Lab 2: Network Commands for Testing and Troubleshooting

Objective:

To familiarize with essential network commands used for testing and troubleshooting network connectivity issues.

Required Tools:

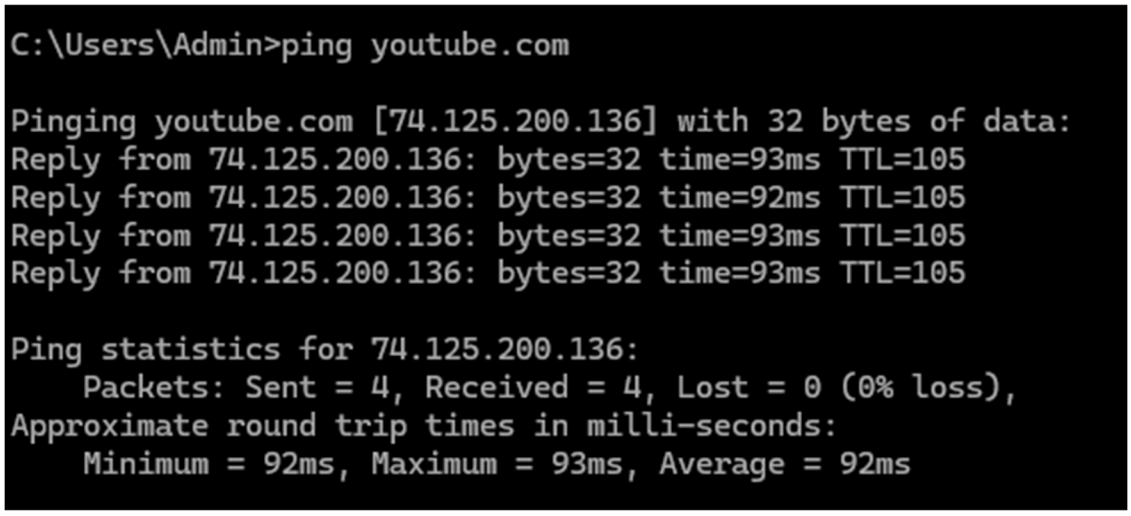
- A computer with command line interface (CLI) access
- Network connection (wired or wireless)

Network Commands:

Syntax and Usage of Common Network Commands:

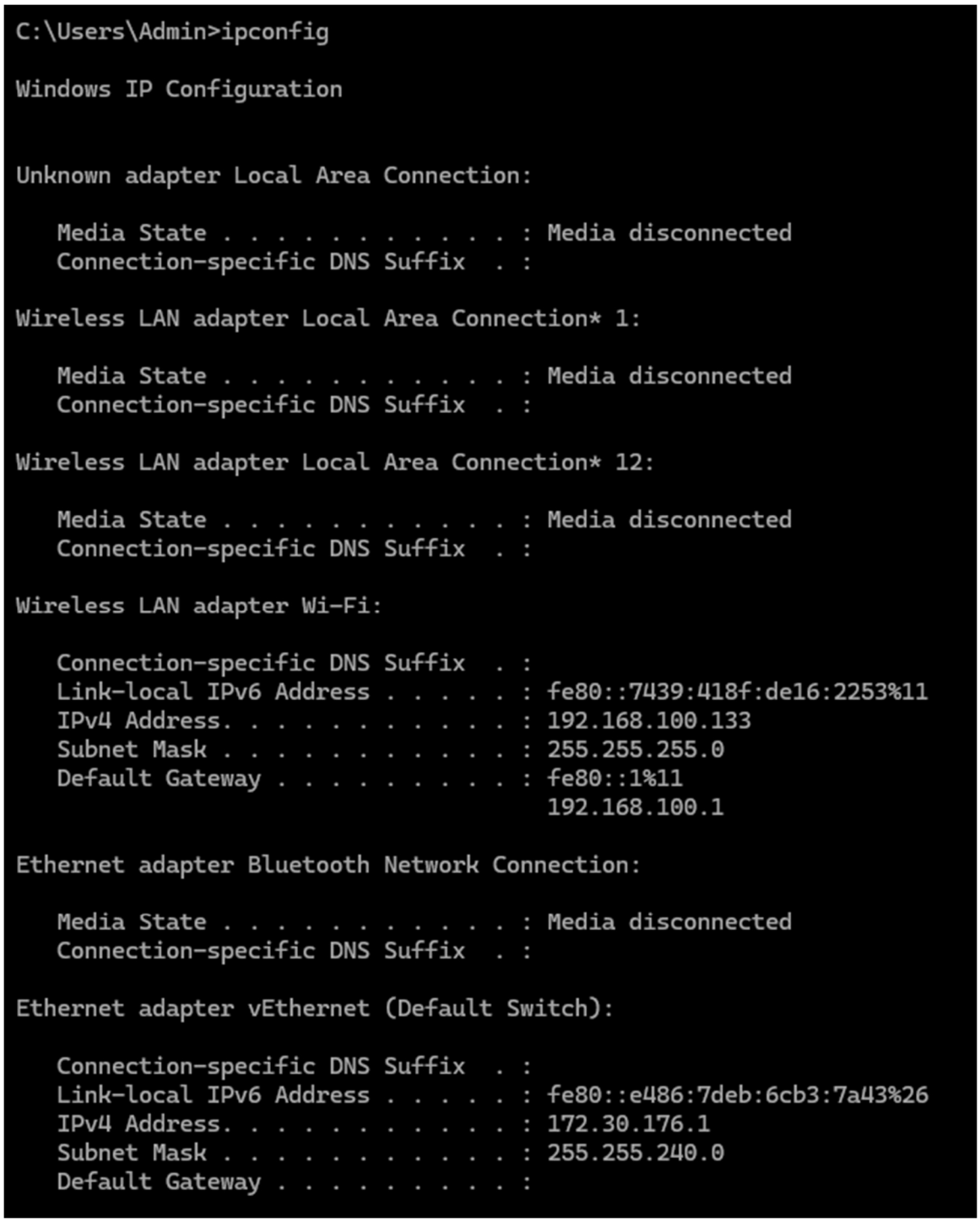
ping

- Syntax: ping [hostname or IP address]
- Usage: Tests the reachability of a host on an IP network and measures the round-trip time for messages sent from the originating host to a destination computer.



ipconfig (Windows) / ifconfig (Linux)

- Syntax: ipconfig or ifconfig
- Usage: Displays all current TCP/IP network configuration values and refreshes DHCP and DNS settings.



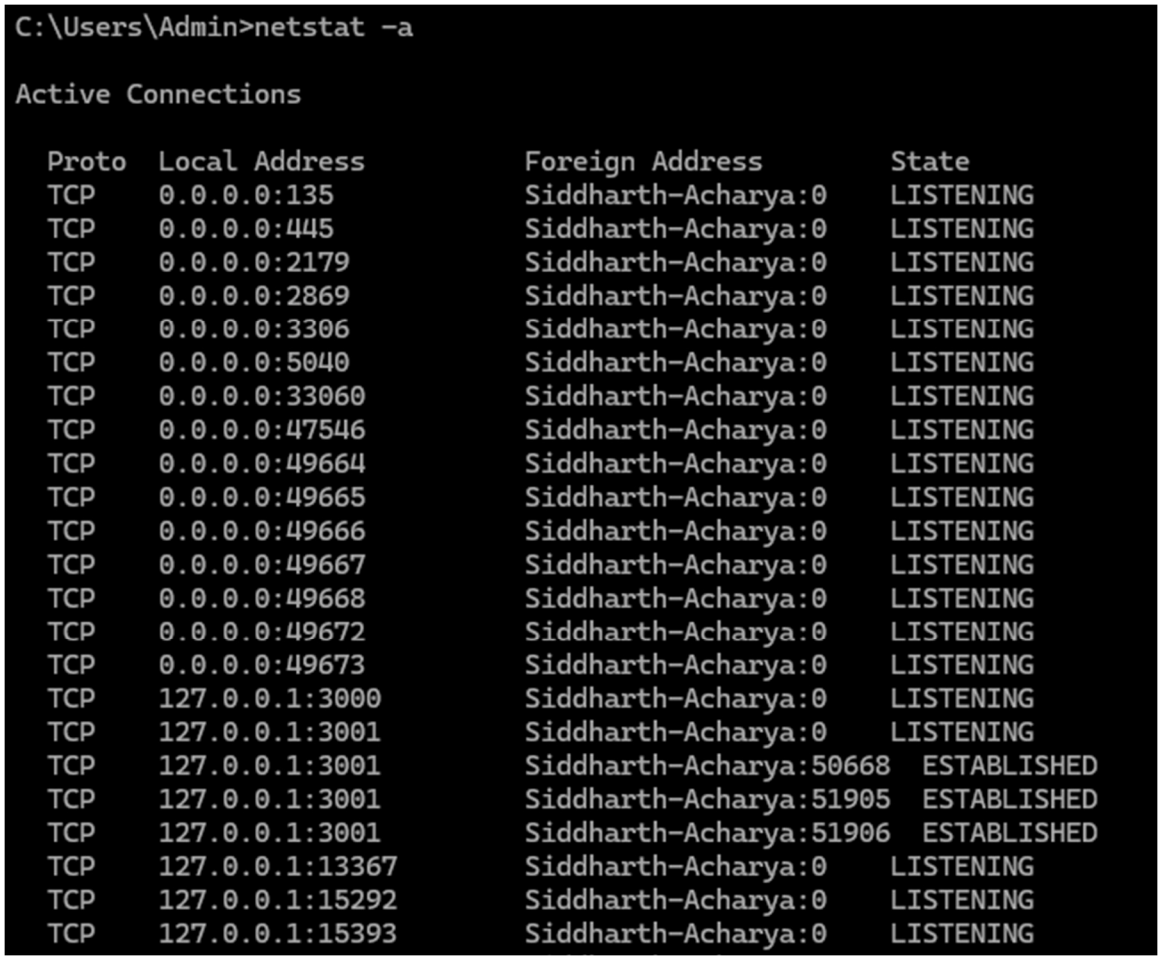
tracert (Windows) / traceroute (Linux)

- Syntax: tracert [hostname or IP address] or traceroute [hostname or IP address]
- Usage: Determines the route taken by packets to reach a specific host by listing all the intermediate routers.

```
C:\Users\Admin>tracert youtube.com

Tracing route to youtube.com [74.125.200.136]
over a maximum of 30 hops:

  1     2 ms   219 ms     6 ms  192.168.100.1
  2    16 ms    10 ms    11 ms  100.80.0.1
  3    12 ms    10 ms    10 ms  100.99.99.11
  4    10 ms    10 ms    10 ms  103.175.92.9
  5    14 ms    13 ms    14 ms  103.175.92.31
  6     *        *        *     Request timed out.
  7    28 ms    27 ms    28 ms  142.250.174.2
  8    23 ms    23 ms    22 ms  142.250.208.225
  9    26 ms    41 ms    27 ms  192.178.82.238
 10    35 ms    33 ms    37 ms  192.178.252.111
 11    69 ms    69 ms    76 ms  142.251.227.238
 12    95 ms    92 ms    99 ms  209.85.247.227
 13    95 ms    97 ms    98 ms  142.251.252.39
 14    94 ms    96 ms    99 ms  216.239.35.145
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24   100 ms   100 ms   100 ms  sa-in-f136.1e100.net [74.125.200.136]

Trace complete.
```

netstat

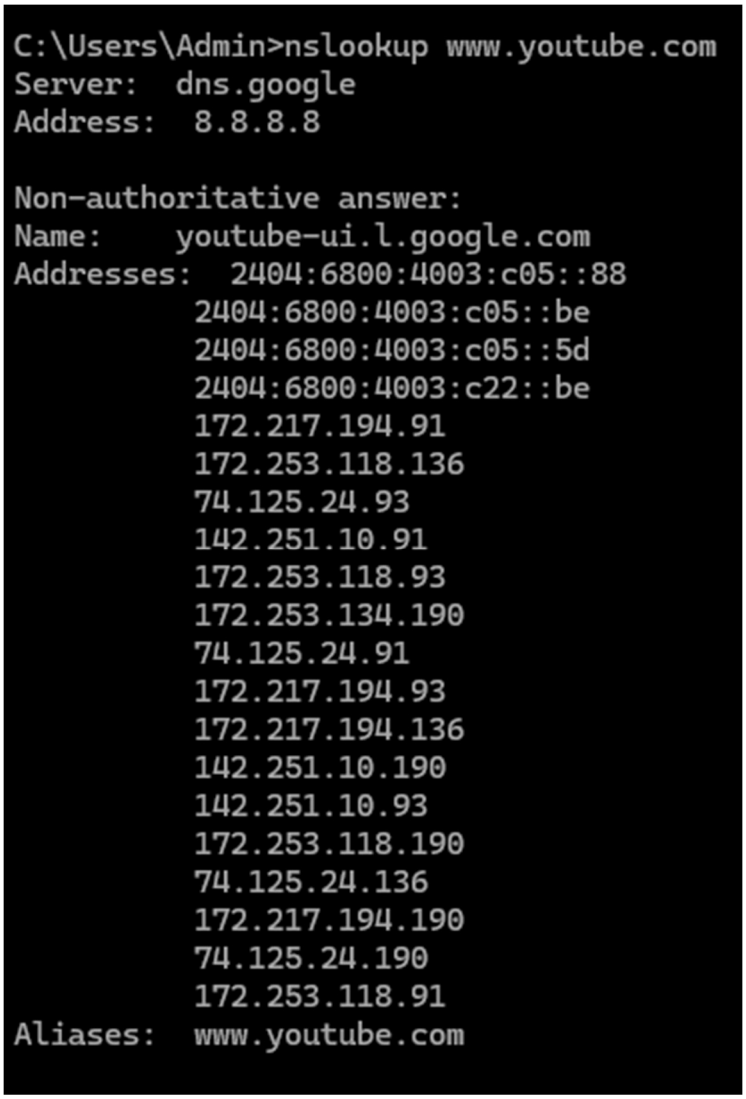
- Syntax: netstat -a or netstat -n
- Usage: Displays active TCP connections, ports on which the computer is listening, Ethernet statistics, and more.



```
C:\Users\Admin>netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:3001         127.0.0.1:50668        ESTABLISHED
  TCP    127.0.0.1:3001         127.0.0.1:51905        ESTABLISHED
  TCP    127.0.0.1:3001         127.0.0.1:51906        ESTABLISHED
  TCP    127.0.0.1:49670        127.0.0.1:49671        ESTABLISHED
  TCP    127.0.0.1:49671        127.0.0.1:49670        ESTABLISHED
  TCP    127.0.0.1:50668        127.0.0.1:3001         ESTABLISHED
  TCP    127.0.0.1:51905        127.0.0.1:3001         ESTABLISHED
  TCP    127.0.0.1:51906        127.0.0.1:3001         ESTABLISHED
  TCP    127.0.0.1:56414        127.0.0.1:58405        ESTABLISHED
  TCP    127.0.0.1:58405        127.0.0.1:56414        ESTABLISHED
  TCP    127.0.0.1:62931        127.0.0.1:62932        ESTABLISHED
  TCP    127.0.0.1:62932        127.0.0.1:62931        ESTABLISHED
  TCP    127.0.0.1:62933        127.0.0.1:62934        ESTABLISHED
  TCP    127.0.0.1:62934        127.0.0.1:62933        ESTABLISHED
  TCP    127.0.0.1:62953        127.0.0.1:62954        ESTABLISHED
  TCP    127.0.0.1:62954        127.0.0.1:62953        ESTABLISHED
  TCP    127.0.0.1:62955        127.0.0.1:62956        ESTABLISHED
  TCP    127.0.0.1:62956        127.0.0.1:62955        ESTABLISHED
  TCP    192.168.100.133:49442  4.213.25.242:443       ESTABLISHED
  TCP    192.168.100.133:51427  163.70.145.63:443      ESTABLISHED
  TCP    192.168.100.133:51735  163.70.145.13:443      ESTABLISHED
  TCP    192.168.100.133:51761  18.97.36.13:443        ESTABLISHED
  TCP    192.168.100.133:51948  8.8.8.8:53             TIME_WAIT
  TCP    192.168.100.133:51949  8.8.8.8:53             TIME_WAIT
  TCP    192.168.100.133:51951  8.8.8.8:53             TIME_WAIT
  TCP    192.168.100.133:51952  8.8.8.8:53             TIME_WAIT
  TCP    192.168.100.133:51953  8.8.8.8:53             TIME_WAIT
  TCP    192.168.100.133:51954  8.8.8.8:53             TIME_WAIT
  TCP    192.168.100.133:51955  34.84.0.87:443         ESTABLISHED
  TCP    192.168.100.133:51959  8.8.8.8:53             TIME_WAIT
  TCP    192.168.100.133:51960  8.8.8.8:53             TIME_WAIT
  TCP    192.168.100.133:52533  43.228.194.51:443      ESTABLISHED
  TCP    192.168.100.133:52745  172.64.148.235:443     ESTABLISHED
  TCP    192.168.100.133:53527  163.70.145.57:443      ESTABLISHED
  TCP    192.168.100.133:54037  18.97.36.5:443         ESTABLISHED
  TCP    192.168.100.133:54284  163.70.145.13:443      ESTABLISHED
  TCP    192.168.100.133:54693  54.80.219.230:443      ESTABLISHED
  TCP    192.168.100.133:55773  20.189.173.23:443      ESTABLISHED
  TCP    192.168.100.133:55775  74.125.24.188:5228     ESTABLISHED
  TCP    192.168.100.133:56052  18.97.36.13:443        ESTABLISHED
  TCP    192.168.100.133:56351  57.144.146.192:443     ESTABLISHED
  TCP    192.168.100.133:56411  8.8.8.8:53             TIME_WAIT
```

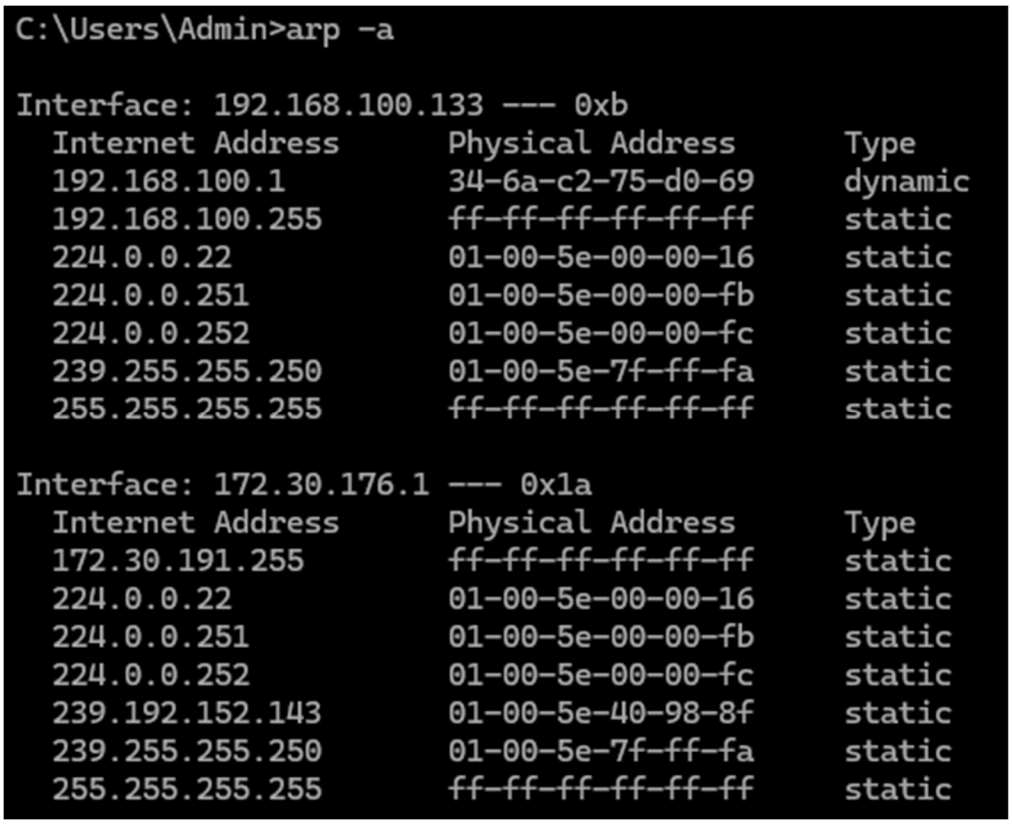
nslookup

- Syntax: nslookup [hostname]
- Usage: Queries the Domain Name System (DNS) to obtain domain name or IP address mapping information.



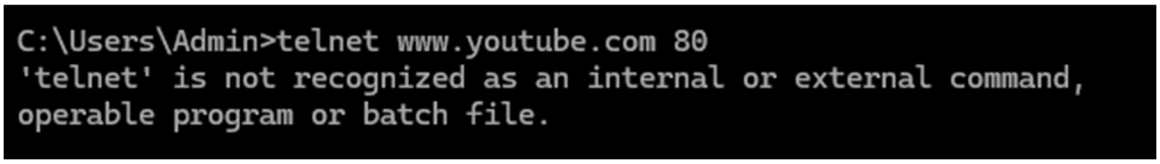
`arp

- Syntax: arp -a
- Usage: Displays and modifies the IP-to-Physical (MAC) address translation table used by the Address Resolution Protocol (ARP).



telnet

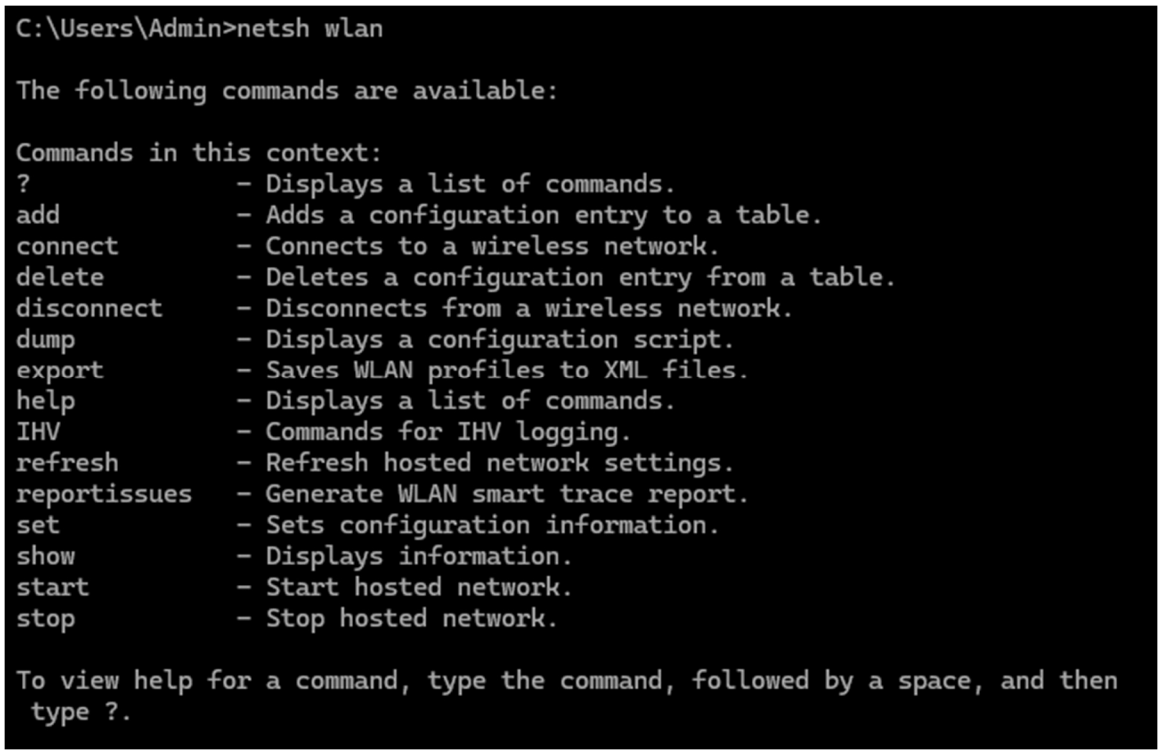
- Syntax: telnet [hostname or IP address] [port]
- Usage: Connects to a remote host using the Telnet protocol, useful for testing connectivity to specific ports.



//No output due to installation issue.

netsh wlan (Windows)

- Syntax: netsh wlan show profiles or netsh wlan connect name=[profile name]
- Usage: Manages wireless network profiles and connections on Windows systems.



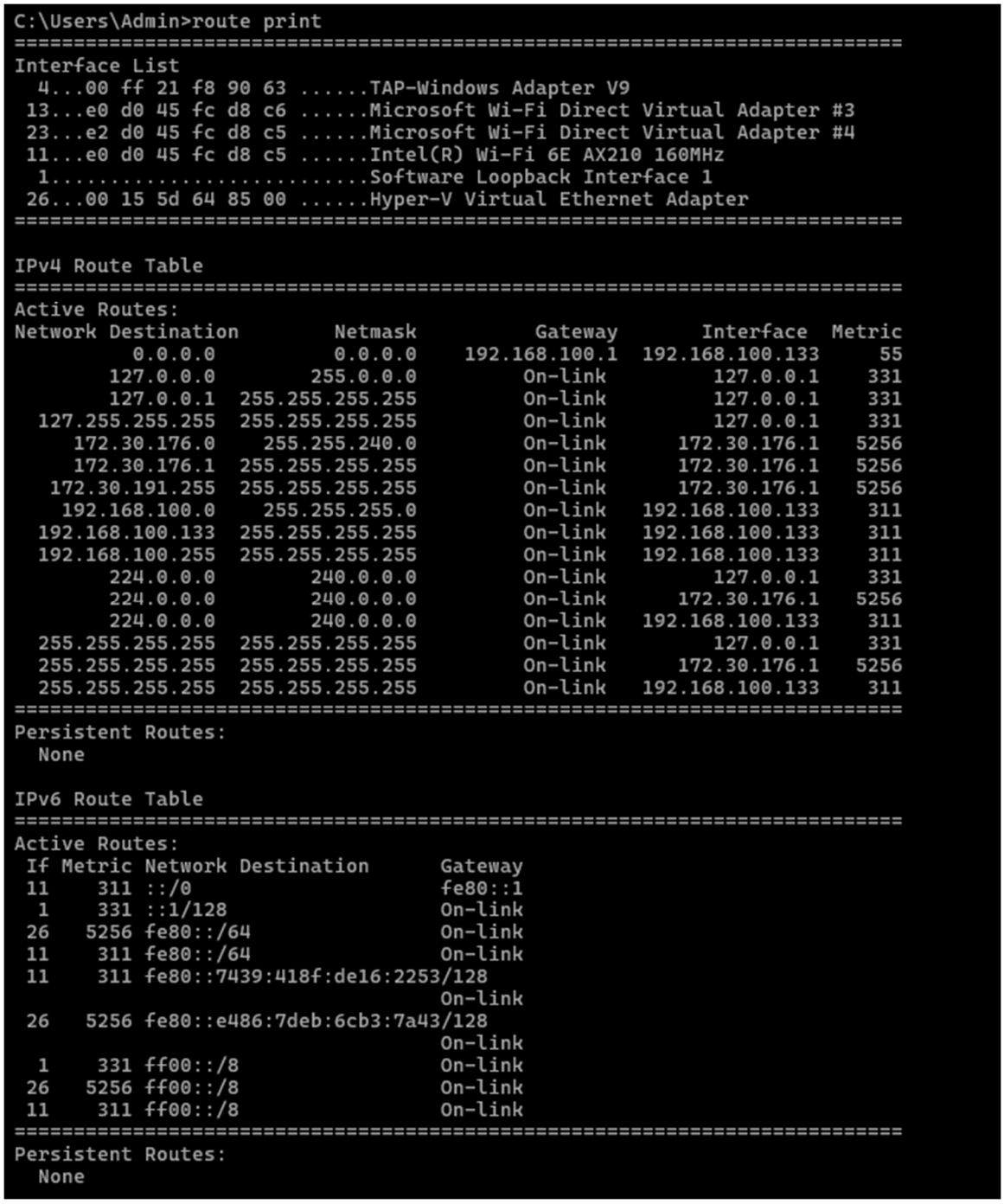
pathping

- Syntax: pathping [hostname or IP address]
- Usage: Combines the functionality of ping and tracert to provide information about network latency and packet loss at each hop.

```
C:\Users\Admin>pathping www.youtube.com

Tracing route to youtube-ui.l.google.com [172.253.118.136]
over a maximum of 30 hops:
  0  Siddharth-Acharya [192.168.100.133]
  1  192.168.100.1
  2  100.80.0.1
  3  100.99.99.11
  4  103.175.92.9
  5  103.175.92.31
  6  103.225.212.15
  7  142.250.174.2
  8  192.178.83.35
  9  216.239.54.92
 10  142.251.239.233
 11  142.251.227.234
 12  209.85.242.157
 13  209.85.255.128
 14  72.14.232.105
 15     *        *        *
Computing statistics for 350 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           Siddharth-Acharya [192.168.100.133]
                                    0/ 100 =  0%   |
  1   13ms     0/ 100 =  0%     0/ 100 =  0%  192.168.100.1
                                    0/ 100 =  0%   |
  2   17ms     0/ 100 =  0%     0/ 100 =  0%  100.80.0.1
                                    0/ 100 =  0%   |
  3   ---    100/ 100 =100%   100/ 100 =100%  100.99.99.11
                                    0/ 100 =  0%   |
  4   20ms     0/ 100 =  0%     0/ 100 =  0%  103.175.92.9
                                    0/ 100 =  0%   |
  5   20ms     0/ 100 =  0%     0/ 100 =  0%  103.175.92.31
                                    0/ 100 =  0%   |
  6   38ms     0/ 100 =  0%     0/ 100 =  0%  103.225.212.15
                                    0/ 100 =  0%   |
  7   32ms     0/ 100 =  0%     0/ 100 =  0%  142.250.174.2
                                    0/ 100 =  0%   |
  8   31ms     0/ 100 =  0%     0/ 100 =  0%  192.178.83.35
                                    0/ 100 =  0%   |
  9   32ms     0/ 100 =  0%     0/ 100 =  0%  216.239.54.92
                                    0/ 100 =  0%   |
 10  ---     100/ 100 =100%   100/ 100 =100%  142.251.239.233
                                    0/ 100 =  0%   |
 11   74ms     0/ 100 =  0%     0/ 100 =  0%  142.251.227.234
                                    0/ 100 =  0%   |
 12  ---     100/ 100 =100%   100/ 100 =100%  209.85.242.157
                                    0/ 100 =  0%   |
 13  103ms     0/ 100 =  0%     0/ 100 =  0%  209.85.255.128
                                    0/ 100 =  0%   |
 14  101ms     0/ 100 =  0%     0/ 100 =  0%  72.14.232.105

Trace complete.
```

route print

- Syntax: route print
- Usage: Displays the current IP routing table on the local machine.



```
C:\Users\Admin>route print
===========================================================================
Interface List
  4...00 ff 21 f8 90 63 ......TAP-Windows Adapter V9
 13...e0 d0 45 fc d8 c6 ......Microsoft Wi-Fi Direct Virtual Adapter #3
 23...e2 d0 45 fc d8 c5 ......Microsoft Wi-Fi Direct Virtual Adapter #4
 11...e0 d0 45 fc d8 c5 ......Intel(R) Wi-Fi 6E AX210 160MHz
  1...........................Software Loopback Interface 1
 26...00 15 5d 64 85 00 ......Hyper-V Virtual Ethernet Adapter
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.100.1  192.168.100.133     55
        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
     172.30.176.0    255.255.240.0         On-link      172.30.176.1   5256
     172.30.176.1  255.255.255.255         On-link      172.30.176.1   5256
   172.30.191.255  255.255.255.255         On-link      172.30.176.1   5256
    192.168.100.0    255.255.255.0         On-link   192.168.100.133    311
  192.168.100.133  255.255.255.255         On-link   192.168.100.133    311
  192.168.100.255  255.255.255.255         On-link   192.168.100.133    311
        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      172.30.176.1   5256
        224.0.0.0        240.0.0.0         On-link   192.168.100.133    311
  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      172.30.176.1   5256
  255.255.255.255  255.255.255.255         On-link   192.168.100.133    311
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
 11    311 ::/0                     fe80::1
  1    331 ::1/128                  On-link
 26   5256 fe80::/64                On-link
 11    311 fe80::/64                On-link
 11    311 fe80::7439:418f:de16:2253/128
                                    On-link
 26   5256 fe80::e486:7deb:6cb3:7a43/128
                                    On-link
  1    331 ff00::/8                 On-link
 26   5256 ff00::/8                On-link
 11    311 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

getmac

- Syntax: getmac
- Usage: Displays the MAC addresses for network adapters on the local machine.

```
C:\Users\Admin>getmac

Physical Address    Transport Name
=================== ============================================================
00-FF-21-F8-90-63   Media disconnected
E0-D0-45-FC-D8-C5   \Device\Tcpip_{6D85EB9B-9CF6-4220-9D52-A5CE24852D00}
```

nbtstat

- Syntax: nbtstat -a [hostname]
- Usage: Displays NetBIOS over TCP/IP statistics, including the NetBIOS name table of a remote computer.

whois

- Syntax: whois [domain name]
- Usage: Retrieves registration information about a domain name from the WHOIS database.

// Some outputs were not displayed due to recognition error.

Procedure

1. Open the command line interface (CLI) on your computer.
2. Use the ipconfig or ifconfig command to check your current network configuration.
3. Usage of the commands are shown in the output files.

Output

All the outputs are attached with the syntax and usage of respective commands.

Conclusion

This lab provided hands-on experience with various network commands essential for diagnosing and troubleshooting network issues. Mastery of these commands is crucial for network administrators and IT professionals to maintain network health and performance.