Study of Network Diagnostics Tools Part-2
Experiment No: AV-341-2025-Lab-2

Saurabh Kumar
SC22B146
February 03, 2025

Date and Time of experiment: January 27, 2025, 14:45 IST

Objectives

- To study the network diagnostic tools: `route`, `netstat`, and `nslookup`.
- Use the network diagnostic tools in your network and understand the various options.

Tools Used

- PC: 12th Gen Intel(R) Core(TM) i5-1240P 1.70 GHz, Windows 11, 64-bit, (Reduced to) 4 GB RAM
- Software used: Command Prompt

Procedure

1. Open the Command Prompt on Windows PC.
2. Use the `route` command to view and manipulate the network routing tables.

Figure 1: `route` command on Command Prompt

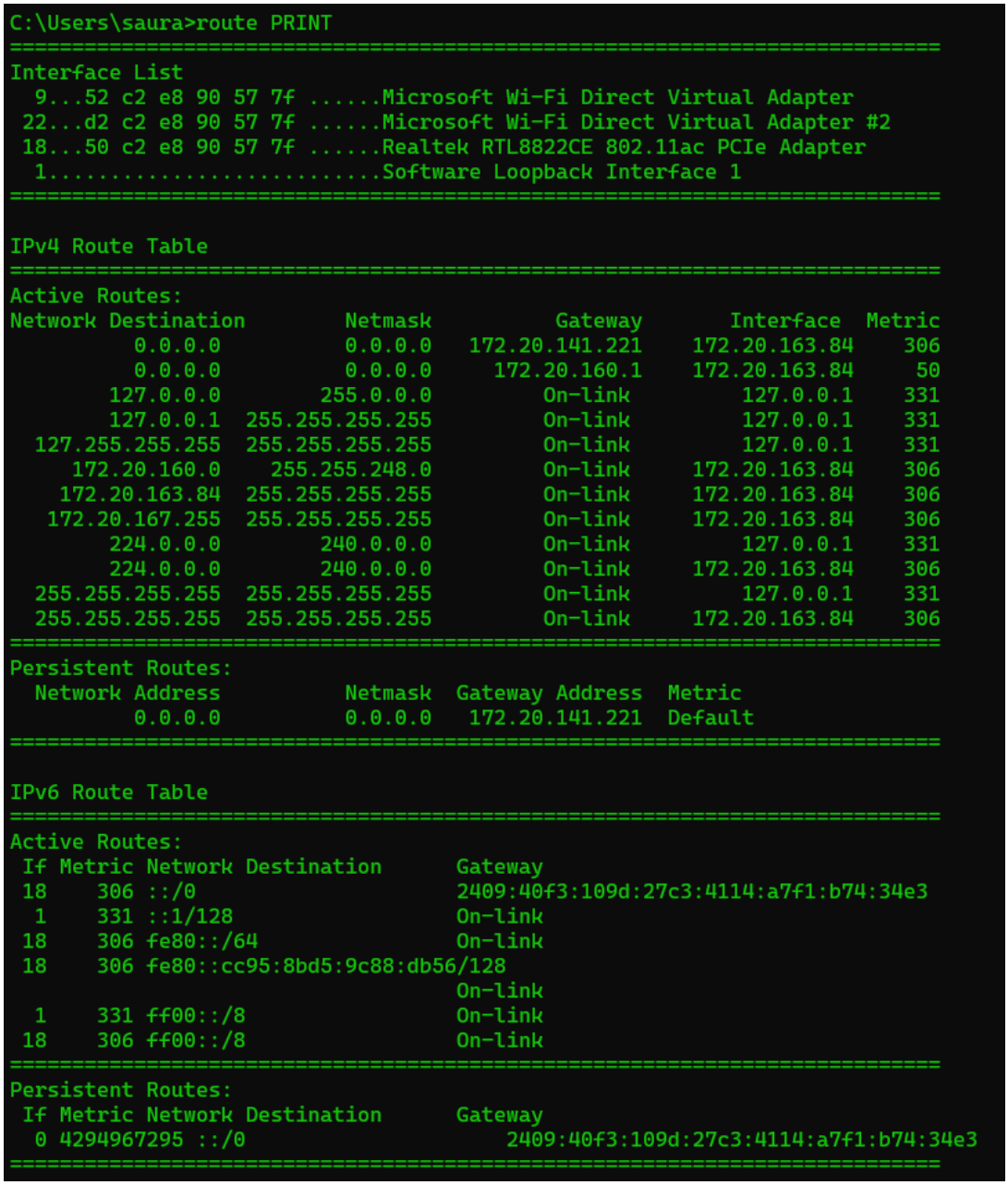

Figure 2: Displaying the current routing table

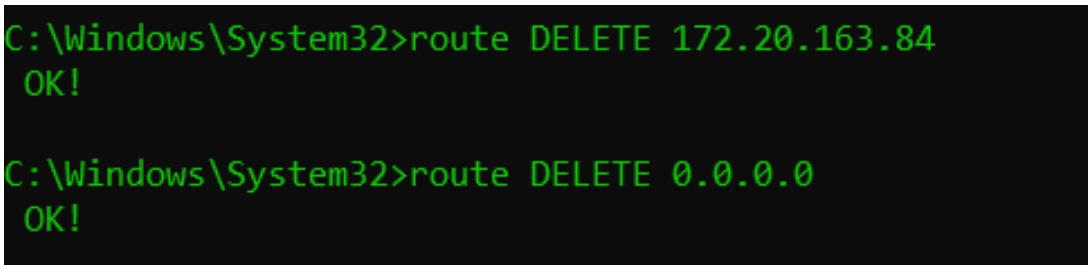

Figure 3: Deleting a route

3. Use the `netstat` command to view network interfaces, connections and ports on which the device is listening.

```
C:\Windows\System32>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49709        LAPTOP-46A3NN66:49710  ESTABLISHED
  TCP    127.0.0.1:49710        LAPTOP-46A3NN66:49709  ESTABLISHED
  TCP    127.0.0.1:49711        LAPTOP-46A3NN66:49712  ESTABLISHED
  TCP    127.0.0.1:49712        LAPTOP-46A3NN66:49711  ESTABLISHED
  TCP    172.20.163.84:49414    20.198.119.84:https    ESTABLISHED
  TCP    172.20.163.84:49415    20.198.119.84:https    ESTABLISHED
  TCP    172.20.163.84:51208    64:https               ESTABLISHED
  TCP    172.20.163.84:51213    151.101.193.91:https   ESTABLISHED
  TCP    172.20.163.84:51224    151.101.1.91:https     ESTABLISHED
  TCP    172.20.163.84:51234    whatsapp-cdn-shv-03-bom2:https  CLOSE_WAIT
  TCP    172.20.163.84:51235    whatsapp-cdn-shv-02-tir3:https  CLOSE_WAIT
  TCP    172.20.163.84:51236    180.149.62.34:https    CLOSE_WAIT
  TCP    172.20.163.84:51237    whatsapp-cdn-shv-04-bom2:https  CLOSE_WAIT
  TCP    172.20.163.84:51238    whatsapp-cdn-shv-01-bom2:https  CLOSE_WAIT
  TCP    172.20.163.84:51239    whatsapp-cdn-shv-01-bom2:https  CLOSE_WAIT
  TCP    172.20.163.84:51240    whatsapp-cdn-shv-02-bom2:https  CLOSE_WAIT
  TCP    172.20.163.84:51241    whatsapp-cdn-shv-01-bom1:https  CLOSE_WAIT
  TCP    172.20.163.84:51242    whatsapp-cdn-shv-02-bom1:https  CLOSE_WAIT
  TCP    172.20.163.84:51256    sl-in-f188:https       ESTABLISHED
  TCP    172.20.163.84:51259    125:https              TIME_WAIT
  TCP    172.20.163.84:51260    125:https              TIME_WAIT
  TCP    172.20.163.84:51261    dns:https              TIME_WAIT
  TCP    172.20.163.84:51263    dns:https              TIME_WAIT
  TCP    172.20.163.84:51264    maa05s25-in-f14:https  TIME_WAIT
  TCP    172.20.163.84:51265    dns:https              TIME_WAIT
  TCP    172.20.163.84:51267    64:https               TIME_WAIT
  TCP    172.20.163.84:51268    150:https              TIME_WAIT
  TCP    172.20.163.84:51270    maa03s28-in-f4:https   TIME_WAIT
  TCP    172.20.163.84:51271    dns:https              TIME_WAIT
  TCP    172.20.163.84:51274    maa03s28-in-f4:https   TIME_WAIT
  TCP    172.20.163.84:51275    dns:https              TIME_WAIT
  TCP    172.20.163.84:51277    maa05s16-in-f10:https  TIME_WAIT
  TCP    172.20.163.84:51279    maa03s28-in-f4:https   TIME_WAIT
  TCP    172.20.163.84:51280    dns:https              TIME_WAIT
  TCP    172.20.163.84:51281    maa03s41-in-f10:https  TIME_WAIT
  TCP    172.20.163.84:51282    maa03s41-in-f10:https  TIME_WAIT
  TCP    172.20.163.84:51283    maa05s28-in-f14:https  TIME_WAIT
  TCP    172.20.163.84:51284    dns:https              TIME_WAIT
  TCP    172.20.163.84:51285    maa05s19-in-f14:https  TIME_WAIT
  TCP    172.20.163.84:51286    maa05s19-in-f14:https  TIME_WAIT
  TCP    172.20.163.84:51287    maa05s26-in-f3:https   TIME_WAIT
  TCP    172.20.163.84:51288    maa05s25-in-f3:https   TIME_WAIT
```

Figure 4: `netstat` command on Command Prompt

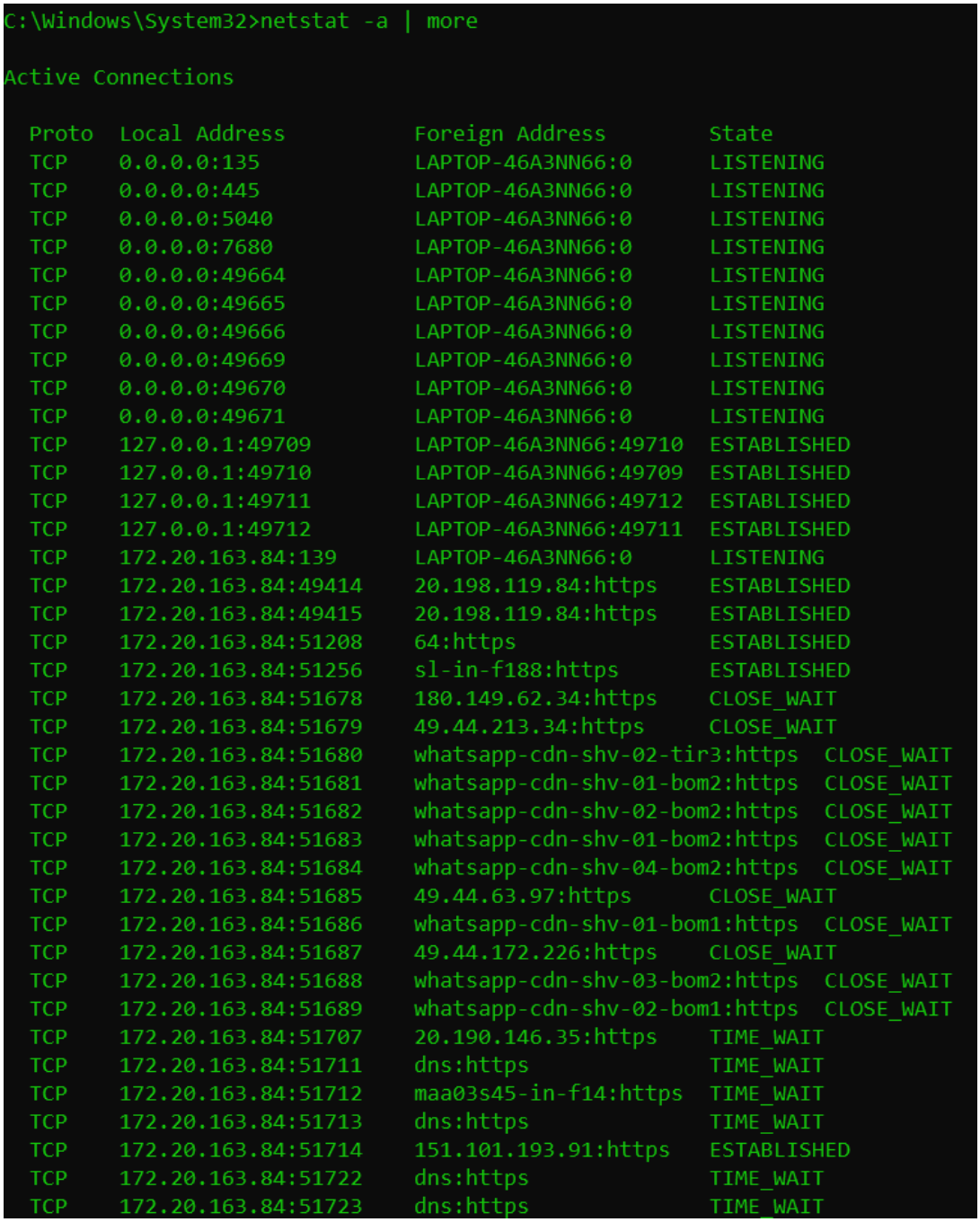

Figure 5: `netstat -a` command on Command Prompt

4. Use the `nslookup` command to identify the the domain name and ip address from the DNS (Domain Name Server) server.

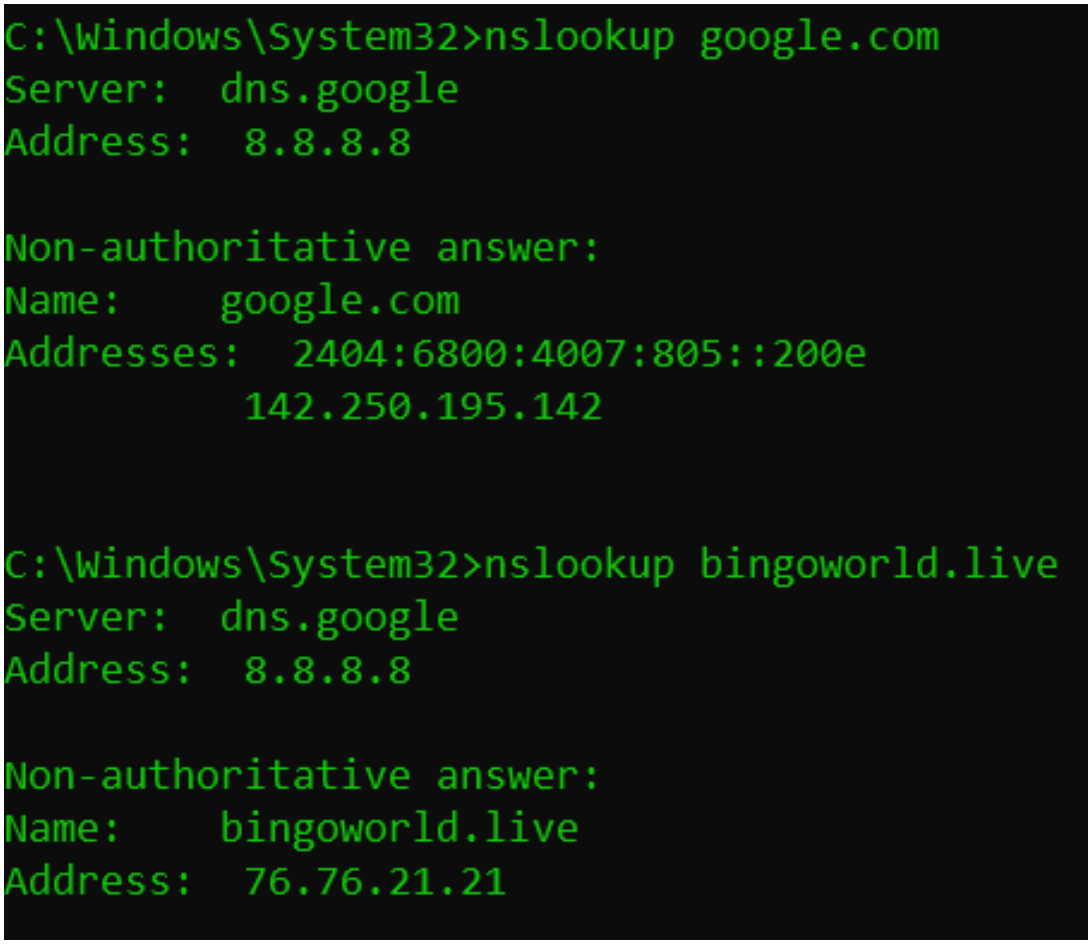

Figure 6: Querying a domain using `nslookup` command

Observations

- The `route` command is used to manipulate the network routing tables which contain the list of networks the device is connected to.
  - `PRINT` option can be used to display all the network routes the device is currently connected to.
  - `DELETE` option can be used to delete a connected network route.
- The `netstat` command is used to display detailed network status information such as active TCP connections, ports on which the computer is listening, Ethernet statistics and other network interfaces. It can be used for security purposes and to block unwanted traffic.
  - Using options like `-a`, we can display all TCP as well as UDP connections.
- The `nslookup` (name service/server lookup) command is used for looking into the domain name and ip address of a particular domain. It can be used locally for identifying different services.

Conclusions

- The network diagnostic tools like `route`, `netstat`, and `nslookup` can be used for viewing, manipulating, and diagnosing network connections, and servers and services.
- Each tool provides unique and valuable information to understand and change the state of the networks and services.