CS 43: Computer Networks

DNS and Email

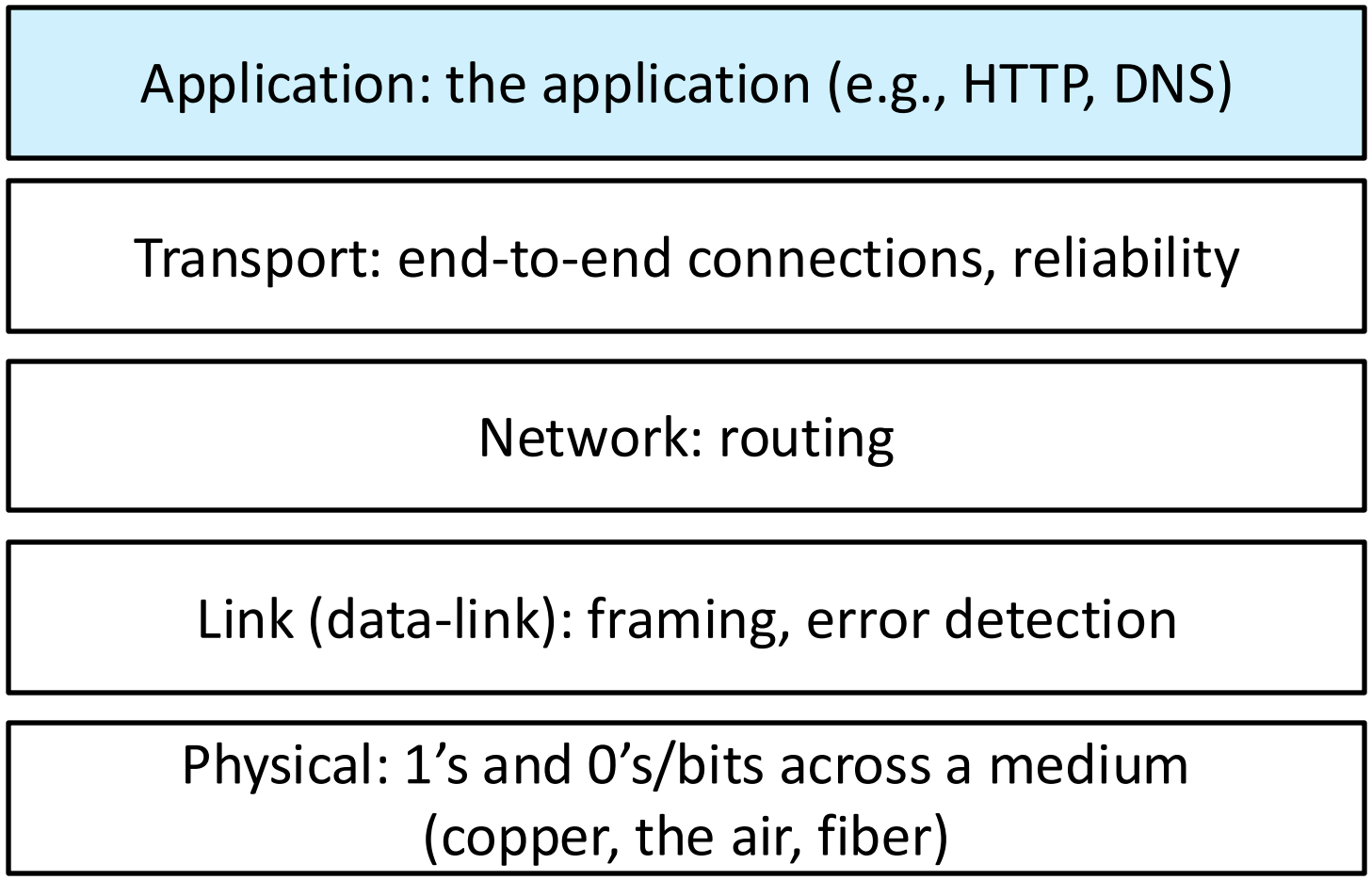
September 29, 2025

Slides adapted from Kurose & Ross, Vasanta Chaganti, Kevin Webb

Let's talk about the quiz

- See Gradescope for your grade

Where we are


Application: the application (e.g., HTTP, DNS)
Transport: end-to-end connections, reliability
Network: routing
Link (data-link): framing, error detection
Physical: 1's and 0's/bits across a medium
(copper, the air, fiber)

Today

- Wrapping up DNS
  - DNS as indirection
  - DNS security
- SMTP Protocol

Julia Evans
@b0rk

everything inside a DNS packet

I literally mean everything, I copied this verbatim from a real DNS request using Wireshark.

(DNS packets are binary but we're showing a human-readable representation here)

Let's look at the actual data being sent during a DNS query:

request

```
Query ID:             0x05a8
Flags:                0x1000
Questions:                 1
Answer records:            0
Authority records:         0
Additional records:        0
Question:
  Name:               example.com
  Type:               A
  Class:              IN
```

- Query ID: randomly generated
- Flags: these flags just mean "this is a request"
- Type: A is for IPv4 Address. other types: MX, CNAME, AAAA, etc
- Class: IN stands for "INternet"

response

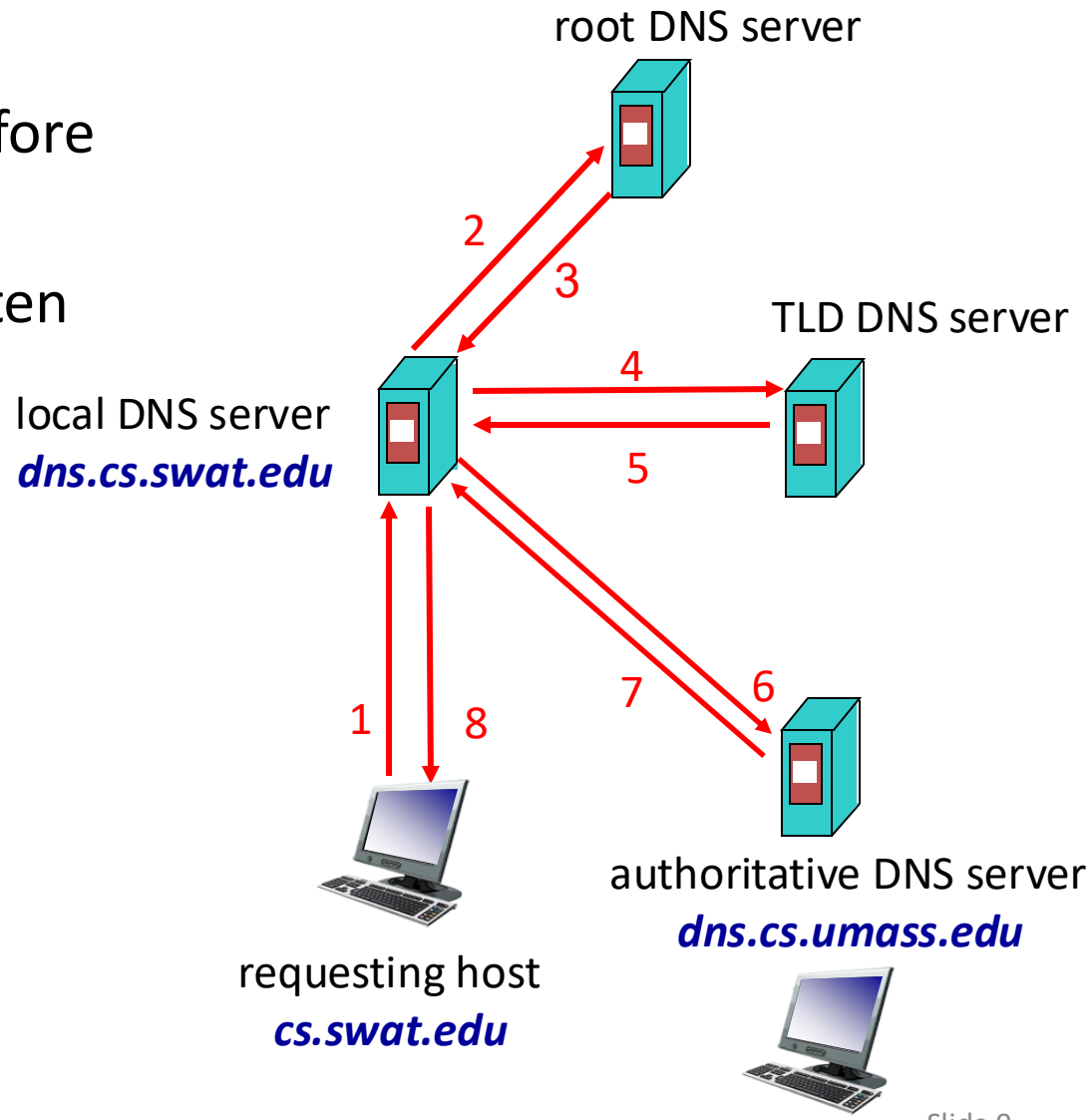
```
Query ID:             0x05a8
Flags:                0x8580
Questions:                 1
Answer records:            1
Authority records:         0
Additional records:        0
Question:
  Name:               example.com
  Type:               A
  Class:              IN
Answer records:
  Name:               example.com
  Type:               A
  Class:              IN
  TTL:                86400
  Content:            93.184.216.34
Authority records:
  (empty)
Additional records:
  (empty)
```

- Query ID: matches request ID
- Flags: the response code is encoded in the last 4 bits of these flags. The 3 main response codes are:
  - NOERROR (success!)
  - NXDOMAIN (doesn't exist!)
  - SERVFAIL (error!)
- Question: copied from request
- Name: domain names aren't case sensitive
- Content: the IP we asked for
- Authority records / Additional records: page 12 ("NS records") talks more about these 2 sections

https://wizardzines.com/comics/dns-packet/

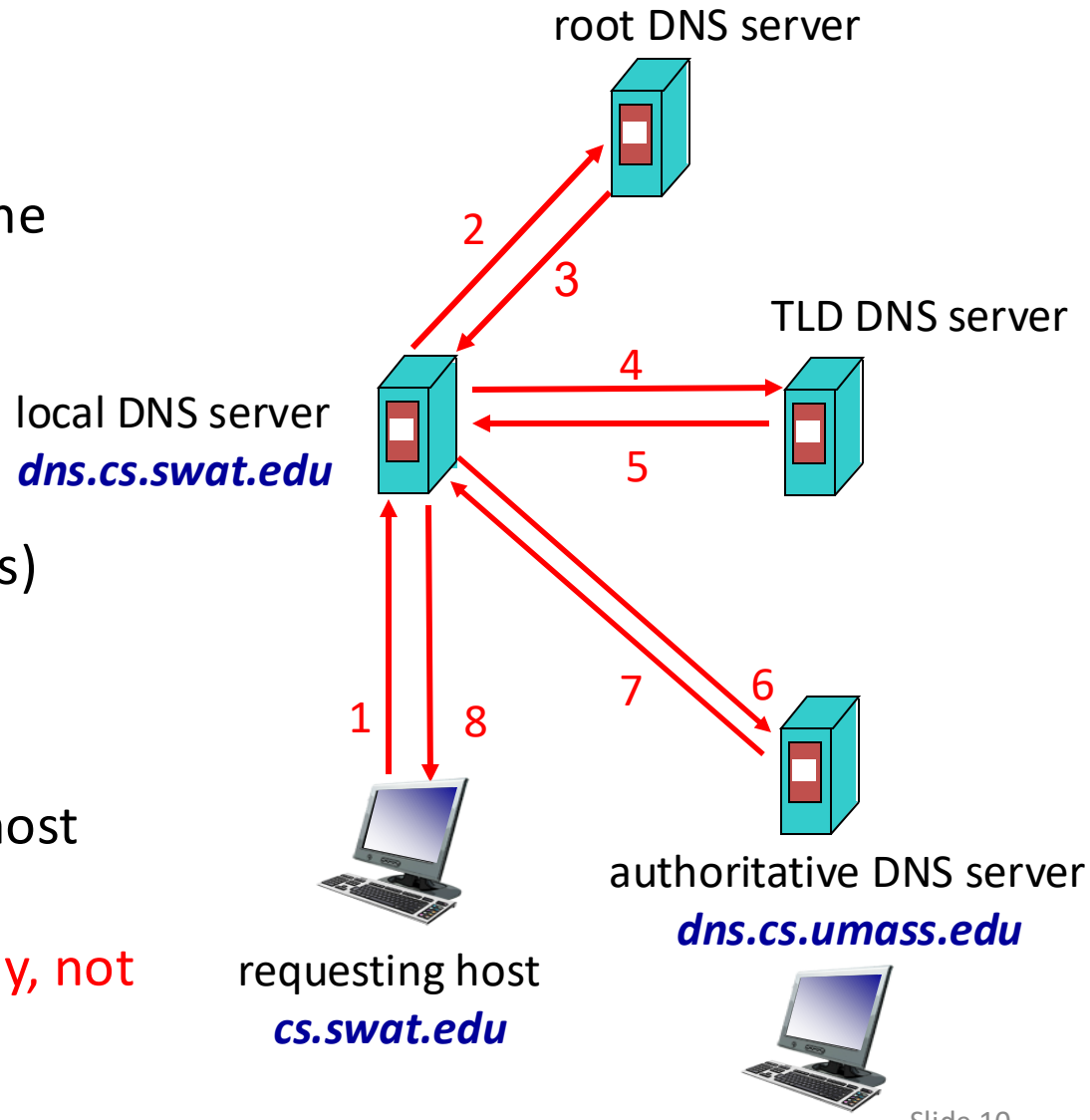
DNS Caching

- Why cache?
  - apprx. 1 sec latency before starting a download
  - Popular sites visited often
- Where to cache?
  - Local DNS server
  - Browser



DNS Caching

- When to cache?
  - learn a mapping? cache!
  - any name server can cache
- For how long?
  - until Time To Live (expires)
- What to cache?
  - TLD servers cached – almost never change
  - Root name servers usually, not visited legitimately



The TTL value should be…

A. Short, to make sure that changes are accurately reflected

B. Long, to avoid re-queries of higher-level DNS servers

C. Something else

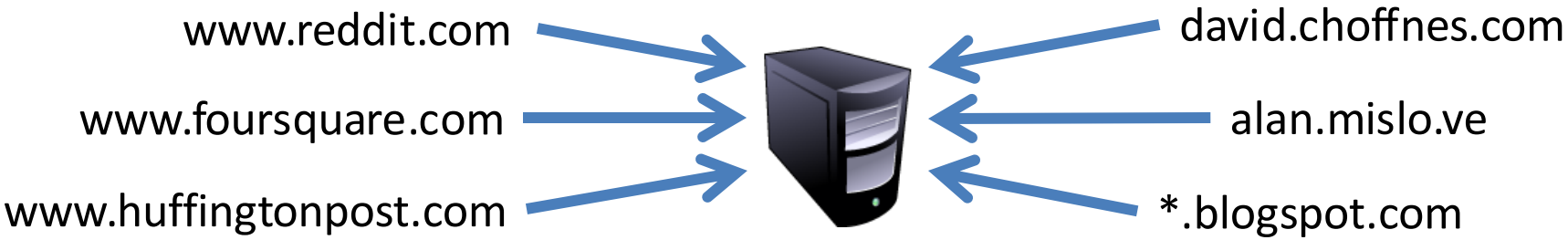
DNS as Indirection Service

- DNS gives us very powerful capabilities
  - Not only easier for humans to reference machines!

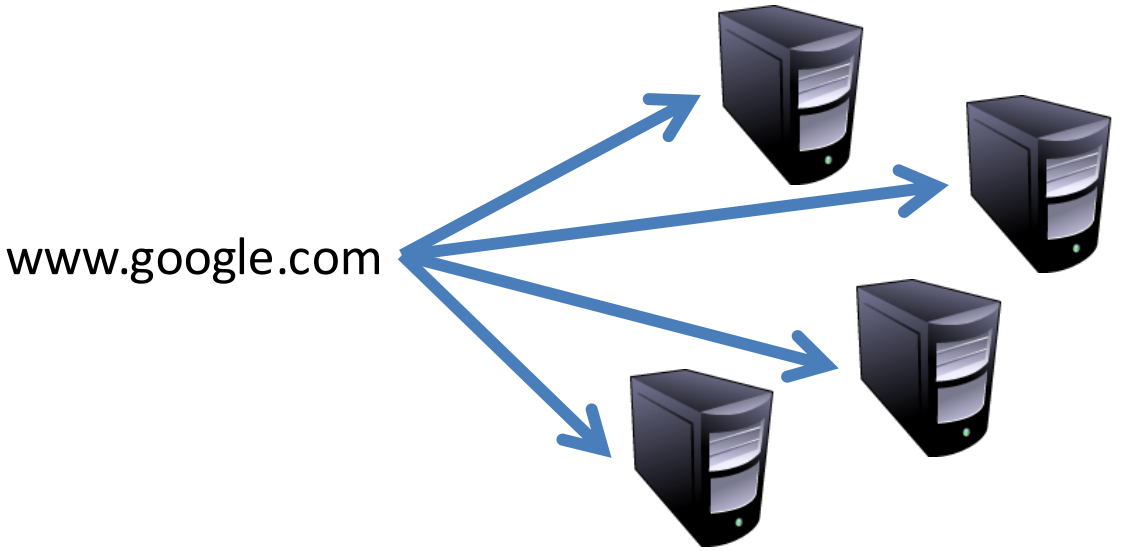
- Changing the IPs of machines becomes trivial
  - e.g. you want to move your web server to a new host
  - Just change the DNS record!

Aliasing and Load Balancing

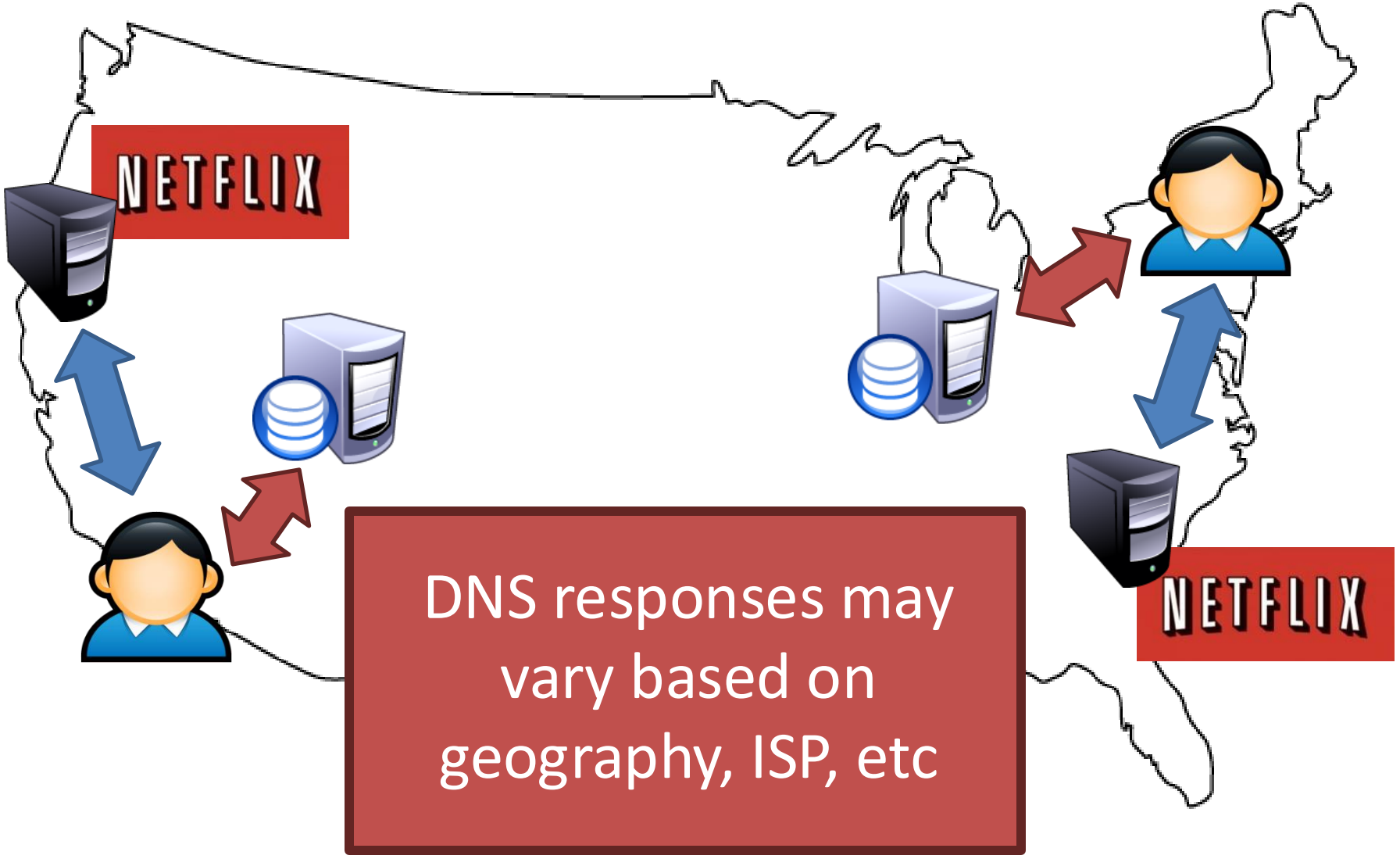
- One machine can have many aliases



  - One domain can map to multiple machines



Content Delivery Networks



Inserting (or changing) records

Example: new startup "Network Utopia"

- Step 1: Register networkuptopia.com at DNS registrar
  - provide names, IP addresses of authoritative name server (primary and secondary)

Inserting (or changing) records

Example: new startup “Network Utopia”

- Step 2: Registrar inserts two RRs into .com TLD server
  - (networkutopia.com, dns1.networkutopia.com, NS)
  - (dns1.networkutopia.com, 212.212.212.1, A)

Inserting (or changing) records

Example: new startup "Network Utopia"

- Step 3: Set up authoritative server at that name/address
  - Create records for the services:

Inserting (or changing) records

Example: new startup "Network Utopia"

- Step 3: Set up authoritative server at that name/address
  - Create records for the services:
    - type A record for www.networkuptopia.com
    - type MX record for @networkutopia.com email

Inserting (or changing) records

- Example: new startup "Network Utopia"
- Register networkuptopia.com at DNS registrar
  - 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)
- Set up authoritative server at that name/address
  - Create records for the services:
    - type A record for www.networkuptopia.com
    - type MX record for @networkutopia.com email

Worksheet: Inserting (or changing) records

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?

- . → nameless root
- .rocks → top-level domain
  - Register fancy.rocks' authoritative DNS server with .rocks domain
  - Step 1: NS record (which says .fancy.rocks can be resolved by dns.fancy.rocks)
    - **`(fancy.rocks 1-day dns.fancy.rocks NS)`**
  - Step 2: A record (dns.fancy.rocks has the IP address 1.2.3.4 (you can come up with any IP address)).
    - **`(dns.fancy.rocks 1-day 1.2.3.4 A)`**

- .fancy.rocks → (server.fancy.rocks)
  - When we reach the authoritative name domain (fancy.rocks) we need to first associate the domain name with the server's name. This is a CNAME record.
    - **`(fancy.rocks 1day server.fancy.rocks CNAME)`**
  - Next, we need to provide the IP address of the server.
    - **`(server.fancy.rocks 12hours 4.5.6.7 A)`**
  - Here, I have set the A record TTL to be smaller (compared to the other records), in case I plan to migrate the server to a different IP address.

Tools

- dig
  - $ dig cs.swarthmore.edu
  - $ dig cs.swarthmore.edu ns
  - $ dig @dns.cs.swarthmore.edu cs.swarthmore.edu mx
  - $ man dig
- host
  - $ host cs.swarthmore.edu
  - $ host -t ns cs.swarthmore.edu
  - $ host -t mx cs.swarthmore.edu dns.cs.swarthmore.edu
  - $ man host

Tools (cont)

- nslookup
  - $ nslookup cs.swarthmore.edu
  - $ nslookup cs.swarthmore.edu dns.cs.swarthmore.edu

- whois
  - $ whois google.com
  - $ whois swarthmore.edu

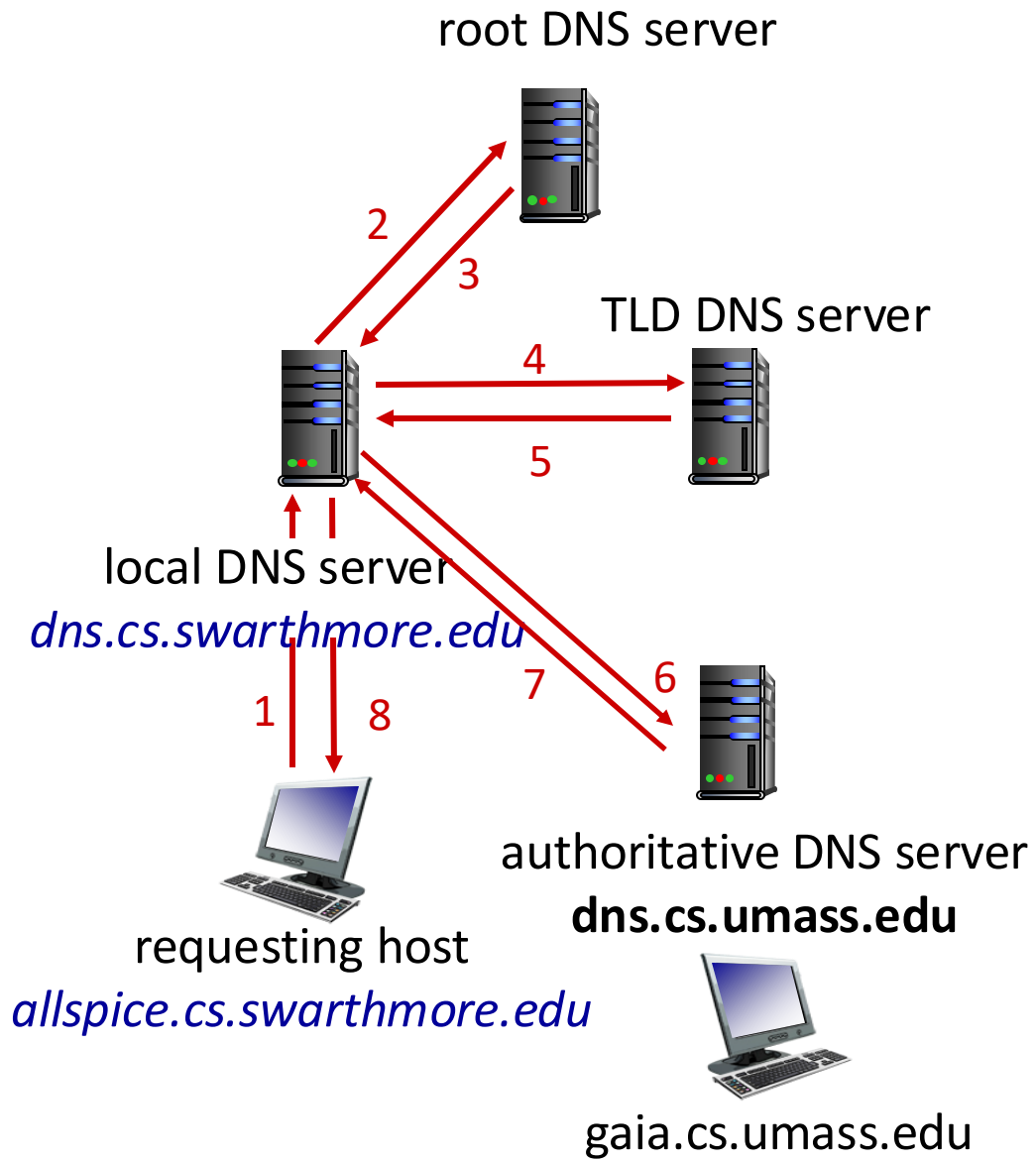
DNS security

DNS Vulnerabilities:

- No authentication
- Connectionless transport layer protocol (UDP)

DNS Attacks:

- Amplification Attack
- Cache Poisoning
- Man-in-the-middle
- DNS Redirection
- DDoS
- DNS Injection



Attacking DNS

DDoS attacks

- Bombard root servers with traffic
  - Not successful to date
  - Traffic Filtering
  - Local DNS servers cache IPs of TLD servers, bypassing root
- Bombard TLD servers
  - Potentially more dangerous

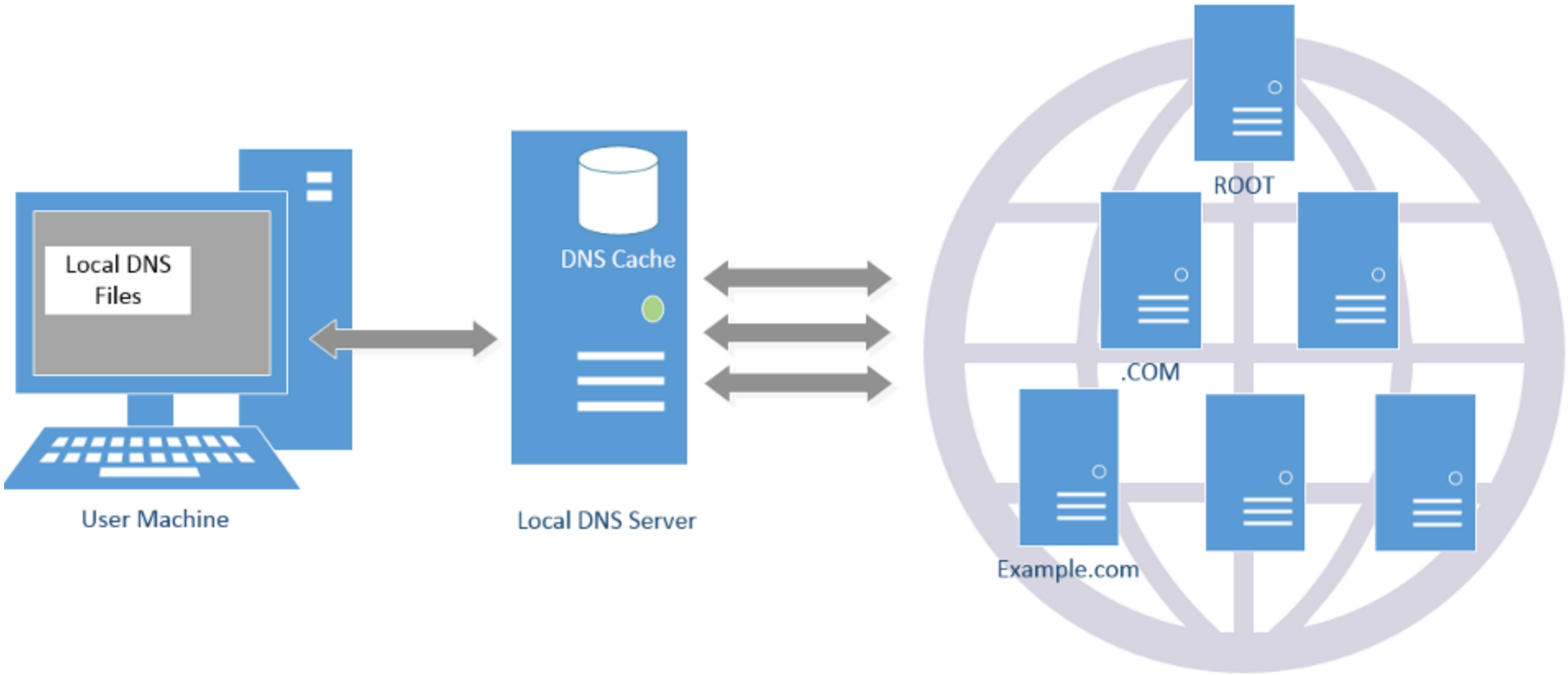
Redirect attacks

- Man-in-middle
  - Intercept queries
- DNS poisoning
  - Send bogus replies to DNS server that caches

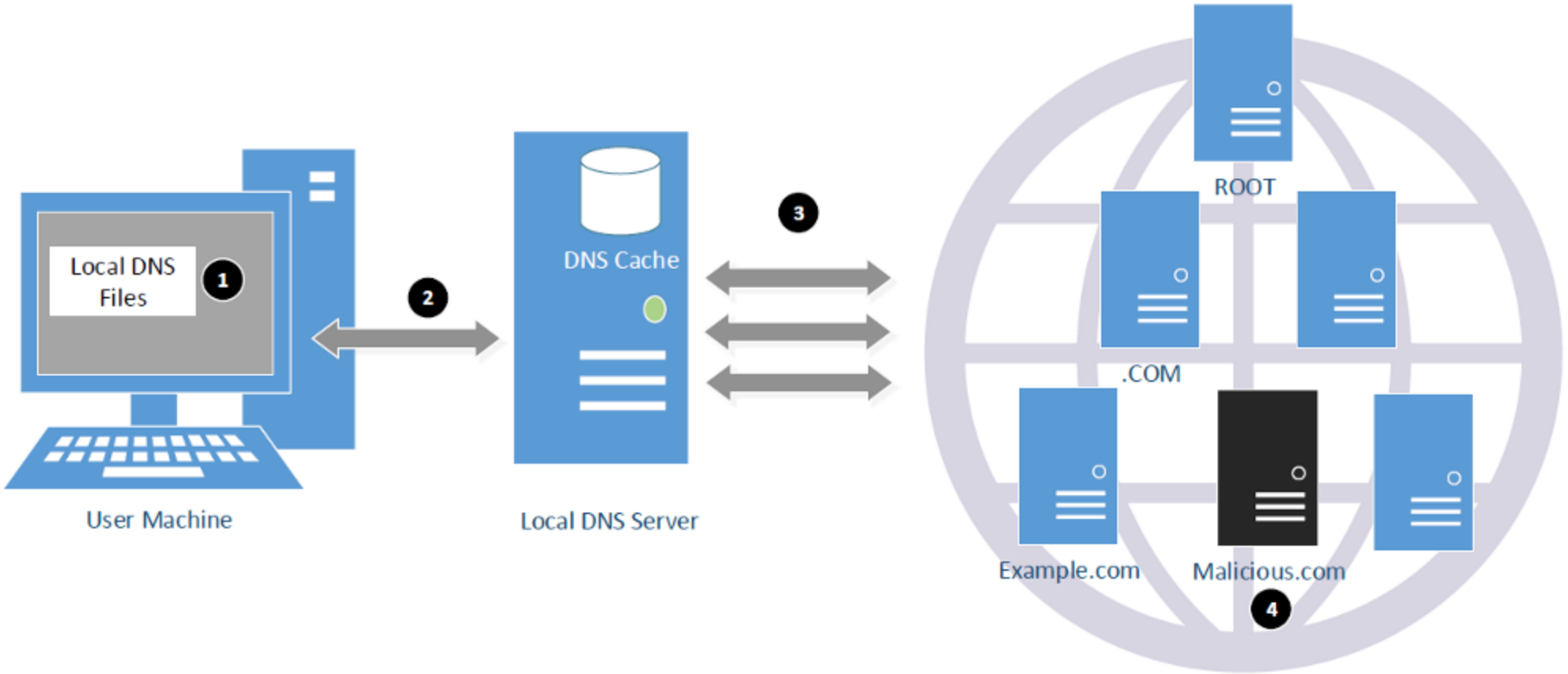
Exploit DNS for DDoS

- Send queries with spoofed source address: target IP
- Requires amplification

DNS Query Process and Cache



Attack Surface Overview



Denial Of Service

- Flood DNS servers with requests until they fail
- October 2002: massive DDoS against the root name servers
  - What was the effect?
  - … users didn't even notice
  - Root zone file is cached almost everywhere
- More targeted attacks can be effective
  - Local DNS server → cannot access DNS
  - Authoritative server → cannot access domain

DNS Hijacking

- Infect their OS or browser with a virus/trojan
  - e.g. Many trojans change entries in /etc/hosts
  - *.bankofamerica.com → evilbank.com
- Man-in-the-middle

  - Response Spoofing
    - Eavesdrop on requests
    - Outrace the servers response

Worksheet: Attacking DNS

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?

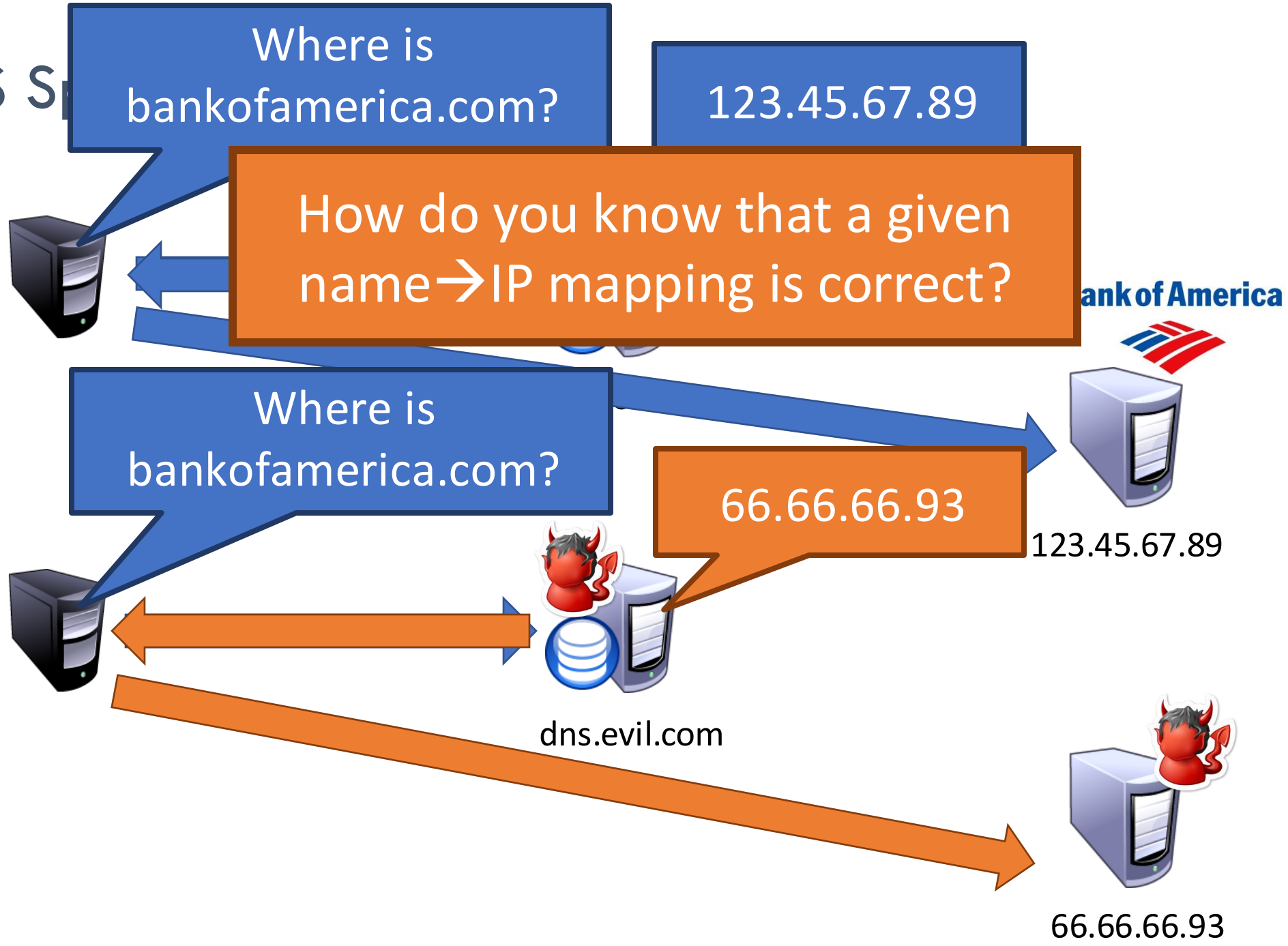
Legitimate Response:

```
; ; <<>> 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
```

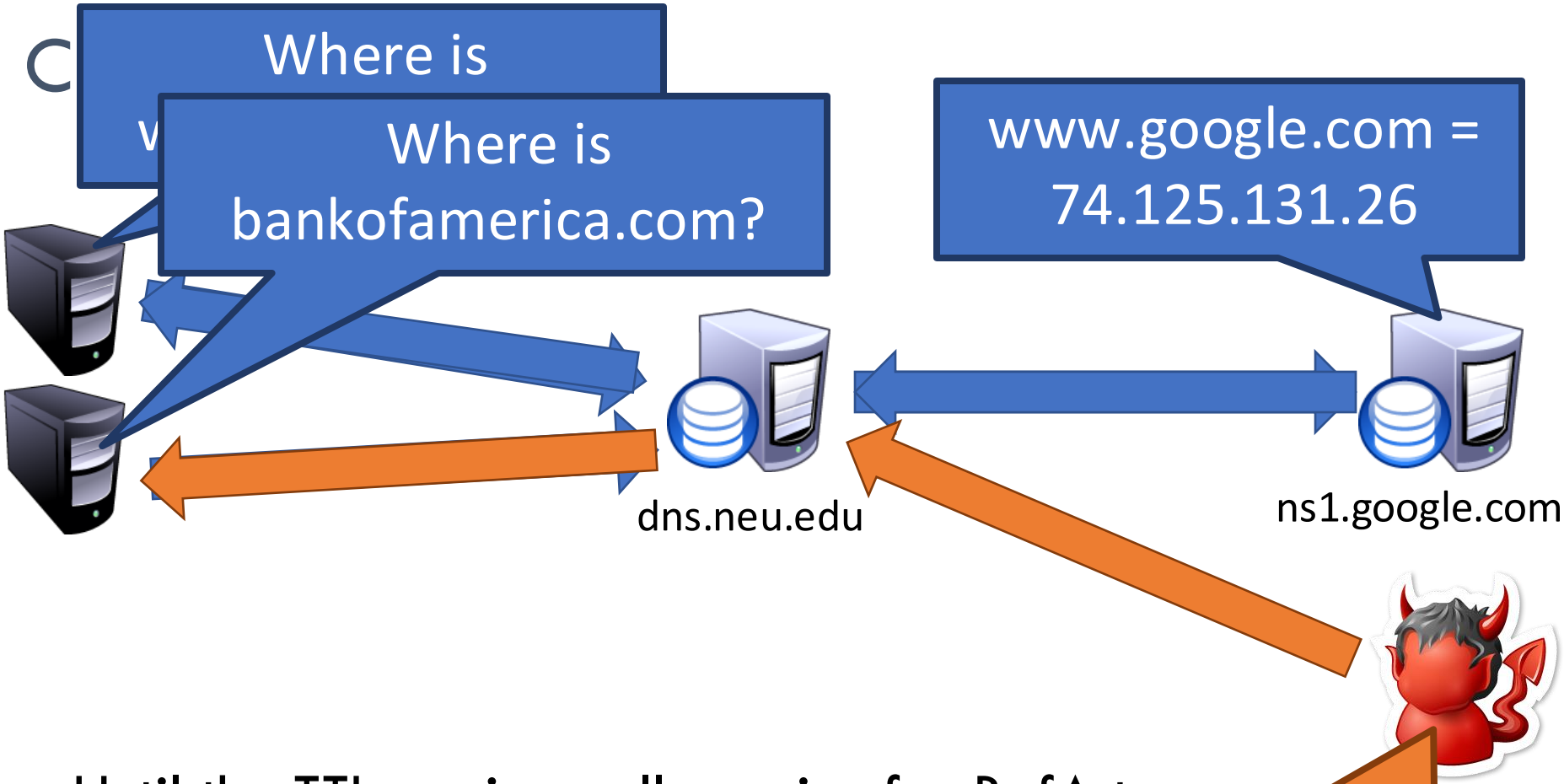
Poisoned DNS Response:

```
; ; <<>> 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
```

DNS S

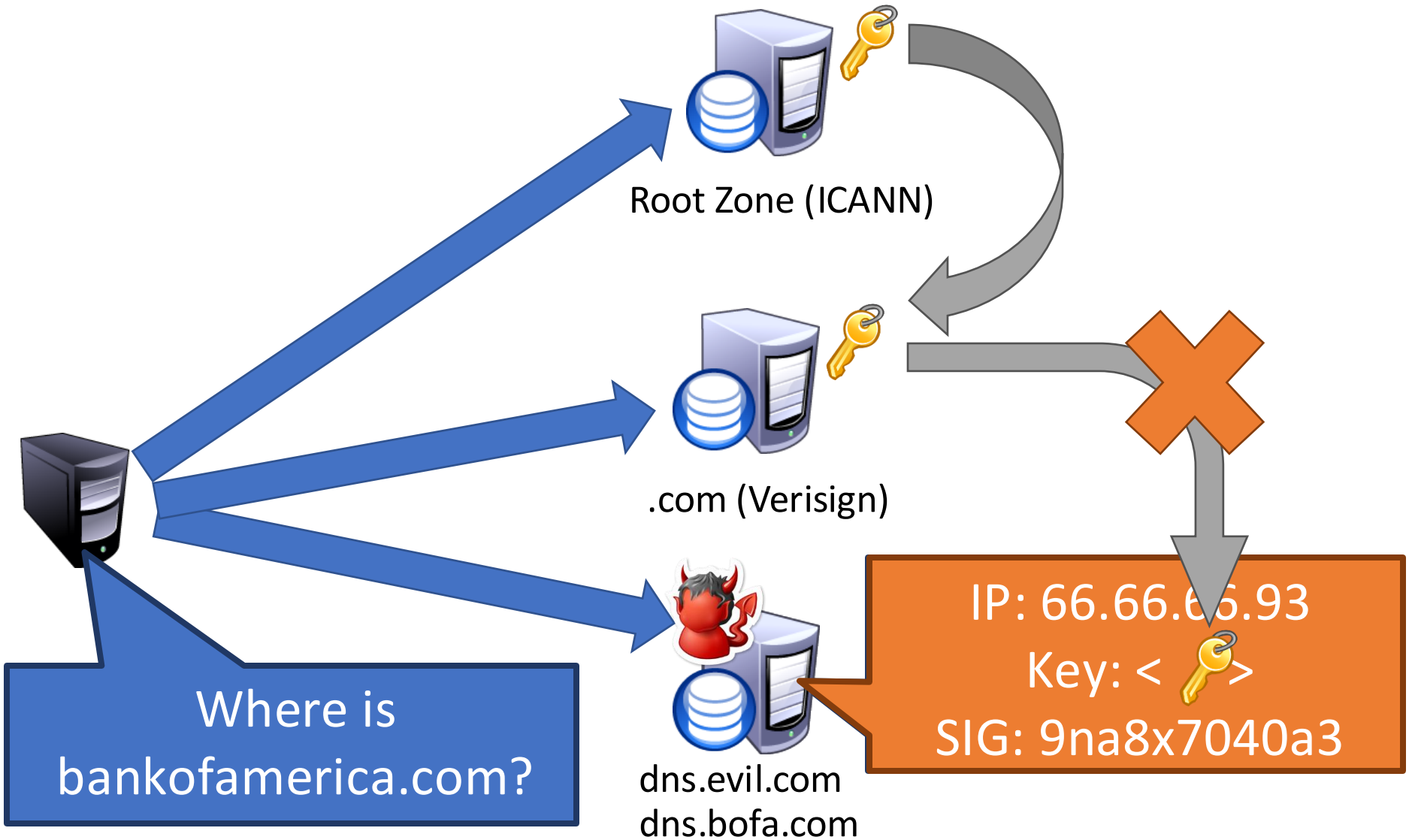

Where is bankofamerica.com?
123.45.67.89
How do you know that a given name→IP mapping is correct?
ank of America
Where is bankofamerica.com?
66.66.66.93
123.45.67.89
dns.evil.com
66.66.66.93

DNS C



- Until the TTL expires, all queries for BofA to dns.neu.edu will return poisoned re
- Much worse than spoofing/man-in-
  - Whole ISPs can be impacted!

DNSSEC Hierarchy of Trust



Solution: DNSSEC

- Cryptographically sign critical resource records
  - Resolver can verify the cryptographic signature
- Two new resource types
  - Type = DNSKEY
    - Name = Zone domain name
    - Value = Public key for the zone
  - Type = RRSIG
    - Name = (type, name) tuple, i.e. the query itself
    - Value = Cryptographic signature of the query results

Creates a hierarchy of trust within each zone

Prevents hijacking and spoofing

Let's talk a little bit about SMTP…

Try SMTP interaction for yourself:

- **`telnet allspice.cs.swarthmore.edu 25`**
- You should see a 220 reply from the server.
- enter HELO, MAIL FROM, RCPT TO, DATA, QUIT commands

(lets you send email without using email client (MUA))

Demo

Sample SMTP interaction

```
$ telnet allspice.cs.swarthmore.edu 25
Trying 130.58.68.9…
Connected to allspice.cs.swarthmore.edu
220 allspice.cs.swarthmore.edu ESMTP Postfix
HELO cs.swarthmore.edu
250 allspice.cs.swarthmore.edu
MAIL FROM:<rware@cs.swarthmore.edu>
250 2.1.0 OK
RCPT TO:<rware@cs.swarthmore.edu>
250 2.1.5 OK
DATA
354 End data with <CR><LF>.<CR><LF>
To: Ranysha Ware <rware@cs.swarthmore.edu>
From: Ranysha Ware <rware@cs.swarthmore.edu>
Subject: Telnet test message

This is a test message, via telnet, to myself.
.
```

Sample SMTP interaction

$ telnet allspice.cs.swarthmore.edu 25
Trying 130.58.68.9…
Connected to allspice.cs.swarthmore.edu
220 allspice.cs.swarthmore.edu ESMTP Postfix
HELO cs.swarthmore.edu
250 allspice.cs.swarthmore.edu
MAIL FROM:<rware@cs.swarthmore.edu>
250 2.1.0 OK
RCPT TO:<rware@cs.swarthmore.edu>
250 2.1.5 OK
DATA
354 End data with <CR><LF>.<CR><LF>
To: Ranysha Ware <rware@cs.swarthmore.edu>
From: Ranysha Ware <rware@cs.swarthmore.edu>
Subject: Telnet test message

This is a test message, via telnet, to myself.

End of message:
CRLF (Dot) CRLF

What keeps us from entering a fake information (e.g., FROM address)?

A. Nothing.

B. The MTA checks that the FROM is valid.

C. We enter a name/password logging into the MTA.

Fun Demo