Sean Blanchard

3/3/2021

COMP429

L05: IP Addresses and Routing
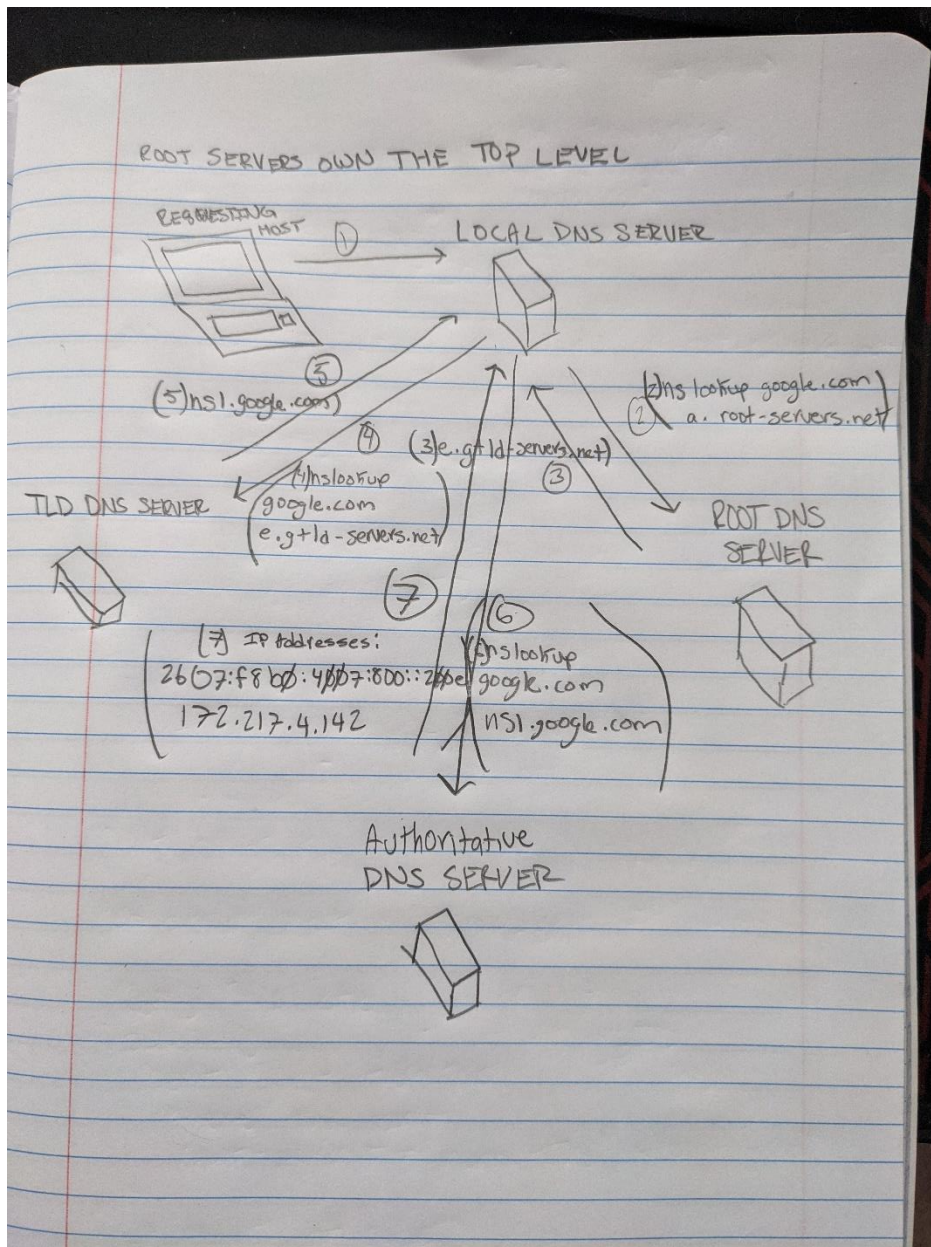
Task 1: Enumeration

1. What is your computers IP address?
   192.168.0.23
2. What is your address on the global Internet?
   **107.185.56.212**

Task 2: DNS is Hierarchical

- Use `nslookup [host] [dns server]` on Windows
- Use `nslookup -type=any [host] [dns server]` on macOS
- Use `you can figure it out yourself` on *nix.
1. Draw a diagram of a DNS request to resolve `google.com`.
   - o It should look like the diagram in Figure 2.19 from the textbook.
   - o Query `a.root-servers.net` as the root DNS server.
   - o The `a.root-servers.net` response will contain a list of TLD DNS servers (Top Level Domain), pick one of them and query that server.
   - o The TLD DNS server will return a DNS server related to google at this point. Pick one and query that server.
   - o Google's DNS server will return an IP address similar to the result from `nslookup google.com`.
   - o Use the information from the queries above to fill in your diagram with real data.

ROOT SERVERS OWN THE TOP LEVEL

REQUESTING HOST ① → LOCAL DNS SERVER

(5) ns1.google.com

dns lookup google.com ② a.root-servers.net

(3) e.gtld-servers.net ③

④ dns lookup google.com e.gtld-servers.net

TLD DNS SERVER

ROOT DNS SERVER

⑦ IP addresses: 2607:f8 b0:4007:800::206e 172.217.4.142

⑥ dns lookup google.com ns1.google.com

Authoritative DNS SERVER

2. What is the TLD (Top Level Domain) DNS server for `csuci.edu`?
l.edu-servers.net
Internet Address = 192.41.162.30
Has AAAA address 2001:500:d937::30

Task 3: NATty Lite

- You need Wireshark for this question.
- Using www.ipchicken.com draw a diagram like Figure 4.25 in the textbook.
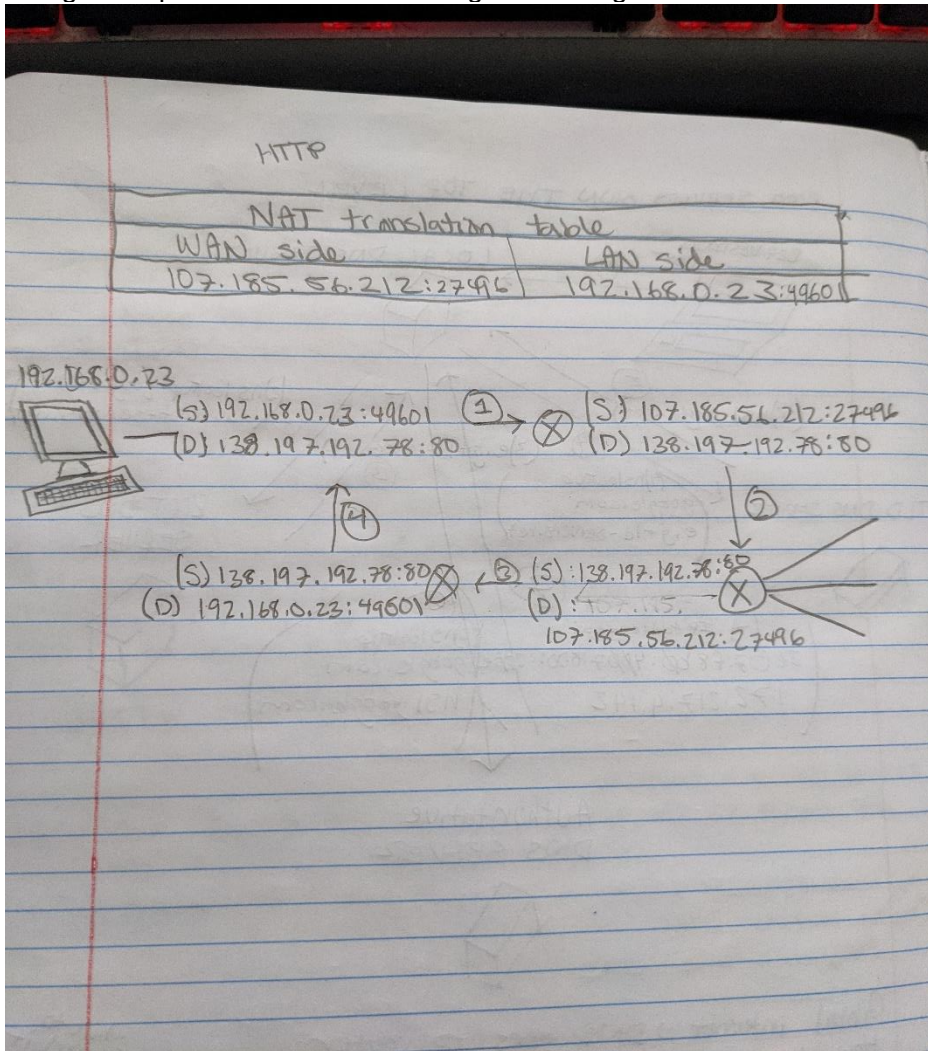
Task 4: Linux Networking

1. Remote into your Linux Virtual Machine (IT, use 421 VM):
   - `ssh -p 2222 student@localhost`
   - Using `ss` on the Linux VM, list the unique socket tuples for all connections.
     - Submit the `ss` command and the socket tuples.
   - Using `netstat` on your host OS (windows or macOS), find the sockets associated with port 2222:
     - macOS: `netstat -nf inet -p tcp | egrep 2222`
     - Windows: `netstat -na | Select-String "2222"`
     - Submit the unique socket tuples.
   - VirtualBox is actually NAT'ing the traffic into your VM's network interface.
     - Draw a diagram like Figure 4.25 in the textbook with information.

```
$ ss
Netid   State   Recv-Q   Send-Q              Local Address:Port        Peer Address:Port
u_str   ESTAB   0        0       /var/run/dbus/system_bus_socket 13402  * 12744
u_str   ESTAB   0        0                     * 548140                 * 548141
u_str   ESTAB   0        0                     * 12806                  * 12807
u_str   ESTAB   0        0                     * 12350                  * 12351
u_str   ESTAB   0        0                     * 548141                 * 548140
u_str   ESTAB   0        0                     * 13056                  * 13057
u_str   ESTAB   0        0                     * 10994                  * 11226
u_str   ESTAB   0        0       /var/run/dbus/system_bus_socket 13403  * 12745
u_str   ESTAB   0        0                     * 13221                  * 13222
u_str   ESTAB   0        0                     * 12745                  * 13403
u_str   ESTAB   0        0                     * 12744                  * 13402
u_str   ESTAB   0        0                     * 12869                  * 12870
u_str   ESTAB   0        0                     * 447408                 * 447409
u_str   ESTAB   0        0                     * 447412                 * 447413
u_str   ESTAB   0        0                     * 447406                 * 447407
u_str   ESTAB   0        0                     * 447413                 * 447412
u_str   ESTAB   0        0                     * 538098                 * 538097
u_str   ESTAB   0        0                     * 447410                 * 447411
u_str   ESTAB   0        0                     * 447407                 * 447406
u_str   ESTAB   0        0                     * 447409                 * 447408
u_str   ESTAB   0        0       /run/systemd/journal/stdout 11226      * 10994
u_str   ESTAB   0        0                     * 538097                 * 538098
u_str   ESTAB   0        0                     * 447411                 * 447410
u_str   ESTAB   0        0                     * 468653                 * 468654
u_str   ESTAB   0        0                     * 468658                 * 468657
u_str   ESTAB   0        0       /run/systemd/journal/stdout 12351      * 12350
u_str   ESTAB   0        0                     * 468656                 * 468655
u_str   ESTAB   0        0                     * 468654                 * 468653
u_str   ESTAB   0        0                     * 468659                 * 468660
u_str   ESTAB   0        0                     * 468655                 * 468656
u_str   ESTAB   0        0       /run/systemd/journal/stdout 12807      * 12806
u_str   ESTAB   0        0                     * 468660                 * 468659
u_str   ESTAB   0        0                     * 468657                 * 468658
u_str   ESTAB   0        0                     * 538087                 * 538088
u_str   ESTAB   0        0       /run/systemd/journal/stdout 13894      * 13893
u_str   ESTAB   0        0                     * 538085                 * 538086
u_str   ESTAB   0        0                     * 448246                 * 448245
u_str   ESTAB   0        0       /run/systemd/journal/stdout 13057      * 13056
u_str   ESTAB   0        0                     * 538084                 * 538083
u_str   ESTAB   0        0                     * 448243                 * 448244
u_str   ESTAB   0        0                     * 538083                 * 538084
u_str   ESTAB   0        0                     * 448245                 * 448246
u_str   ESTAB   0        0                     * 13401                  * 13400
u_str   ESTAB   0        0                     * 547217                 * 0
u_str   ESTAB   0        0                     * 538082                 * 538081
u_str   ESTAB   0        0                     * 447423                 * 447422
u_str   ESTAB   0        0                     * 538086                 * 538085
u_str   ESTAB   0        0                     * 448244                 * 448243
u_str   ESTAB   0        0                     * 538088                 * 538087
u_str   ESTAB   0        0                     * 448247                 * 448248
u_str   ESTAB   0        0                     * 538081                 * 538082
```

```
u_str   ESTAB   0   0                                      * 447422              * 447423
u_str   ESTAB   0   0                                      * 13400               * 13401
u_str   ESTAB   0   0                                      * 13893               * 13894
u_str   ESTAB   0   0   /var/run/dbus/system_bus_socket 15181 * 15180
u_str   ESTAB   0   0                                      * 13449               * 13450
u_str   ESTAB   0   0                                      * 13427               * 13428
u_str   ESTAB   0   0                                      * 15143               * 15144
u_str   ESTAB   0   0        /run/systemd/journal/stdout 12870  * 12869
u_str   ESTAB   0   0        /run/systemd/journal/stdout 13222  * 13221
u_str   ESTAB   0   0   /var/run/dbus/system_bus_socket 13428 * 13427
u_str   ESTAB   0   0   /var/run/dbus/system_bus_socket 13450 * 13449
u_str   ESTAB   0   0                                      * 15180               * 15181
u_str   ESTAB   0   0        /run/systemd/journal/stdout 15144  * 15143
u_str   ESTAB   0   0                                      * 448248              * 448247
u_str   ESTAB   0   0                                      * 538614              * 538615
u_str   ESTAB   0   0                                      * 538618              * 538619
u_str   ESTAB   0   0                                      * 538615              * 538614
u_str   ESTAB   0   0                                      * 538617              * 538616
u_str   ESTAB   0   0                                      * 538619              * 538618
u_str   ESTAB   0   0                                      * 538616              * 538617
tcp     ESTAB   0   0                      10.0.2.15:ssh           10.0.2.2:50776
```

```
C:\Users\sean1>netstat -na | findstr "2222"
  TCP    0.0.0.0:2222          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:2222        127.0.0.1:50776       ESTABLISHED
  TCP    127.0.0.1:50776       127.0.0.1:2222        ESTABLISHED
```


Handwritten notes:

Tuple:
- local / Port: 10.0.2.15:22 (ssh'ed into) → server IP address
- Peer / Port: 10.0.2.2:50776 → port that is connecting from comp
  - IP address that connected from

NAT translation table

WAN side	LAN side
10.0.2.2.1:50776	127.0.0.1:50776

(S) 127.0.0.1:50776   ① → (X)   (S) 10.0.2.2:50776
(D) 127.0.0.1:2222   (D) 127.0.0.1:2222
                                         ↓ ②
                                        (X)
            ④ ↑   ↓
(S): 127.0.0.1:2222 ← ③   (S): 127.0.0.1:2222
(D):127.0.0.1:50776   (D) 10.0.2.2:50776