

# 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.

```

C:\Users\saura>route

Manipulates network routing tables.

ROUTE [-f] [-p] [-4|-6] command [destination]
      [MASK netmask] [gateway] [METRIC metric] [IF interface]

-f          Clears the routing tables of all gateway entries. If this is
            used in conjunction with one of the commands, the tables are
            cleared prior to running the command.

-p          When used with the ADD command, makes a route persistent across
            boots of the system. By default, routes are not preserved
            when the system is restarted. Ignored for all other commands,
            which always affect the appropriate persistent routes.

-4          Force using IPv4.

-6          Force using IPv6.

command     One of these:
            PRINT      Prints a route
            ADD        Adds a route
            DELETE     Deletes a route
            CHANGE     Modifies an existing route

destination Specifies the host.
MASK          Specifies that the next parameter is the 'netmask' value.
netmask       Specifies a subnet mask value for this route entry.
            If not specified, it defaults to 255.255.255.255.
gateway       Specifies gateway.
interface     the interface number for the specified route.
METRIC        specifies the metric, ie. cost for the destination.

All symbolic names used for destination are looked up in the network database
file NETWORKS. The symbolic names for gateway are looked up in the host name
database file HOSTS.

If the command is PRINT or DELETE. Destination or gateway can be a wildcard,
(wildcard is specified as a star '*'), or the gateway argument may be omitted.

If Dest contains a * or ?, it is treated as a shell pattern, and only
matching destination routes are printed. The '*' matches any string,
and '?' matches any one char. Examples: 157.*.1, 157.*, 127.*, *224*.

Pattern match is only allowed in PRINT command.

Diagnostic Notes:
    Invalid MASK generates an error, that is when (DEST & MASK) != DEST.
    Example> route ADD 157.0.0.0 MASK 155.0.0.0 157.55.80.1 IF 1
             The route addition failed: The specified mask parameter is invalid. (Destination & Mask) != Destination.

Examples:

> route PRINT
> route PRINT -4
> route PRINT -6
> route PRINT 157*      .... Only prints those matching 157*

> route ADD 157.0.0.0 MASK 255.0.0.0 157.55.80.1 METRIC 3 IF 2
destination^    ^mask    ^gateway    metric^    ^
                                   Interface^

If IF is not given, it tries to find the best interface for a given
gateway.
> route ADD 3ffe::/32 3ffe::1

```

Figure 1: route command on Command Prompt

```

C:\Users\saura>route PRINT
=====
Interface List
  9...52 c2 e8 90 57 7f .....Microsoft Wi-Fi Direct Virtual Adapter
 22...d2 c2 e8 90 57 7f .....Microsoft Wi-Fi Direct Virtual Adapter #2
 18...50 c2 e8 90 57 7f .....Realtek RTL8822CE 802.11ac PCIe Adapter
 1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
    0.0.0.0                0.0.0.0        172.20.141.221    172.20.163.84     306
    0.0.0.0                0.0.0.0        172.20.160.1      172.20.163.84     50
   127.0.0.0             255.0.0.0           On-link          127.0.0.1     331
   127.0.0.1       255.255.255.255           On-link          127.0.0.1     331
 127.255.255.255  255.255.255.255           On-link          127.0.0.1     331
 172.20.160.0       255.255.248.0           On-link          172.20.163.84     306
 172.20.163.84     255.255.255.255           On-link          172.20.163.84     306
 172.20.167.255   255.255.255.255           On-link          172.20.163.84     306
   224.0.0.0       240.0.0.0           On-link          127.0.0.1     331
   224.0.0.0       240.0.0.0           On-link          172.20.163.84     306
 255.255.255.255  255.255.255.255           On-link          127.0.0.1     331
 255.255.255.255  255.255.255.255           On-link          172.20.163.84     306
=====
Persistent Routes:
Network Address          Netmask  Gateway Address  Metric
    0.0.0.0              0.0.0.0    172.20.141.221  Default
=====

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
 18   306 ::/0                2409:40f3:109d:27c3:4114:a7f1:b74:34e3
 1    331 ::1/128             On-link
 18   306 fe80::/64           On-link
 18   306 fe80::cc95:8bd5:9c88:db56/128
                                On-link
 1    331 ff00::/8             On-link
 18   306 ff00::/8             On-link
=====
Persistent Routes:
If Metric Network Destination      Gateway
 0 4294967295 ::/0                2409:40f3:109d:27c3:4114:a7f1:b74:34e3
=====

```

Figure 2: Displaying the current routing table

```

C:\Windows\System32>route DELETE 172.20.163.84
OK!

C:\Windows\System32>route DELETE 0.0.0.0
OK!

```

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

```
C:\Windows\System32>netstat -a | more
```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	LAPTOP-46A3NN66:0	LISTENING
TCP	0.0.0.0:445	LAPTOP-46A3NN66:0	LISTENING
TCP	0.0.0.0:5040	LAPTOP-46A3NN66:0	LISTENING
TCP	0.0.0.0:7680	LAPTOP-46A3NN66:0	LISTENING
TCP	0.0.0.0:49664	LAPTOP-46A3NN66:0	LISTENING
TCP	0.0.0.0:49665	LAPTOP-46A3NN66:0	LISTENING
TCP	0.0.0.0:49666	LAPTOP-46A3NN66:0	LISTENING
TCP	0.0.0.0:49669	LAPTOP-46A3NN66:0	LISTENING
TCP	0.0.0.0:49670	LAPTOP-46A3NN66:0	LISTENING
TCP	0.0.0.0:49671	LAPTOP-46A3NN66:0	LISTENING
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	172.20.163.84:139	LAPTOP-46A3NN66:0	LISTENING
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	172.20.163.84:51256	sl-in-f188:https	ESTABLISHED
TCP	172.20.163.84:51678	180.149.62.34:https	CLOSE_WAIT
TCP	172.20.163.84:51679	49.44.213.34:https	CLOSE_WAIT
TCP	172.20.163.84:51680	whatsapp-cdn-shv-02-tir3:https	CLOSE_WAIT
TCP	172.20.163.84:51681	whatsapp-cdn-shv-01-bom2:https	CLOSE_WAIT
TCP	172.20.163.84:51682	whatsapp-cdn-shv-02-bom2:https	CLOSE_WAIT
TCP	172.20.163.84:51683	whatsapp-cdn-shv-01-bom2:https	CLOSE_WAIT
TCP	172.20.163.84:51684	whatsapp-cdn-shv-04-bom2:https	CLOSE_WAIT
TCP	172.20.163.84:51685	49.44.63.97:https	CLOSE_WAIT
TCP	172.20.163.84:51686	whatsapp-cdn-shv-01-bom1:https	CLOSE_WAIT
TCP	172.20.163.84:51687	49.44.172.226:https	CLOSE_WAIT
TCP	172.20.163.84:51688	whatsapp-cdn-shv-03-bom2:https	CLOSE_WAIT
TCP	172.20.163.84:51689	whatsapp-cdn-shv-02-bom1:https	CLOSE_WAIT
TCP	172.20.163.84:51707	20.190.146.35:https	TIME_WAIT
TCP	172.20.163.84:51711	dns:https	TIME_WAIT
TCP	172.20.163.84:51712	maa03s45-in-f14:https	TIME_WAIT
TCP	172.20.163.84:51713	dns:https	TIME_WAIT
TCP	172.20.163.84:51714	151.101.193.91:https	ESTABLISHED
TCP	172.20.163.84:51722	dns:https	TIME_WAIT
TCP	172.20.163.84:51723	dns:https	TIME_WAIT

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.

```
C:\Windows\System32>nslookup google.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:     google.com
Addresses: 2404:6800:4007:805::200e
          142.250.195.142

C:\Windows\System32>nslookup bingoworld.live
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:     bingoworld.live
Address:  76.76.21.21
```

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.