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.cs.virginia.edu, www.google.com, ietf.org
- The domain name system (DNS) is an Internet-wide distributed database that translates betweem domain names and IP addresses

- **How important is DNS?**

  Imagine what happens when the local DNS server is down.

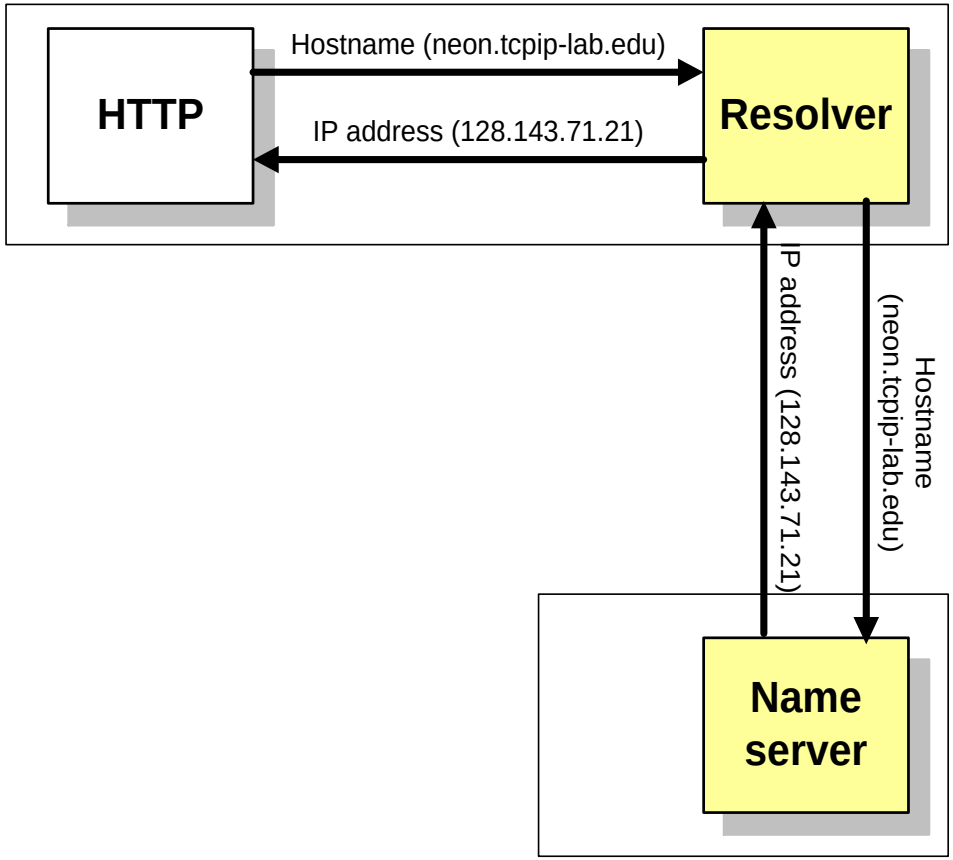
Before there was DNS ….

…. 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.

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



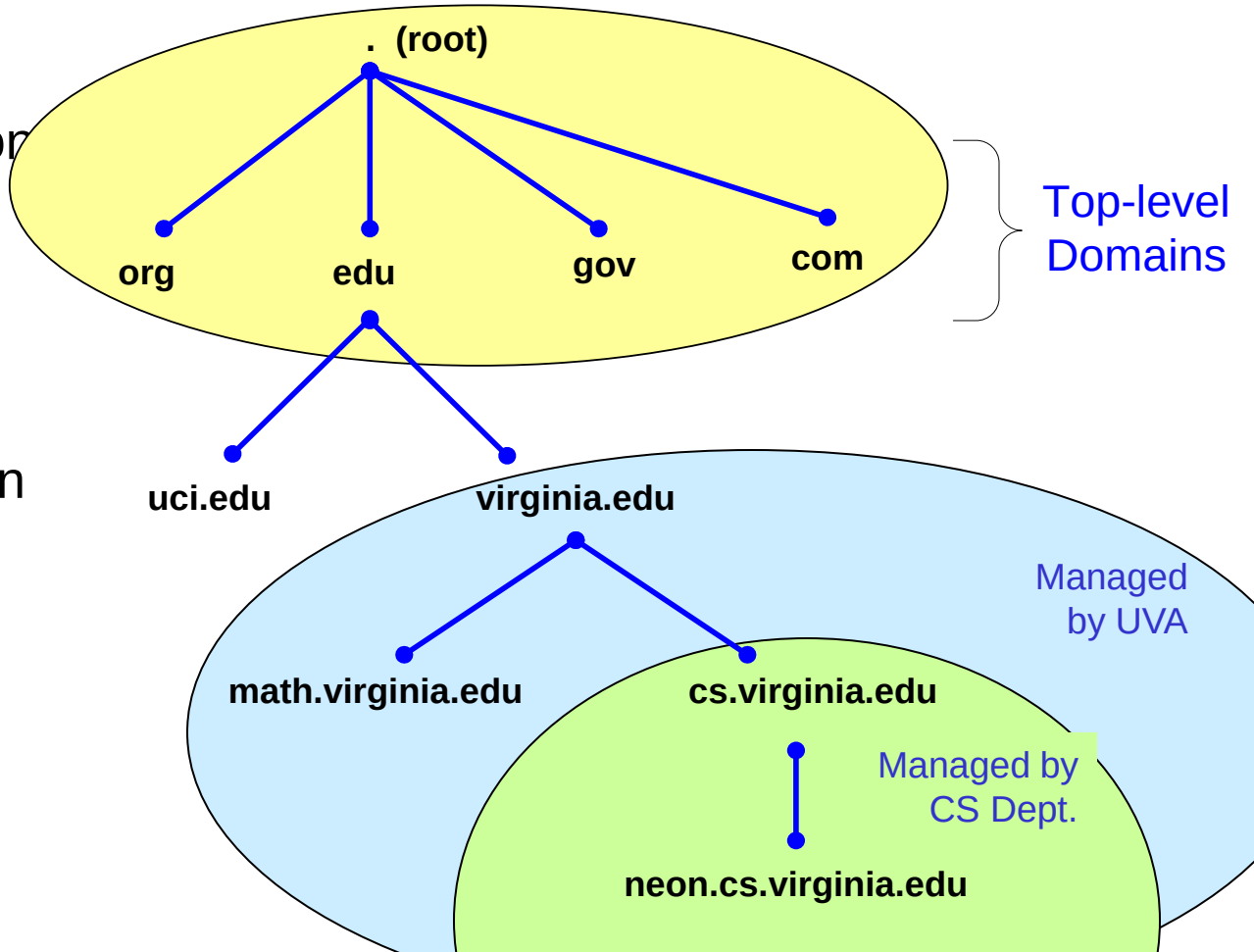
- Reverse lookups are also possible, i.e., find the hostname given an IP address

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 have domain name suffix virginia.edu
  - All hosts on network 128.143.136/24 are in the Computer Science Department of the University of Virginia

DNS Name hierarchy

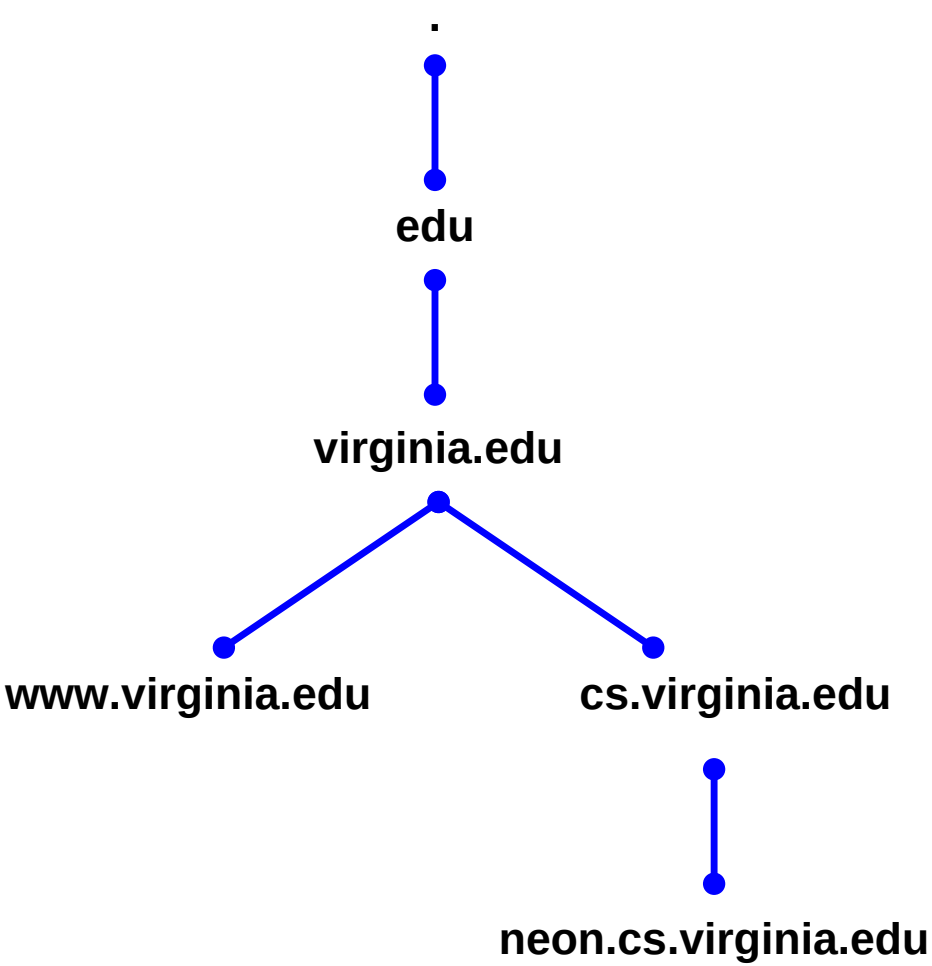
- DNS hierarchy can be represented by a tree
- Below top-level domain, administration of name space is delegated to organizations
- Each organization can delegate further



Domain name system

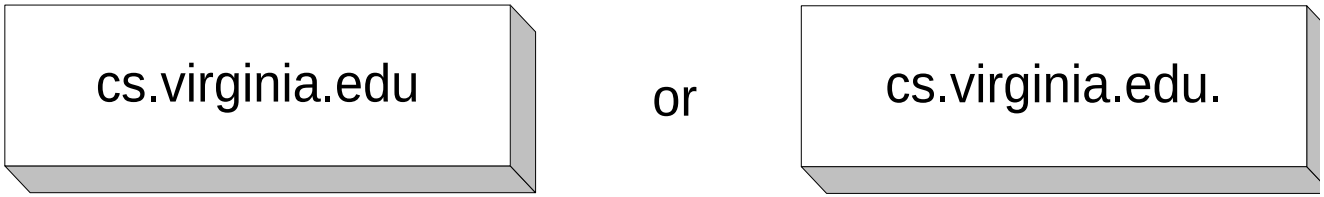
- Each node in the DNS tree represents a DNS name
- Each branch below a node is a DNS domain.
  - DNS domain can contain hosts or other domains (subdomains)

- 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.



- 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

Top-level domains

- Three types of top-level domains:
  - Generic Top Level Domains (gTLD): 3-character code indicates the function of the organization
    - Used primarily within the US
    - Examples: gov, mil, edu, org, com, net
  - Country Code Top Level Domain (ccTLD): 2-character country or region code
    - Examples: us, va, 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.

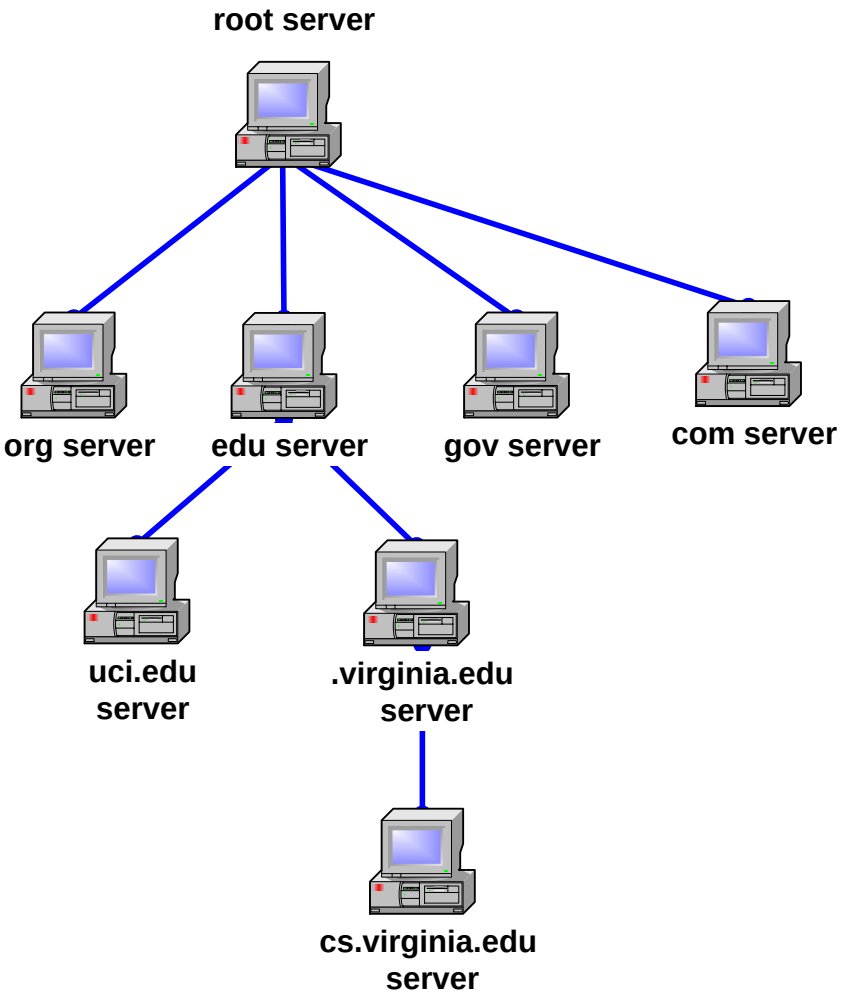
Generic Top Level Domains (gTLD)

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

- gTLDs are authoritatively administered by the Internet central name registration authority ICANN

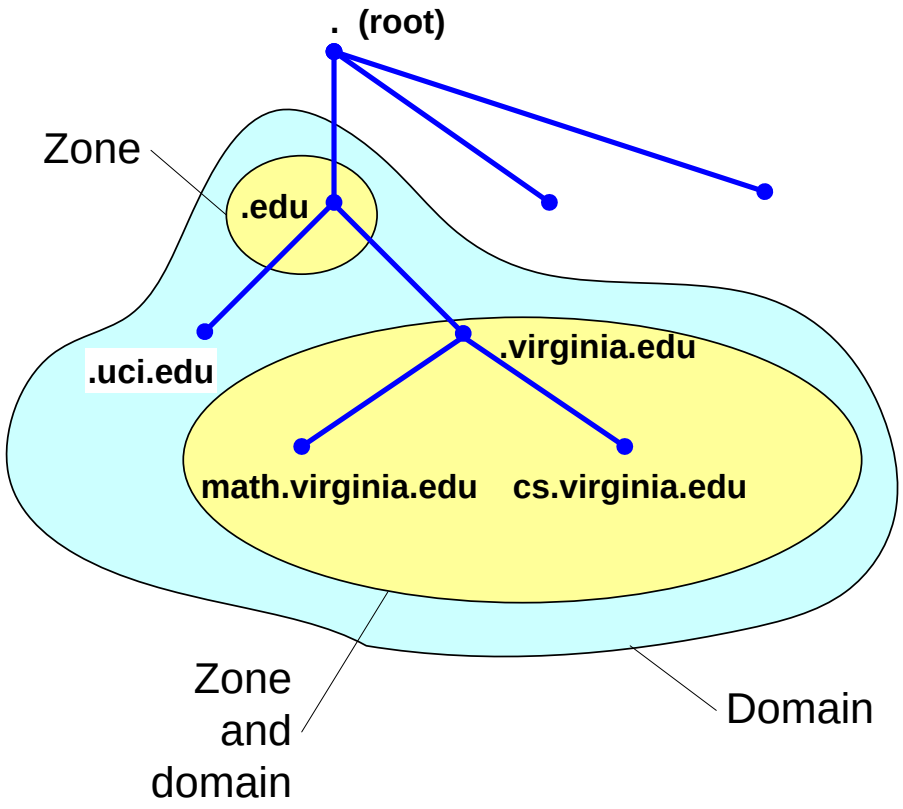
Hierarchy of name servers

- 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.
- DNS server answers queries about hosts in its zone



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 consists of multiple nodes)
- A server can divide part of its zone and delegate it to other servers



Primary and secondary name servers

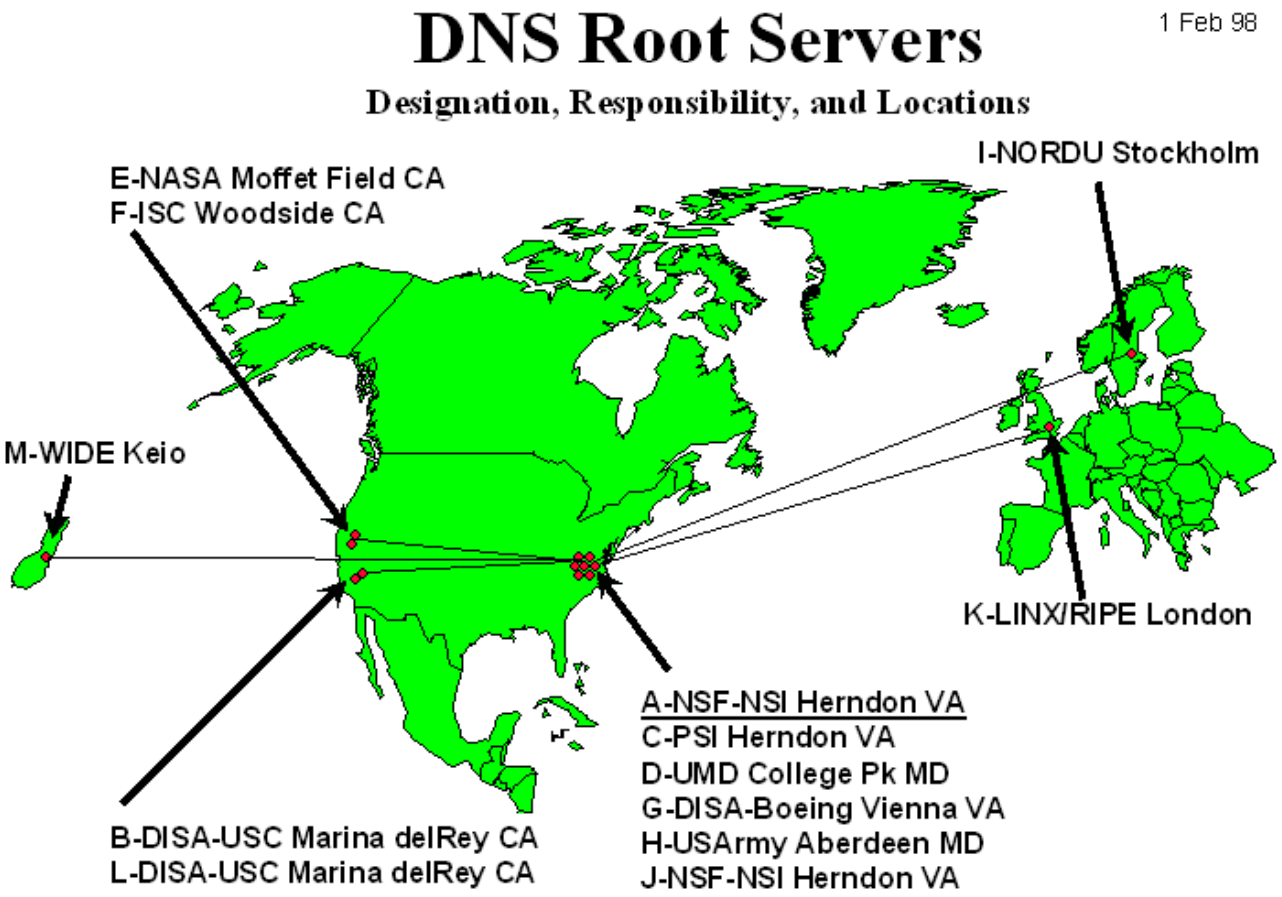
- For each zone, there must be a primary name server and a secondary name server
  - The primary server (master server) maintains a zone file which has information about the zone. Updates are made to the primary server
  - The secondary server copies data stored at the primary server.

Adding a host:

- When a new host is added (“gold.cs.virginia.edu”) 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

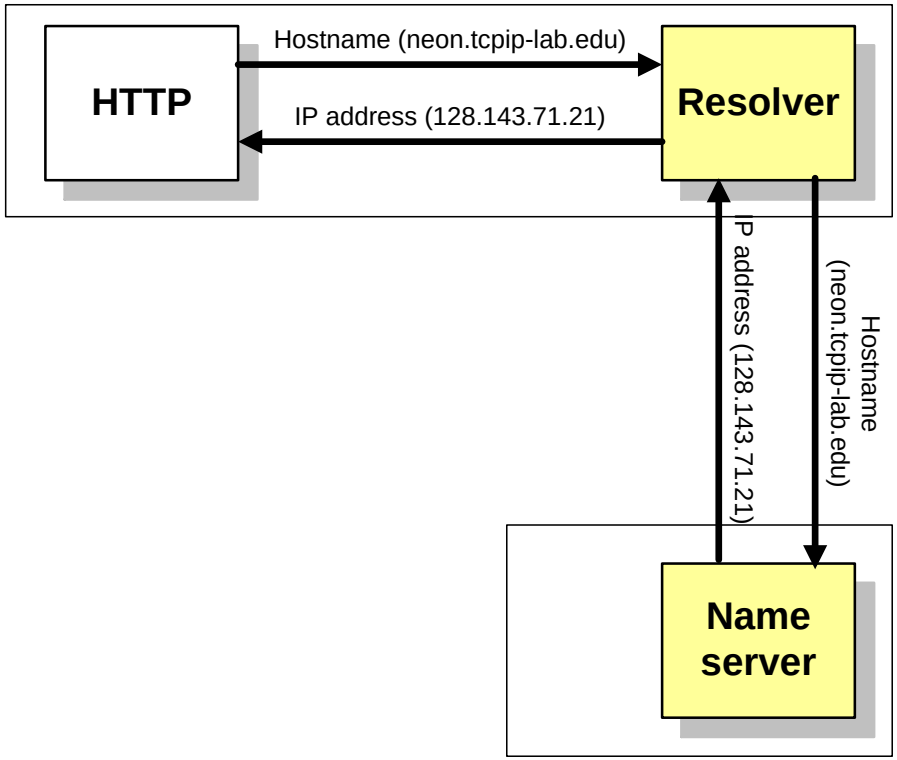


Addresses of root servers (2004)

A.ROOT-SERVERS.NET.	(VeriSign, Dulles, VA)	198.41.0.4
B.ROOT-SERVERS.NET.	(ISI, Marina Del Rey CA)	192.228.79.201
C.ROOT-SERVERS.NET.	(Cogent Communications)	192.33.4.12
D.ROOT-SERVERS.NET.	(University of Maryland)	128.8.10.90
E.ROOT-SERVERS.NET.	(Nasa Ames Research Center)	192.203.230.10
F.ROOT-SERVERS.NET.	(Internet Systems Consortium)	192.5.5.241
G.ROOT-SERVERS.NET.	(US Department of Defense)	192.112.36.4
H.ROOT-SERVERS.NET.	(US Army Research Lab)	128.63.2.53
I.ROOT-SERVERS.NET.	(Autonomica/NORDUnet)	192.36.148.17
J.ROOT-SERVERS.NET.	(Verisign, multiple cities)	192.58.128.30
K.ROOT-SERVERS.NET.	(RIPE,Europe multiple cities)	193.0.14.129
L.ROOT-SERVERS.NET.	(IANA, Los Angeles)	198.32.64.12
M.ROOT-SERVERS.NET.	(WIDE, Tokyo, Seoul, Paris)	202.12.27.33

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.



Recursive and Iterative Queries

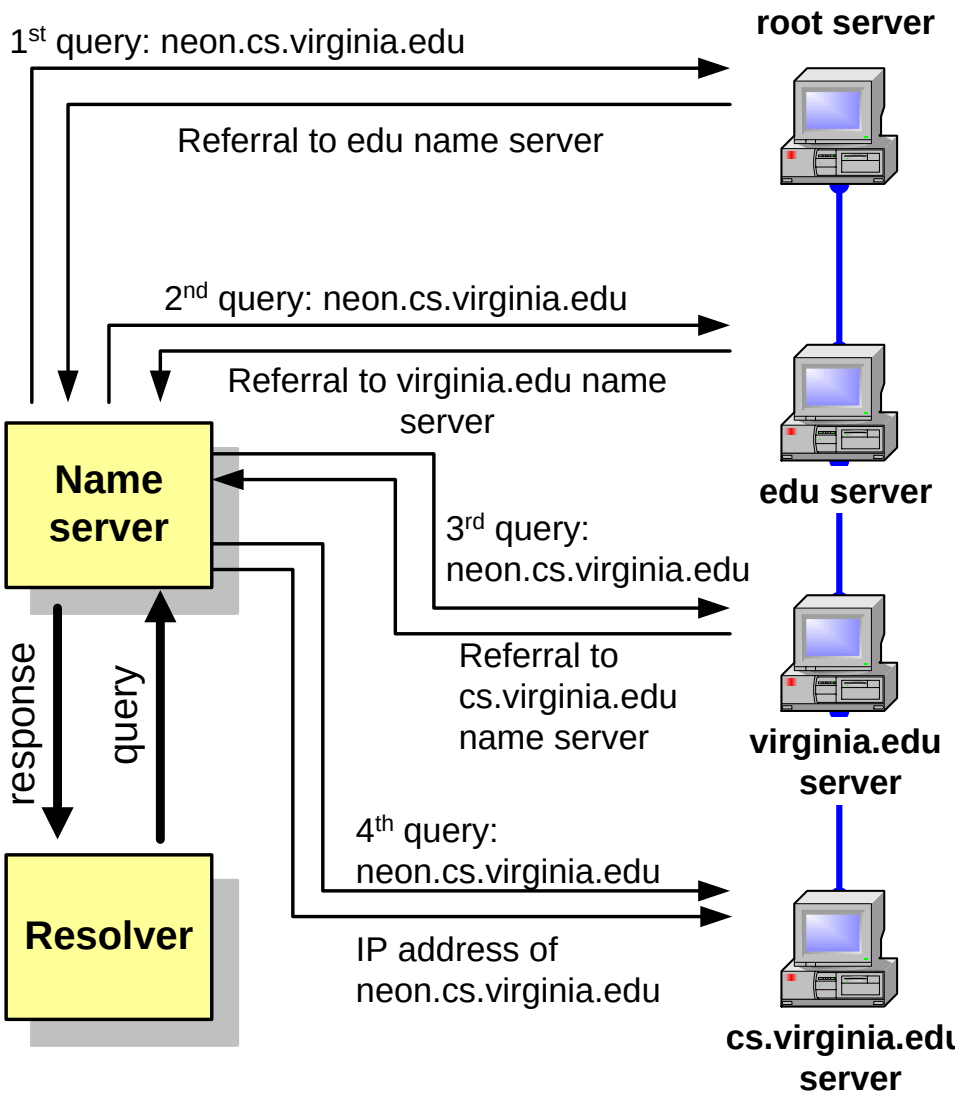
- There are two types of queries:
  - Recursive queries
  - Iterative (non-recursive) queries

- 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

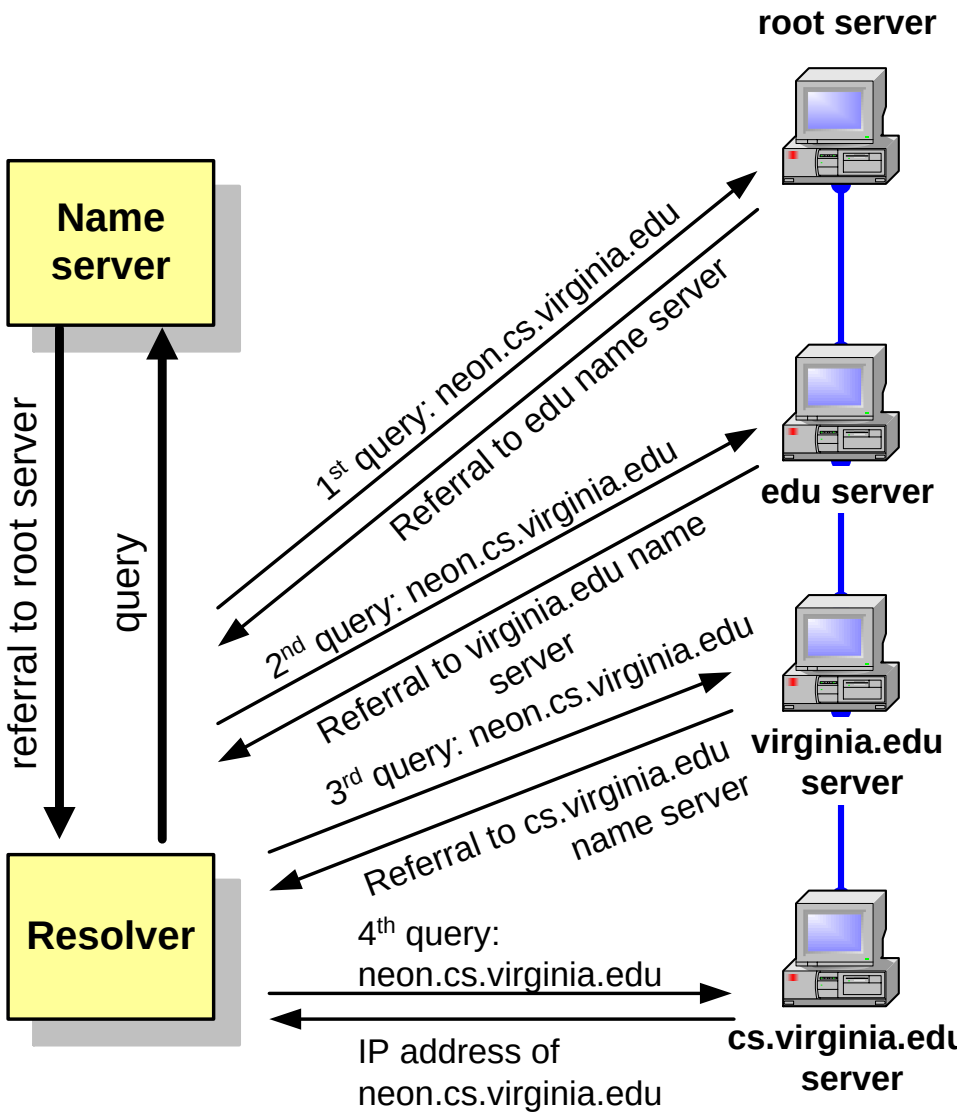
Recursive queries

- 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



Iterative queries

- In an iterative query, the name server sends a closest known" authoritative name server the a referral to the root server.
- This involves more work for the resolver



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
- Note: If an entry is sent from a cache, the reply from the server is marked as “unauthoritative”

Resource Records

- The database records of the DNS distributed data base are called resource records (RR)
- Resource records are stored in configuration files (zone files) at name servers.

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.mvlab.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