# CS4450 Problem Set #5

April 27, 2018

# 1 DNS

(a) In this problem, we use the useful dig tool available on Unix and Linux hosts to explore the hierarchy of DNS servers. Recall that a DNS server higher in the DNS hierarchy delegates a DNS query to a DNS server lower in the hierarchy, by sending back to the DNS client the name of that lower-level DNS server. First read the man page for dig, and then answer the following questions.

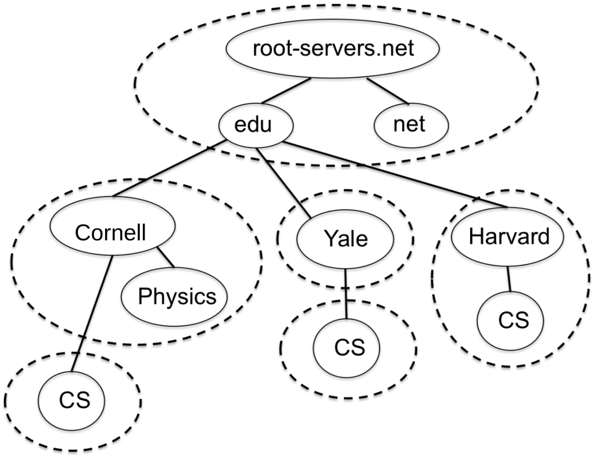
- Starting with a root DNS server (from one of the root servers [a-m].root- servers.net), initiate a sequence of queries for the IP address for your departments Web server by using dig. Show the list of the names of DNS servers in the delegation chain in answering your query.
- Repeat the first part for several popular Web sites, such as google.com, yahoo.com, or amazon.com.

(b) Suppose you can access the caches in the local DNS servers of your department. Can you propose a way to roughly determine the Web servers (outside your department) that are most popular among the users in your department? Explain.

(c) Suppose that your department has a local DNS server for all computers in the department. You are an ordinary user (i.e., not a network/system administrator). Can you determine if an external Web site was likely accessed from a computer in your department a couple of seconds ago? Explain.

## 2 DNS

Consider the DNS topology in the figure below **each DNS zone is indicated with a dashed line**. There is only one DNS server per each zone, and it happens to have the same name as the highest node in that zone: Cornell.EDU, CS.Cornell.EDU, Harvard.EDU, Yale.EDU, CS.Yale.EDU, and root-servers.net.



For each of the queries below, list in order all the DNS servers queried during the name resolution. Assume there is no caching performed at any level of the hierarchy.

(a) A user on **john.cs.harvard.edu** launches the query:

```
dig einstein.physics.cornell.edu
```

(b) A user on **einstein.physics.cornell.edu** launches the query:

```
dig dan.cs.yale.edu
```

# 3 DNS

Consider the partial output of the dig command given below:

```
; <<>> DiG 9.9.4-RedHat-9.9.4-18.el7_1.3 <<>>
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47902

;; ANSWER SECTION:
harvard.edu. 1306 IN MX 100 b-00171101.pphosted.com.
harvard.edu. 1630 IN MX 100 a-00171101.pphosted.com.

;; AUTHORITY SECTION:
harvard.edu. 172100 IN NS ext-1.harvard.edu.

;; ADDITIONAL SECTION:
a-00171101.pphosted.com.        1313    IN A 67.231.148.27
b-00171101.pphosted.com.        1797    IN A 67.231.156.27
ext-1.harvard.edu.            172756    IN A 128.103.200.35

;; Query time: 1 msec
;; SERVER: 128.112.136.10#53(128.112.136.10)
;; WHEN: Mon Mar 07 12:49:47 EST 2016
;; MSG SIZE  rcvd: 224
```

(a) List the IP address(es) of the name server(s) of harvard.edu.

(b) List the IP address(es) of the mail server(s) of harvard.edu.

(c) For how many seconds are the entries for the address records of the mail and name servers valid?