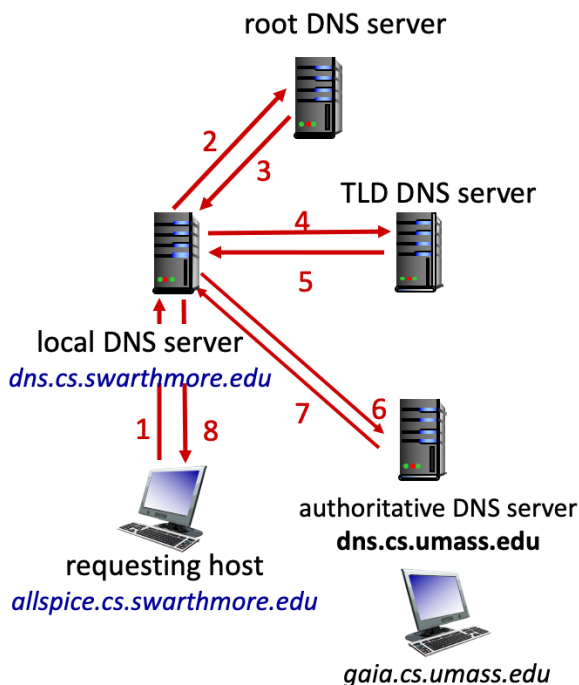


Worksheet Class 7: DNS

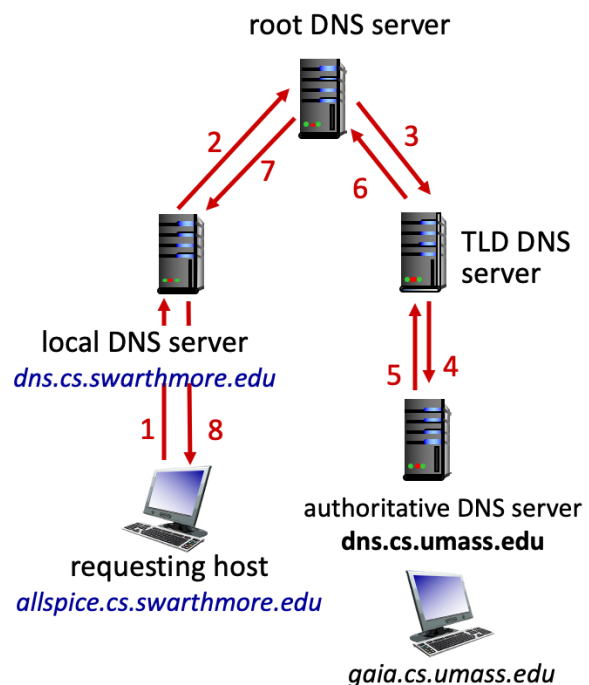
Note: These dig outputs were captured in a previous year. Today's answers differ: .org, freebsd.org and mit.edu have all changed name servers since. The structure of each response is what matters here.

Q1. Which of the two DNS query models would you use to resolve a hostname to an IP address? Why?

A. Iterative



B. Recursive



Q2. Answer the following questions in the context of the DNS response below:

- A. How many answers were returned? What does it mean if the answer section is empty?
- B. What is the time-to-live in this RR in seconds?
- C. How many additional records are present?

```
$ dig @a.root-servers.net www.freebsd.org +norecurse
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57494
;; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;www.freebsd.org.  IN  A

;; AUTHORITY SECTION:
org. 172800 IN NS b0.org.afiliast-nst.org.
org. 172800 IN NS d0.org.afiliast-nst.org.

;; ADDITIONAL SECTION:
b0.org.afiliast-nst.org. 172800 IN A 199.19.54.1
d0.org.afiliast-nst.org. 172800 IN A 199.19.57.1
```

Q3. The query below asks a .org server (199.19.54.1) for the IP address of www.freebsd.org.

- A. How many answers were returned?
- B. What do the authoritative and additional records tell us?

A. What do the authoritative records and additional records tell us?

```
$ dig @199.19.54.1 www.freebsd.org +norecurse
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39912
;; QUERY: 1, ANSWER: 0, AUTHORITY: 3, ADDITIONAL: 0

;; QUESTION SECTION:
;www.freebsd.org.  IN  A

;; AUTHORITY SECTION:
freebsd.org. 86400 IN NS ns1.isc-sns.net.
freebsd.org. 86400 IN NS ns2.isc-sns.com.
freebsd.org. 86400 IN NS ns3.isc-sns.info.
```

- Q4. Answer the following questions in the context of the DNS response below:
- A. Assuming this is the next DNS query we do, following the query in Q3; list the server being contacted here, and whether this is an authoritative name server, top-level domain or the root server.

```
$ dig @ns1.isc-sns.net www.freebsd.org +norecurse
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17037
;; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 3

;; QUESTION SECTION:
;www.freebsd.org.  IN  A

;; ANSWER SECTION:
www.freebsd.org.  3600  IN  A  69.147.83.33

;; AUTHORITY SECTION:
freebsd.org.  3600  IN  NS  ns2.isc-sns.com.
freebsd.org.  3600  IN  NS  ns1.isc-sns.net.
freebsd.org.  3600  IN  NS  ns3.isc-sns.info.

;; ADDITIONAL SECTION:
ns1.isc-sns.net.  3600  IN  A  72.52.71.1
ns2.isc-sns.com.  3600  IN  A  38.103.2.1
ns3.isc-sns.info. 3600  IN  A  63.243.194.1
```

Q5. Adding a new DNS Entry: You've just received venture capital funding for a fancy new Internet service named fancy.rocks with the brand new ".rocks" top-level domain name. You have a webserver with the host name "server.fancy.rocks" and an authoritative DNS server "dns.fancy.rocks".

What new DNS entries need to be added? What servers do they need to be added to?

Q6. Attacking DNS

Security risk #1: malicious DNS server

- So far from what we have seen it seems as though if *any* of the DNS servers queried are malicious, they can lie to us and fool us about the answer to our DNS query.
- What are the potential consequences?
- Consider the following legitimate DNS response for eecs.mit.edu followed by a poisoned response. What are the consequences to www.swarthmore.edu with the poisoned DNS response?

Legitimate Response:

```
; ; <<>> DiG 9.6.0-APPLE-P2 <<>> eecs.mit.edu a
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19901
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3,
ADDITIONAL: 3
```

```
;; QUESTION SECTION:
```

```
;eecs.mit.edu.                IN      A
```

```
;; ANSWER SECTION:
```

```
eecs.mit.edu.                21600   IN      A      18.62.1.6
```

```
;; AUTHORITY SECTION:
```

```
mit.edu.                    11088   IN      NS      BITSY.mit.edu.
```

```
mit.edu.                    11088   IN      NS      W20NS.mit.edu.
```

```
mit.edu.                    11088   IN      NS      STRAWB.mit.edu.
```

```
;; ADDITIONAL SECTION:
```

```
STRAWB.mit.edu.            126738  IN      A      18.6.6.6
```

```
BITSY.mit.edu.            166408  IN      A      18.72.0.3
```

```
W20NS.mit.edu.            126738  IN      A      18.70.0.160
```

Poisoned DNS Response

```
; ; <<>> DiG 9.6.0-APPLE-P2 <<>> eecs.mit.edu a
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19901
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3,
ADDITIONAL: 3

;; QUESTION SECTION:
;eecs.mit.edu.                IN      A

;; ANSWER SECTION:
eecs.mit.edu.                21600   IN      A      18.62.1.6

;; AUTHORITY SECTION:
mit.edu.                    11088   IN      NS      BITSY.mit.edu.
mit.edu.                    11088   IN      NS      W20NS.mit.edu.
mit.edu.                    30000   IN      NS      www.swarthmore.edu

;; ADDITIONAL SECTION:
www.swarthmore.edu.        30000   IN      A      18.6.6.6
BITSY.mit.edu.             166408  IN      A      18.72.0.3
W20NS.mit.edu.             126738  IN      A      18.70.0.160
```