign |
                            |                  |  |  Name  |
                            +------------------|--| Server |
                         maintenance responses |  +--------+
```

Shared database holds domain space data for the local name server and resolver.

The data is a mixture of authoritative data maintained by the periodic refresh operations of the name server and cached data from previous resolver requests.

Recursive and Iterative Queries

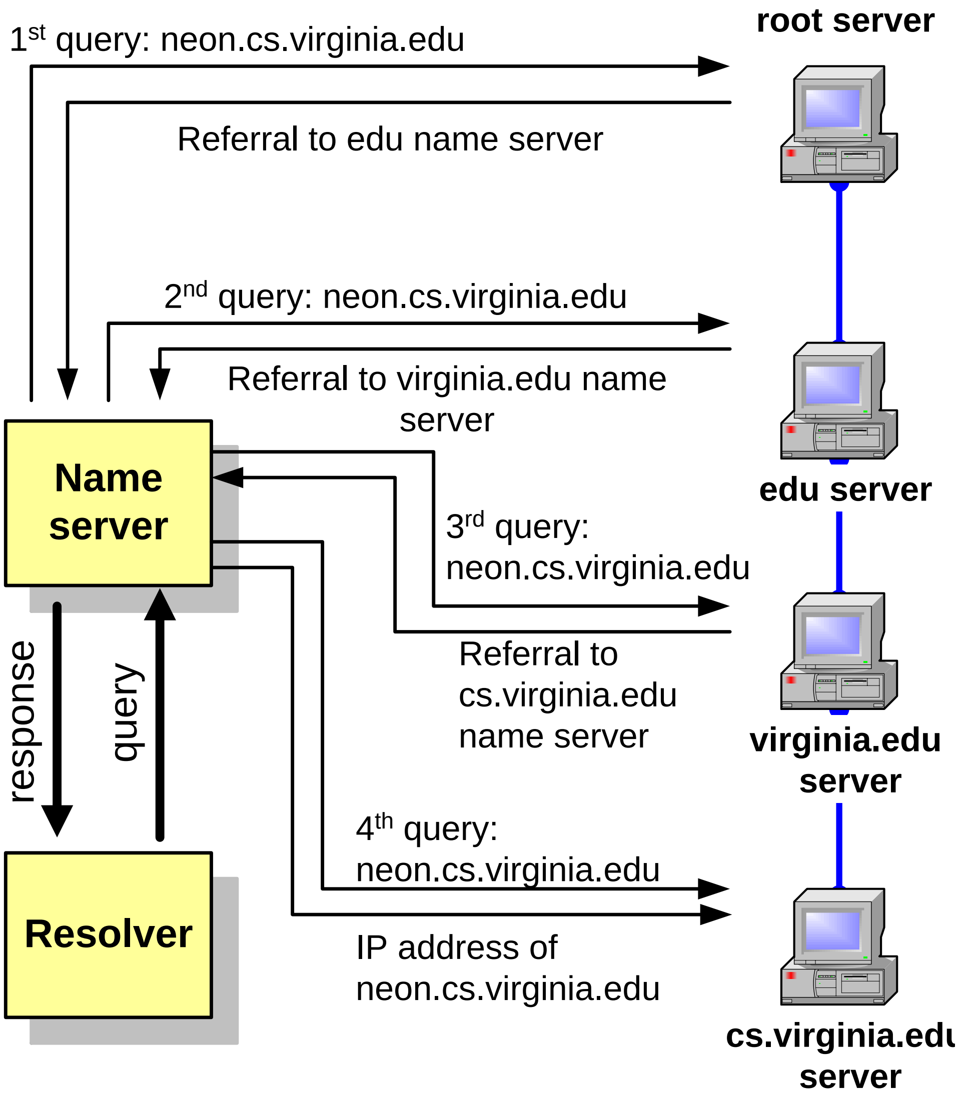
- There are two types of queries:
  - Recursive queries
  - Iterative (non-recursive) queries

- The type of query is determined by a bit in the DNS query

- Recursive query: When the name server of a host cannot resolve a query, the server issues a query to resolve the query
- Iterative queries: When the name server of a host cannot resolve a query, it sends a referral to another server to the resolver

Recursive queries

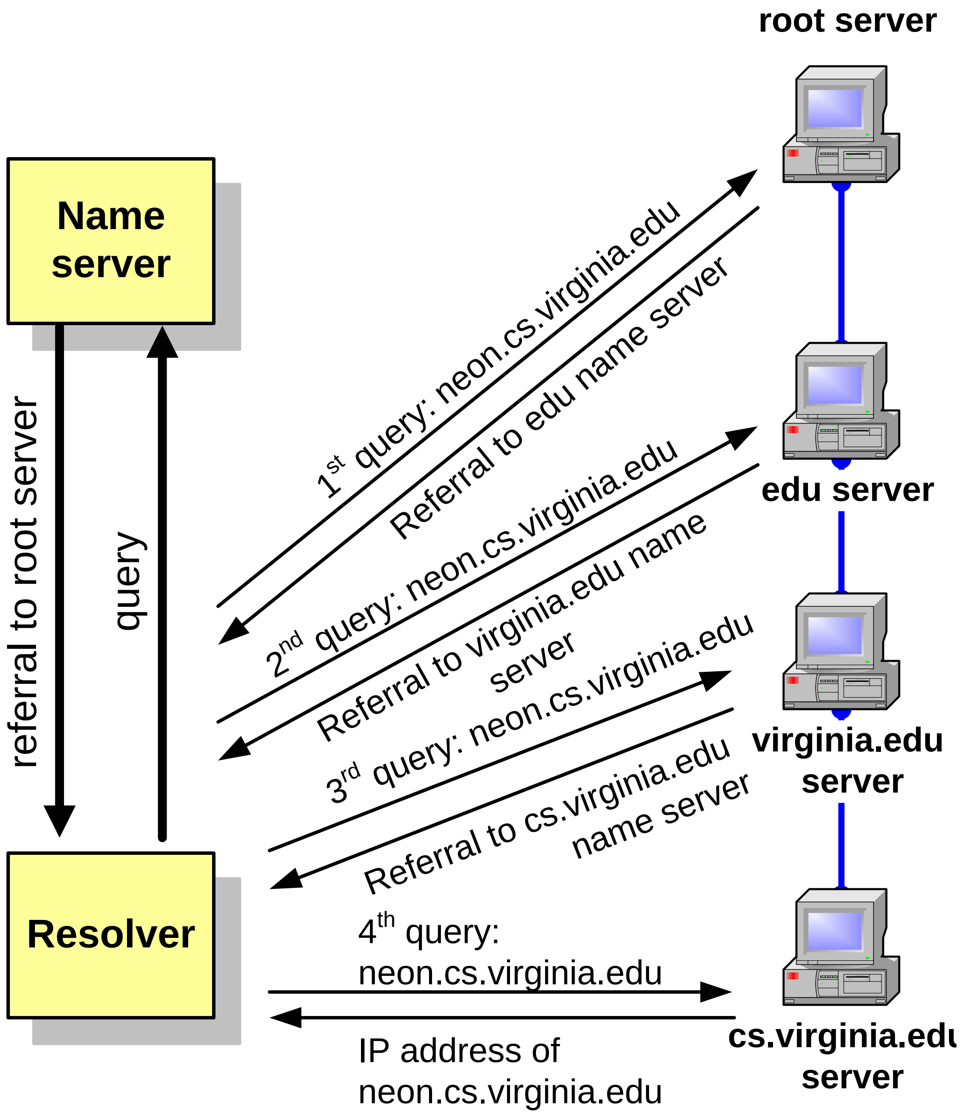
- In a recursive query, the resolver expects the response from the name server
- If the server cannot supply the answer, it will send the query to the "closest known" authoritative name server (here: In the worst case, the closest known server is the root server)
- The root sever sends a referral to the "edu" server. Querying this server yields a referral to the server of "virginia.edu"
- … and so on

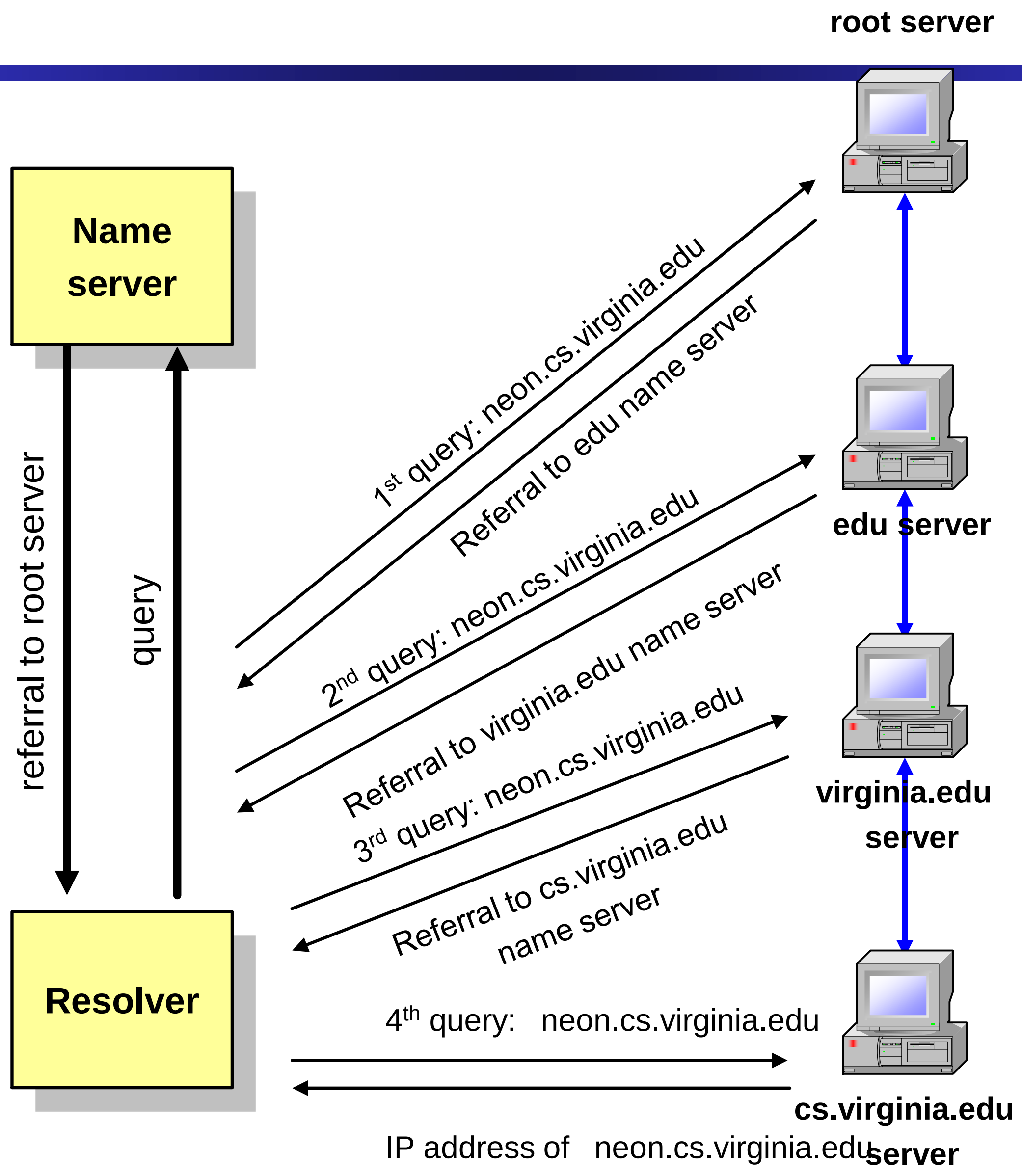

1st query: neon.cs.virginia.edu
root server
Referral to edu name server
2nd query: neon.cs.virginia.edu
Referral to virginia.edu name server
Name server
edu server
3rd query: neon.cs.virginia.edu
Referral to cs.virginia.edu name server
response
query
virginia.edu server
4th query: neon.cs.virginia.edu
Resolver
IP address of neon.cs.virginia.edu
cs.virginia.edu server

Iterative queries

- In an iterative query, the name server sends a closest known authoritative name server (here a referral to the root server).

- This involves more work for the resolver


root server
Name server
referral to root server
query
1st query: neon.cs.virginia.edu
Referral to edu name server
2nd query: neon.cs.virginia.edu
Referral to virginia.edu name server
3rd query: neon.cs.virginia.edu
Referral to cs.virginia.edu name server
edu server
virginia.edu server
Resolver
4th query: neon.cs.virginia.edu
IP address of neon.cs.virginia.edu
cs.virginia.edu server



root server

Name server

Resolver

query

referral to root server

1st query: neon.cs.virginia.edu

Referral to edu name server

edu server

2nd query: neon.cs.virginia.edu

Referral to virginia.edu name server

virginia.edu server

3rd query: neon.cs.virginia.edu

Referral to cs.virginia.edu name server

4th query: neon.cs.virginia.edu

cs.virginia.edu server

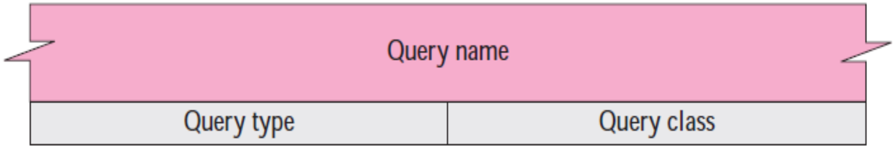
IP address of neon.cs.virginia.edu

Caching

- To reduce DNS traffic, name servers caches information on domain name/IP address mappings
- When an entry for a query is in the cache, the server does not contact other servers
    - Cache entries timeout (disappear) after some time
    - TLD servers typically cached in local name servers
    - Thus root name servers not often visited
- Note: If an entry is sent from a cache, the reply from the server is marked as “unauthoritative”

Types of Records

- Question Record
  - Used by the client to get information from a server

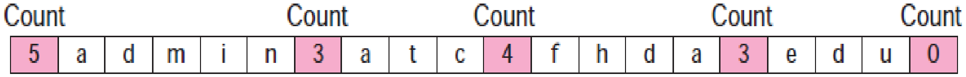


Query name

Query type

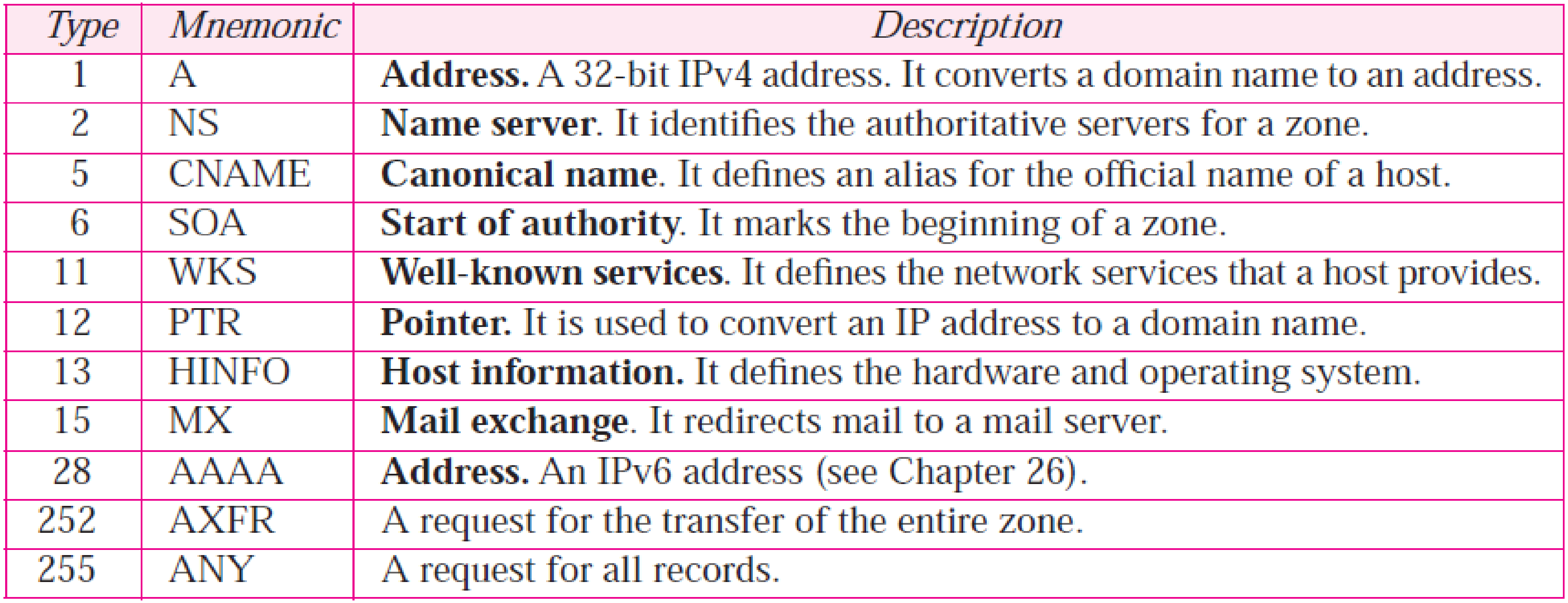
Query class

- Fields
  - Query name
    - Variable-length field containing a domain name
  - Query type
    - 16 bit
    - QTYPES are superset of TYPEs
  - Query class
    - 16 bit



Count Count Count Count Count

5 a d m i n 3 a t c 4 f h d a 3 e d u 0



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.

```
Additional QTYPES:

AXFR    252 A request for a transfer of an entire zone
MAILB   253 A request for mailbox-related records (MB,MG or MR)
MAILA   254 A request for mail agent RRs (Obsolete)
*       255 A request for all records
```

Types of Records

The CLASS resource field is rarely used.

Mostly used value is IN which indicates that this record is of the "Internet" CLASS of DNS record

Other values are CH (for Chaosnet) and HS (for Hesiod) etc.

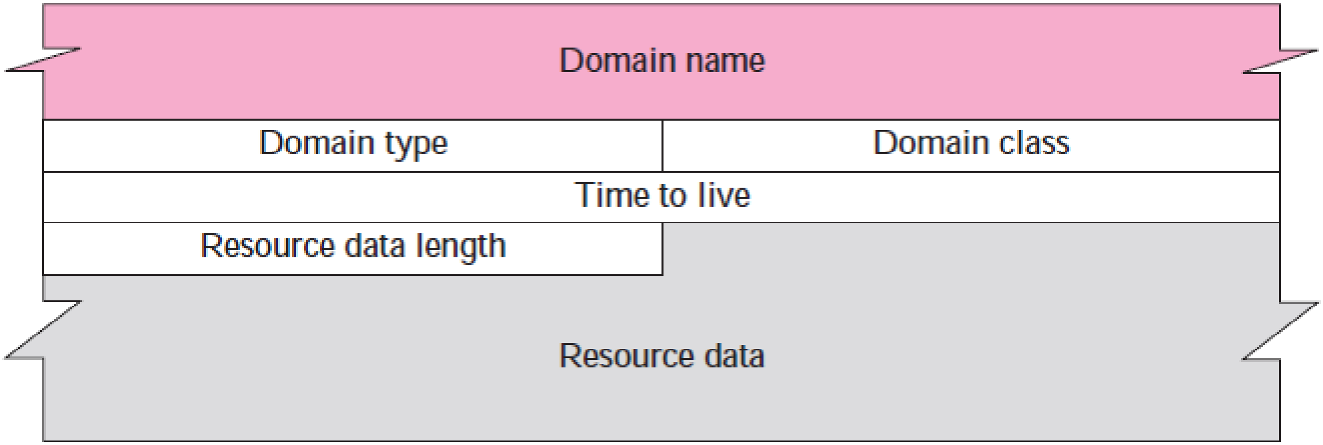
The CLASS field will almost always be IN in a DNS answer

Resource records

Resource records, often abbreviated as RR, are the content of DNS responses

Types of Records

- Resource Records
- Fields
  - Domain Name
  - Domain Type
  - Domain Class
  - TTL
    - Number of seconds the answer is valid
  - Resource data length
  - Resource data



Domain name

Domain type | Domain class

Time to live

Resource data length

Resource data

DNS Records

- DNS: distributed database storing **resource records** (**RR**)

RR format: **`(Name, Value, Type, TTL)`**

- TTL : Time to Live of the RR
  - Determines when a resource should be removed from a cache

DNS Records

RR format: **(Name, Value, Type, TTL)**

- Type=A
  - Name is a hostname
  - Value is the IP address for the hostname
  - Provides standard hostname to IP address mappings
  - Example
    - (relay1.bar.foo.com, 145.37.93.126, A)
  - The record AAAA (also quad-A record) specifies IPv6 address for given host. So it works the same way as the A record and the difference is the type of IP address

DNS Records

RR format: **`(Name, Value, Type, TTL)`**

- Type=NS
  - **Name** is a domain
  - **Value** is the hostname of an authoritative DNS server
  - Used to route DNS queries further along in the query chain
  - Example
    - (foo.com, dns.foo.com, NS)

DNS Records

RR format: **`(Name, Value, Type, TTL)`**

- Type=CNAME
  - **Name** is an alias hostname
  - **Value** is a canonical hostname
  - Used to answer DNS queries for canonical or primary name for a hostname
  - Example
    - (foo.com, relay1.bar.foo.com, CNAME)
    - (www.foo.com, relay1.bar.foo.com, CNAME)
    - (mail.foo.com, relay1.bar.foo.com, CNAME)

DNS Records

RR format: **`(Name, Value, Type, TTL)`**

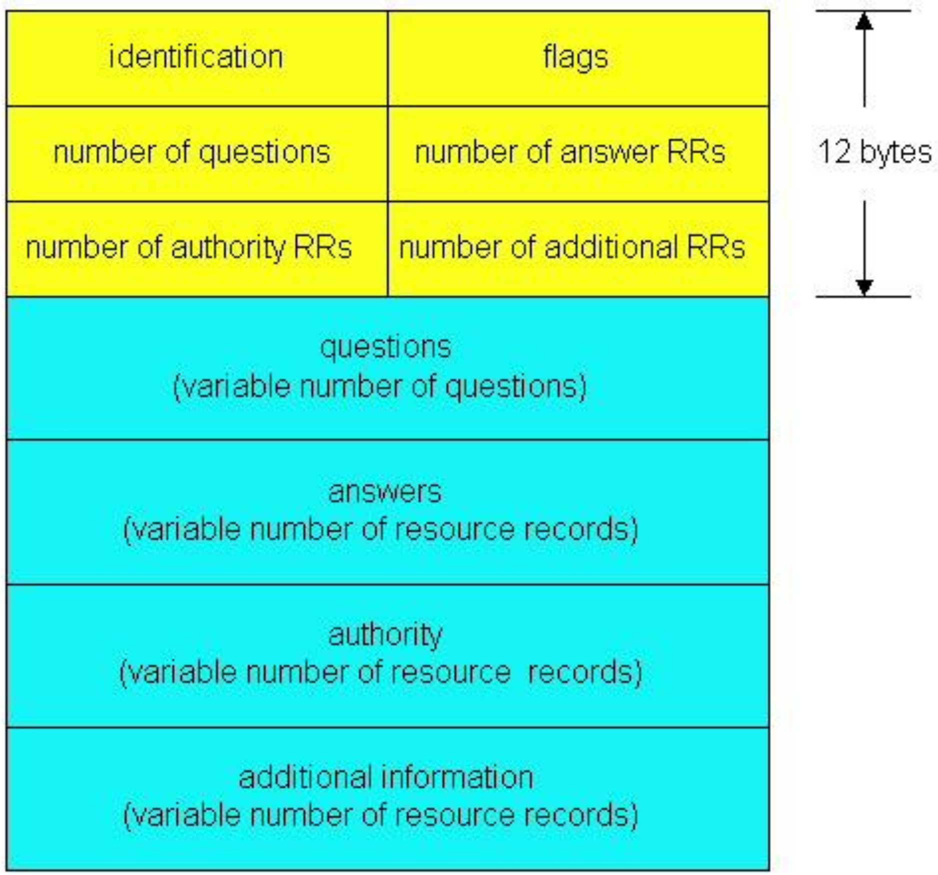
- Type=MX
  - **Name** is the alias hostname of the mailserver
  - **Value** is the canonical name of a mail server
  - Allows hostnames of mail servers to have simple aliases
  - Example
    - (foo.com, mail.bar.foo.com, MX)

DNS protocol, messages

- DNS protocol : query and reply messages, both with same message format

Message header (12 bytes)

- ❒ Identification: 16 bit # for query, reply to query uses the same #
- ❒ Flags:
  - ❖ Query or reply
  - ❖ Recursion desired
  - ❖ Recursion available
  - ❖ Reply is authoritative



identification

flags

number of questions

number of answer RRs

number of authority RRs

number of additional RRs

12 bytes

questions
(variable number of questions)

answers
(variable number of resource records)

authority
(variable number of resource records)

additional information
(variable number of resource records)

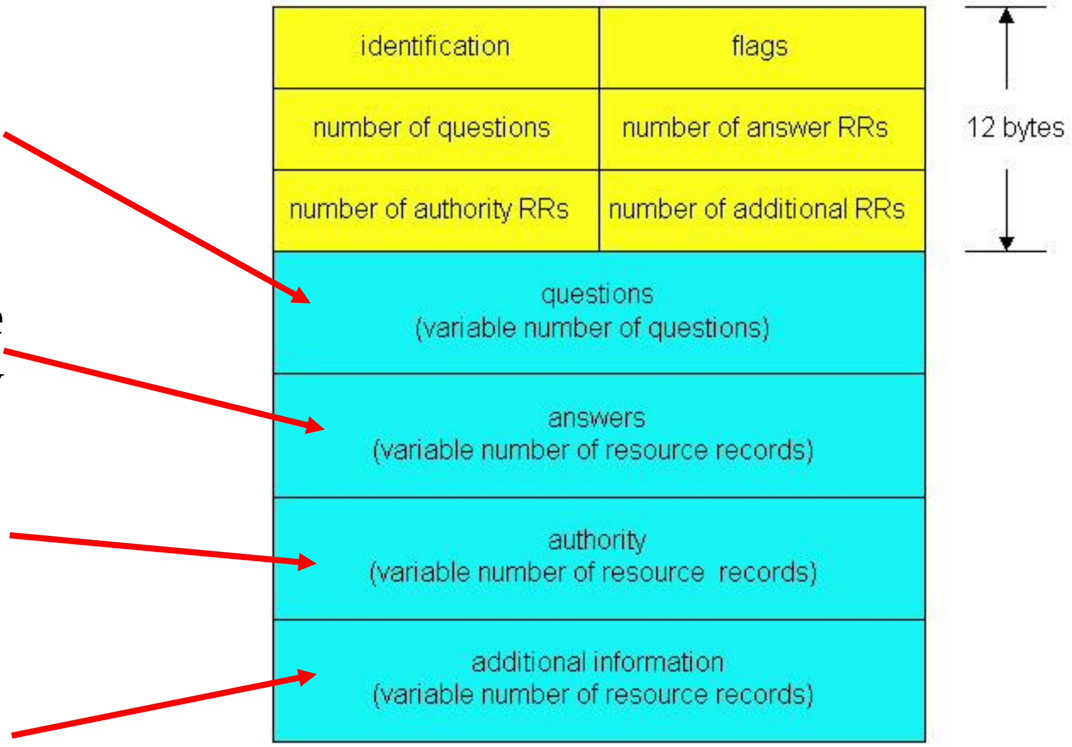
DNS protocol, messages

Name, type fields
for a query

RRs in response
to query

Records for
authoritative servers

Additional "helpful"
info that may be used



identification

flags

number of questions

number of answer RRs

number of authority RRs

number of additional RRs

12 bytes

questions
(variable number of questions)

answers
(variable number of resource records)

authority
(variable number of resource records)

additional information
(variable number of resource records)

Inserting records into DNS

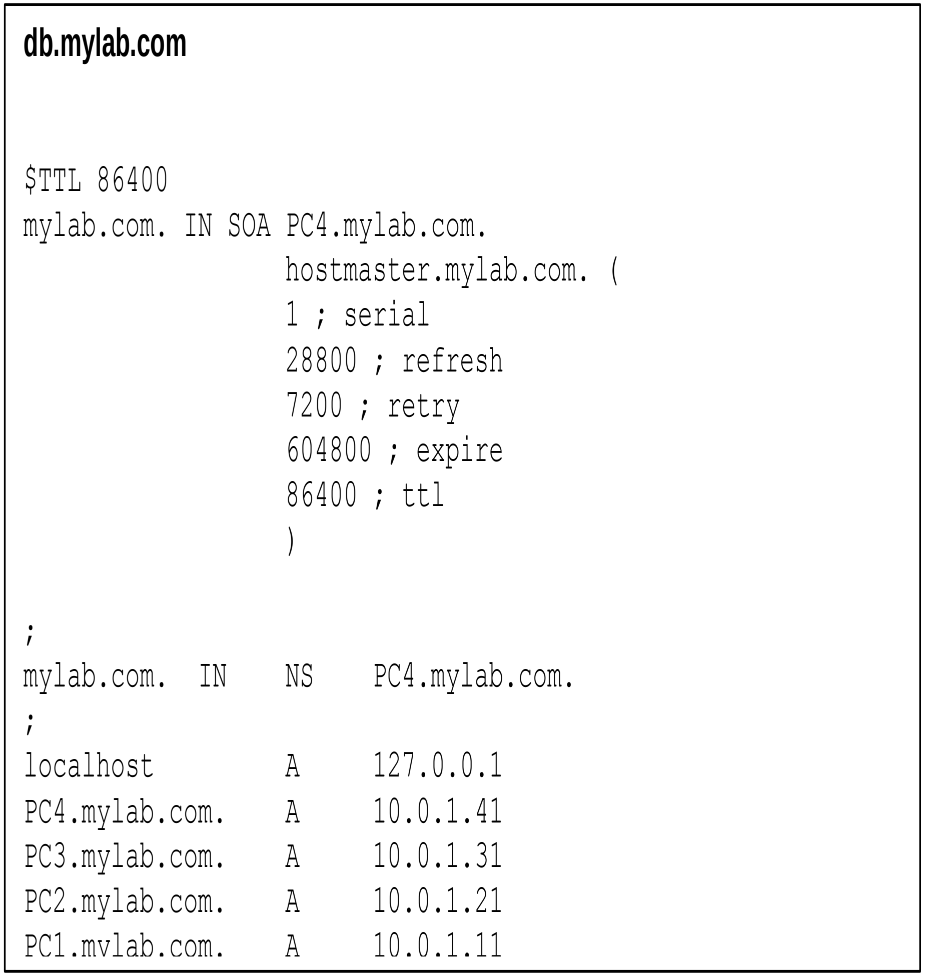
- Example: new startup “Network Utopia”
- Register name networkutopia.com at DNS registrar (e.g., Network Solutions)
  - Registrar is a commercial entity that verifies the uniqueness of the domain name
    - Internet Corporation for Assigned Names and Numbers (ICANN) accredits the various registrars
    - Complete list of accredited registrars is available at http://www.intenic.net
  - 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)
- Create authoritative server
  - Type A record for www.networkutopia.com
  - Type MX record for networkutopia.com

Security of DNS

- DNS can be attacked in several ways
  - The attacker may read the response of a DNS server to find the nature or names of sites to build the user’s profile
  - The attacker may intercept the response of a DNS server and change it
  - The attacker may flood the DNS server to overwhelm it or eventually crash it
- DNS Security (DNSSEC)
  - IETF standard
  - Provides message origin authentication and message integrity using digital signature

Resource Records

- The database records of the distributed database are called resource records (RR)
- Resource records are stored in configuration files (zone files) at name servers.
- Left Resource records for a zone:



db.mylab.com

```
$TTL 86400
mylab.com. IN SOA PC4.mylab.com.
                  hostmaster.mylab.com. (
                  1 ; serial
                  28800 ; refresh
                  7200 ; retry
                  604800 ; expire
                  86400 ; ttl
                  )

;
mylab.com.  IN    NS    PC4.mylab.com.
;
localhost         A     127.0.0.1
PC4.mylab.com.    A     10.0.1.41
PC3.mylab.com.    A     10.0.1.31
PC2.mylab.com.    A     10.0.1.21
PC1.mylab.com.    A     10.0.1.11
```

Resource Records

db.mylab.com

```
$TTL 86400
mylab.com. IN SOA PC4.mylab.com. hostmaster.mylab.com. (
                  1 ; serial
                  28800 ; refresh
                  7200 ; retry
                  604800 ; expire
                  86400 ; ttl
                  )

;
mylab.com.  IN    NS    PC4.mylab.com.
;
localhost         A     127.0.0.1
PC4.mylab.com.    A     10.0.1.41
PC3.mylab.com.    A     10.0.1.31
PC2.mylab.com.    A     10.0.1.21
PC1.mylab.com.    A     10.0.1.11
```

Max. age of cached data
in seconds

* Start of authority (SOA) record
Means: “This name server is authoritative for the zone Mylab.com”
* PC4.mylab.com is the name server
* hostmaster@mylab.com is the email address of the person in charge

Name server (NS) record.
One entry for each authoritative name server

Address (A) records.
One entry for each hostaddress