Bialystok University of Technology

Faculty of Electrical Engineering

LABORATORY REPORT

Computer Networks

IS-FEE-10082S

Subject:
Network Tools in Windows and Linux

Instructor: Andrzej Zankiewicz, PhD

Students:

Burak Düzenli

Bahadır Emre Yıldırım

Białystok, April 2025

Contents

1 Objective

The goal of this laboratory exercise is to familiarize students with basic and advanced network diagnostic and configuration tools available in Windows and Linux operating systems. This includes the usage of command-line utilities such as `ipconfig`, `ping`, `tracert`/`traceroute`, `netstat`, `arp`, `nslookup`, and also network traffic analysis software like Wireshark.

2 Equipment and Software Used

- Microsoft Windows 10

- Ubuntu Linux Distribution

- Wireshark (Latest version)

- Access to LAN/Internet

- Command-line interface (cmd / terminal)

3 Tasks and Results

3.1 IP Configuration

Windows

The command `ipconfig /all` was used to retrieve the IP configuration.

```
1  ipconfig /all
```

Listing 1: Windows IP Configuration

Result:

```
1  Windows IP Configuration
2
3     Host Name . . . . . . . . . . . . : DESKTOP-GK8G3P9
4     Primary Dns Suffix  . . . . . . . :
5     Node Type . . . . . . . . . . . . : Hybrid
6     IP Routing Enabled. . . . . . . . : No
7     WINS Proxy Enabled. . . . . . . . : No
8
9  Ethernet adapter Ethernet:
10
11     Media State . . . . . . . . . . . : Media disconnected
12     Connection-specific DNS Suffix  . :
13     Description . . . . . . . . . . . : Realtek PCIe GbE Family
          Controller
14     Physical Address. . . . . . . . . : D4-93-90-0F-F4-24
```

```
15     DHCP Enabled. . . . . . . . . . . : Yes
16     Autoconfiguration Enabled . . . . : Yes
17
18
19  Ethernet adapter Ethernet 2:
20
21     Connection-specific DNS Suffix  . :
22     Description . . . . . . . . . . . : VirtualBox Host-Only Ethernet
           Adapter
23     Physical Address. . . . . . . . . : 0A-00-27-00-00-13
24     DHCP Enabled. . . . . . . . . . . : No
25     Autoconfiguration Enabled . . . . : Yes
26     IPv4 Address. . . . . . . . . . . : 192.168.56.1(Preferred)
27     Subnet Mask . . . . . . . . . . . : 255.255.255.0
28     Default Gateway . . . . . . . . . :
29     NetBIOS over Tcpip. . . . . . . . : Enabled
```

Listing 2: Output of ipconfig /all

Discussion: This command displays details such as IP address, MAC address, subnet mask, gateway, and DHCP status. It is crucial for troubleshooting IP-related issues.

Linux

The equivalent command in Linux is:

```
1  ifconfig
```

Listing 3: Linux IP Configuration

Discussion: Similar to Windows, this reveals interface-level IP data. The interface names in Linux (e.g., eth0, enp0s3) may vary based on the system.

3.2   Ping Command

Windows

```
1  ping 8.8.8.8
2  ping -t 8.8.8.8
3  ping -l 64 8.8.8.8
4  ping -n 6 8.8.8.8
5  ping -a 8.8.8.8
```

Listing 4: Windows Ping Test

Result:

```
1  C:\Users\Student>ping 8.8.8.8
2
3  Pinging 8.8.8.8 with 32 bytes of data:
4  Reply from 8.8.8.8: bytes=32 time=27ms TTL=118
```

```
5 Reply from 8.8.8.8: bytes=32 time=28ms TTL=118
6 Reply from 8.8.8.8: bytes=32 time=28ms TTL=118
7 Reply from 8.8.8.8: bytes=32 time=27ms TTL=118
8
9 Ping statistics for 8.8.8.8:
10     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
11 Approximate round trip times in milli-seconds:
12     Minimum = 27ms, Maximum = 28ms, Average = 27ms
13
14 C:\Users\Student>ping -t 8.8.8.8
15
16 Pinging 8.8.8.8 with 32 bytes of data:
17 Reply from 8.8.8.8: bytes=32 time=27ms TTL=118
18 Reply from 8.8.8.8: bytes=32 time=27ms TTL=118
19 Reply from 8.8.8.8: bytes=32 time=28ms TTL=118
20 Reply from 8.8.8.8: bytes=32 time=28ms TTL=118
21 Reply from 8.8.8.8: bytes=32 time=28ms TTL=118
22 Reply from 8.8.8.8: bytes=32 time=27ms TTL=118
23 Reply from 8.8.8.8: bytes=32 time=28ms TTL=118
24 Reply from 8.8.8.8: bytes=32 time=28ms TTL=118
25 Reply from 8.8.8.8: bytes=32 time=28ms TTL=118
26 Reply from 8.8.8.8: bytes=32 time=28ms TTL=118
27 Reply from 8.8.8.8: bytes=32 time=28ms TTL=118
28 Reply from 8.8.8.8: bytes=32 time=28ms TTL=118
29 Reply from 8.8.8.8: bytes=32 time=28ms TTL=118
30 Reply from 8.8.8.8: bytes=32 time=28ms TTL=118
31 Reply from 8.8.8.8: bytes=32 time=28ms TTL=118
32 Reply from 8.8.8.8: bytes=32 time=28ms TTL=118
33 Reply from 8.8.8.8: bytes=32 time=28ms TTL=118
34 Reply from 8.8.8.8: bytes=32 time=28ms TTL=118
35 Reply from 8.8.8.8: bytes=32 time=28ms TTL=118
36
37 Ping statistics for 8.8.8.8:
38     Packets: Sent = 19, Received = 19, Lost = 0 (0% loss),
39 Approximate round trip times in milli-seconds:
40     Minimum = 27ms, Maximum = 28ms, Average = 27ms
41 Control-C
42 ^C
43 C:\Users\Student>ping -l 64 8.8.8.8
44
45 Pinging 8.8.8.8 with 64 bytes of data:
46 Reply from 8.8.8.8: bytes=64 time=27ms TTL=118
47 Reply from 8.8.8.8: bytes=64 time=28ms TTL=118
48 Reply from 8.8.8.8: bytes=64 time=28ms TTL=118
49 Reply from 8.8.8.8: bytes=64 time=28ms TTL=118
50
51 Ping statistics for 8.8.8.8:
52     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
53 Approximate round trip times in milli-seconds:
54     Minimum = 27ms, Maximum = 28ms, Average = 27ms
```

```
55
56  C:\Users\Student>ping -n 6 8.8.8.8
57
58  Pinging 8.8.8.8 with 32 bytes of data:
59  Reply from 8.8.8.8: bytes=32 time=28ms TTL=118
60  Reply from 8.8.8.8: bytes=32 time=28ms TTL=118
61  Reply from 8.8.8.8: bytes=32 time=28ms TTL=118
62  Reply from 8.8.8.8: bytes=32 time=28ms TTL=118
63  Reply from 8.8.8.8: bytes=32 time=28ms TTL=118
64  Reply from 8.8.8.8: bytes=32 time=28ms TTL=118
65
66  Ping statistics for 8.8.8.8:
67      Packets: Sent = 6, Received = 6, Lost = 0 (0% loss),
68  Approximate round trip times in milli-seconds:
69      Minimum = 28ms, Maximum = 28ms, Average = 28ms
70
71  C:\Users\Student>ping -a 8.8.8.8
72
73  Pinging dns.google [8.8.8.8] with 32 bytes of data:
74  Reply from 8.8.8.8: bytes=32 time=28ms TTL=118
75  Reply from 8.8.8.8: bytes=32 time=28ms TTL=118
76  Reply from 8.8.8.8: bytes=32 time=28ms TTL=118
77  Reply from 8.8.8.8: bytes=32 time=28ms TTL=118
78
79  Ping statistics for 8.8.8.8:
80      Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
81  Approximate round trip times in milli-seconds:
82      Minimum = 28ms, Maximum = 28ms, Average = 28ms
```

Listing 5: Results of the pings.

Discussion: The options used:

- -t: sends ping continuously until interrupted.

- -l: sets packet size.

- -n: sets number of echo requests.

- -a: resolves hostname from IP.

Linux

Linux alternatives are:

```
1  ping 8.8.8.8
2  ping -s 32 8.8.8.8
3  ping -c 8 8.8.8.8
4  ping -H 8 8.8.8.8
```

Listing 6: Linux Ping Test

Result:

```
   1     ( k a l i kali )-[~]
   2   $   ping 8.8.8.8
   3 PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
   4 64 bytes from 8.8.8.8: icmp_seq=1 ttl=118 time=38.8 ms
   5 64 bytes from 8.8.8.8: icmp_seq=2 ttl=118 time=36.9 ms
   6 64 bytes from 8.8.8.8: icmp_seq=3 ttl=118 time=37.5 ms
   7 64 bytes from 8.8.8.8: icmp_seq=4 ttl=118 time=28.7 ms
   8 64 bytes from 8.8.8.8: icmp_seq=5 ttl=118 time=28.6 ms
   9 64 bytes from 8.8.8.8: icmp_seq=6 ttl=118 time=28.9 ms
  10 64 bytes from 8.8.8.8: icmp_seq=7 ttl=118 time=28.5 ms
  11 64 bytes from 8.8.8.8: icmp_seq=8 ttl=118 time=28.8 ms
  12 64 bytes from 8.8.8.8: icmp_seq=9 ttl=118 time=28.6 ms
  13 64 bytes from 8.8.8.8: icmp_seq=10 ttl=118 time=28.6 ms
  14 64 bytes from 8.8.8.8: icmp_seq=11 ttl=118 time=28.2 ms
  15 64 bytes from 8.8.8.8: icmp_seq=12 ttl=118 time=28.1 ms
  16 64 bytes from 8.8.8.8: icmp_seq=13 ttl=118 time=28.4 ms
  17 64 bytes from 8.8.8.8: icmp_seq=14 ttl=118 time=28.5 ms
  18 64 bytes from 8.8.8.8: icmp_seq=15 ttl=118 time=28.3 ms
  19 64 bytes from 8.8.8.8: icmp_seq=16 ttl=118 time=28.1 ms
  20 64 bytes from 8.8.8.8: icmp_seq=17 ttl=118 time=28.3 ms
  21 64 bytes from 8.8.8.8: icmp_seq=18 ttl=118 time=28.1 ms
  22 64 bytes from 8.8.8.8: icmp_seq=19 ttl=118 time=28.8 ms
  23 64 bytes from 8.8.8.8: icmp_seq=20 ttl=118 time=28.0 ms
  24 64 bytes from 8.8.8.8: icmp_seq=21 ttl=118 time=28.8 ms
  25 64 bytes from 8.8.8.8: icmp_seq=22 ttl=118 time=29.0 ms
  26 ^C
  27 --- 8.8.8.8 ping statistics ---
  28 22 packets transmitted, 22 received, 0% packet loss, time 21038ms
  29 rtt min/avg/max/mdev = 28.042/29.747/38.754/3.190 ms
  30
  31     ( k a l i kali )-[~]
  32   $   ping -s 32 8.8.8.8
  33 PING 8.8.8.8 (8.8.8.8) 32(60) bytes of data.
  34 40 bytes from 8.8.8.8: icmp_seq=1 ttl=118 time=28.1 ms
  35 40 bytes from 8.8.8.8: icmp_seq=2 ttl=118 time=28.3 ms
  36 40 bytes from 8.8.8.8: icmp_seq=3 ttl=118 time=28.2 ms
  37 40 bytes from 8.8.8.8: icmp_seq=4 ttl=118 time=28.5 ms
  38 40 bytes from 8.8.8.8: icmp_seq=5 ttl=118 time=28.6 ms
  39 40 bytes from 8.8.8.8: icmp_seq=6 ttl=118 time=28.4 ms
  40 40 bytes from 8.8.8.8: icmp_seq=7 ttl=118 time=28.9 ms
  41 40 bytes from 8.8.8.8: icmp_seq=8 ttl=118 time=28.7 ms
  42 40 bytes from 8.8.8.8: icmp_seq=9 ttl=118 time=28.3 ms
  43 40 bytes from 8.8.8.8: icmp_seq=10 ttl=118 time=28.5 ms
  44 40 bytes from 8.8.8.8: icmp_seq=11 ttl=118 time=28.5 ms
  45 40 bytes from 8.8.8.8: icmp_seq=12 ttl=118 time=28.1 ms
  46 40 bytes from 8.8.8.8: icmp_seq=13 ttl=118 time=28.6 ms
  47 40 bytes from 8.8.8.8: icmp_seq=14 ttl=118 time=28.1 ms
  48 ^C
  49 --- 8.8.8.8 ping statistics ---
  50 14 packets transmitted, 14 received, 0% packet loss, time 13020ms
```

```
 51 rtt min/avg/max/mdev = 28.069/28.409/28.938/0.241 ms
 52
 53          ( k a l i kali )-[~]
 54   $     ping -c 8 8.8.8.8
 55 PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
 56 64 bytes from 8.8.8.8: icmp_seq=1 ttl=118 time=28.0 ms
 57 64 bytes from 8.8.8.8: icmp_seq=2 ttl=118 time=28.4 ms
 58 64 bytes from 8.8.8.8: icmp_seq=3 ttl=118 time=28.4 ms
 59 64 bytes from 8.8.8.8: icmp_seq=4 ttl=118 time=29.1 ms
 60 64 bytes from 8.8.8.8: icmp_seq=5 ttl=118 time=28.8 ms
 61 64 bytes from 8.8.8.8: icmp_seq=6 ttl=118 time=28.6 ms
 62 64 bytes from 8.8.8.8: icmp_seq=7 ttl=118 time=29.0 ms
 63 64 bytes from 8.8.8.8: icmp_seq=8 ttl=118 time=28.8 ms
 64
 65 --- 8.8.8.8 ping statistics ---
 66 8 packets transmitted, 8 received, 0% packet loss, time 7013ms
 67 rtt min/avg/max/mdev = 28.040/28.629/29.066/0.320 ms
 68
 69          ( k a l i kali )-[~]
 70   $     ping -H 8.8.8.8
 71 PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
 72 64 bytes from dns.google (8.8.8.8): icmp_seq=1 ttl=118 time=28.2 ms
 73 64 bytes from dns.google (8.8.8.8): icmp_seq=2 ttl=118 time=28.5 ms
 74 64 bytes from dns.google (8.8.8.8): icmp_seq=3 ttl=118 time=28.2 ms
 75 64 bytes from dns.google (8.8.8.8): icmp_seq=4 ttl=118 time=28.7 ms
 76 64 bytes from dns.google (8.8.8.8): icmp_seq=5 ttl=118 time=28.5 ms
 77 64 bytes from dns.google (8.8.8.8): icmp_seq=6 ttl=118 time=28.1 ms
 78 64 bytes from dns.google (8.8.8.8): icmp_seq=7 ttl=118 time=28.2 ms
 79 64 bytes from dns.google (8.8.8.8): icmp_seq=8 ttl=118 time=28.6 ms
 80 64 bytes from dns.google (8.8.8.8): icmp_seq=9 ttl=118 time=28.1 ms
 81 64 bytes from dns.google (8.8.8.8): icmp_seq=10 ttl=118 time=28.1 ms
 82 64 bytes from dns.google (8.8.8.8): icmp_seq=11 ttl=118 time=28.5 ms
 83 64 bytes from dns.google (8.8.8.8): icmp_seq=12 ttl=118 time=28.5 ms
 84 64 bytes from dns.google (8.8.8.8): icmp_seq=13 ttl=118 time=28.3 ms
 85 64 bytes from dns.google (8.8.8.8): icmp_seq=14 ttl=118 time=28.6 ms
 86 64 bytes from dns.google (8.8.8.8): icmp_seq=15 ttl=118 time=28.1 ms
 87 64 bytes from dns.google (8.8.8.8): icmp_seq=16 ttl=118 time=28.2 ms
 88 64 bytes from dns.google (8.8.8.8): icmp_seq=17 ttl=118 time=28.2 ms
 89 ^C
 90 --- 8.8.8.8 ping statistics ---
 91 17 packets transmitted, 17 received, 0% packet loss, time 16037ms
 92 rtt min/avg/max/mdev = 28.065/28.329/28.651/0.192 ms
```

Listing 7: Linux ping test results.

3.3   Traceroute Command

Windows

```
 1 tracert 8.8.8.8
```

```
2 tracert -d 8.8.8.8
3 tracert -h 5 8.8.8.8
```

Listing 8: Windows Traceroute

Result:

```
1 C:\Users\Student>tracert 8.8.8.8
2
3 Tracing route to dns.google [8.8.8.8]
4 over a maximum of 30 hops:
5
6    1    <1 ms    <1 ms    <1 ms   10.1.0.1
7    2     *         *         *      Request timed out.
8    3     1 ms      1 ms      1 ms   212.33.95.1
9    4     1 ms      1 ms      1 ms   212.33.70.144
10   5     1 ms      1 ms      1 ms   212.33.70.221
11   6     8 ms      7 ms      8 ms   z-Bialystok.poznan-gw2.rtr.pionier.gov.
     pl [212.191.237.165]
12   7    28 ms     27 ms     27 ms   core2.ams.net.google.com
     [80.249.209.100]
13   8    28 ms     29 ms     28 ms   74.125.242.187
14   9    27 ms     28 ms     27 ms   142.251.48.175
15  10    28 ms     28 ms     27 ms   dns.google [8.8.8.8]
16
17 Trace complete.
18
19 C:\Users\Student>tracert -d 8.8.8.8
20
21 Tracing route to 8.8.8.8 over a maximum of 30 hops
22
23   1    <1 ms    <1 ms    <1 ms   10.1.0.1
24   2     *         *         *      Request timed out.
25   3     1 ms      1 ms     <1 ms   212.33.95.1
26   4     1 ms      1 ms     <1 ms   212.33.70.144
27   5     1 ms      1 ms     <1 ms   212.33.70.221
28   6     7 ms      7 ms      7 ms   212.191.237.165
29   7    28 ms     27 ms     27 ms   80.249.209.100
30   8    28 ms     28 ms     28 ms   74.125.242.187
31   9    28 ms     28 ms     28 ms   142.251.48.175
32  10    28 ms     28 ms     27 ms   8.8.8.8
33
34 Trace complete.
35
36 C:\Users\Student>tracert -h 5 8.8.8.8
37
38 Tracing route to dns.google [8.8.8.8]
39 over a maximum of 5 hops:
40
41   1    <1 ms    <1 ms    <1 ms   10.1.0.1
42   2     *         *         *      Request timed out.
```

```
43   3       1 ms       1 ms       1 ms   212.33.95.1
44   4       1 ms       1 ms     <1 ms   212.33.70.144
45   5       1 ms       1 ms     <1 ms   212.33.70.221
46
47 Trace complete.
```

Listing 9: Traceroute results.

Discussion:

- **-d**: disabling the resolution of host names on the designated path.

- **-h**: sets maximum number of hops.

Linux

```
1 traceroute 8.8.8.8
```

Listing 10: Linux Traceroute

Result:

```
1          ( k a l i kali )-[~]
2    $      traceroute 8.8.8.8
3 traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
4  1  * * 10.1.0.1 (10.1.0.1)  1.582 ms
5  2  * * *
6  3  212.33.95.1 (212.33.95.1)  1.420 ms  1.377 ms  1.333 ms
7  4  212.33.70.144 (212.33.70.144)  1.755 ms  1.711 ms  1.676 ms
8  5  212.33.70.221 (212.33.70.221)  1.174 ms  1.137 ms  1.092 ms
9  6  z-Bialystok.poznan-gw2.rtr.pionier.gov.pl (212.191.237.165)  7.826
      ms  7.623 ms  7.831 ms
10 7  core2.ams.net.google.com (80.249.209.100)  27.542 ms  27.504 ms
      27.468 ms
11 8  74.125.242.187 (74.125.242.187)  28.000 ms 74.125.243.133
      (74.125.243.133)  28.485 ms 74.125.242.165 (74.125.242.165)  28.596
      ms
12 9  108.170.227.9 (108.170.227.9)  28.548 ms 172.253.71.201
      (172.253.71.201)  27.800 ms 142.251.48.181 (142.251.48.181)  27.759
      ms
13 10  dns.google (8.8.8.8)  27.435 ms  27.388 ms  27.964 ms
```

Listing 11: Traceroute results.

3.4 Netstat Command

```
1 netstat -a
2 netstat -n
3 netstat -e
```

Listing 12: Windows Netstat Test

9

Result:

```
1  traceroute 8.8.8.8
```

Listing 13: Linux Traceroute

Result:

```
1   C:\Users\Student>netstat -a
2
3   Active Connections
4
5     Proto   Local Address          Foreign Address        State
6     TCP     0.0.0.0:135            DESKTOP-TJCLUI7:0       LISTENING
7     TCP     0.0.0.0:445            DESKTOP-TJCLUI7:0       LISTENING
8     TCP     0.0.0.0:902            DESKTOP-TJCLUI7:0       LISTENING
9     TCP     0.0.0.0:912            DESKTOP-TJCLUI7:0       LISTENING
10    TCP     0.0.0.0:5040           DESKTOP-TJCLUI7:0       LISTENING
11    TCP     0.0.0.0:49664          DESKTOP-TJCLUI7:0       LISTENING
12    TCP     0.0.0.0:49665          DESKTOP-TJCLUI7:0       LISTENING
13    TCP     0.0.0.0:49666          DESKTOP-TJCLUI7:0       LISTENING
14    TCP     0.0.0.0:49667          DESKTOP-TJCLUI7:0       LISTENING
15    TCP     0.0.0.0:49668          DESKTOP-TJCLUI7:0       LISTENING
16    TCP     0.0.0.0:49670          DESKTOP-TJCLUI7:0       LISTENING
17    TCP     10.1.0.118:139         DESKTOP-TJCLUI7:0       LISTENING
18    TCP     10.1.0.118:49734       172.211.123.250:https  ESTABLISHED
19    TCP     10.1.0.118:50185       a23-211-41-92:https     ESTABLISHED
20    TCP     10.1.0.118:50190       40.126.31.67:https      TIME_WAIT
21    TCP     127.0.0.1:50110        DESKTOP-TJCLUI7:50111   ESTABLISHED
22    TCP     127.0.0.1:50111        DESKTOP-TJCLUI7:50110   ESTABLISHED
23    TCP     192.168.56.1:139       DESKTOP-TJCLUI7:0       LISTENING
24    TCP     192.168.119.1:139      DESKTOP-TJCLUI7:0       LISTENING
25    TCP     [::]:135               DESKTOP-TJCLUI7:0       LISTENING
26    TCP     [::]:445               DESKTOP-TJCLUI7:0       LISTENING
27    TCP     [::]:49664             DESKTOP-TJCLUI7:0       LISTENING
28    TCP     [::]:49665             DESKTOP-TJCLUI7:0       LISTENING
29    TCP     [::]:49666             DESKTOP-TJCLUI7:0       LISTENING
30    TCP     [::]:49667             DESKTOP-TJCLUI7:0       LISTENING
31    TCP     [::]:49668             DESKTOP-TJCLUI7:0       LISTENING
32    TCP     [::]:49670             DESKTOP-TJCLUI7:0       LISTENING
33    TCP     [::1]:49669            DESKTOP-TJCLUI7:0       LISTENING
34    TCP     [::1]:50112            DESKTOP-TJCLUI7:50113   ESTABLISHED
35    TCP     [::1]:50113            DESKTOP-TJCLUI7:50112   ESTABLISHED
36    UDP     0.0.0.0:5050           *:*
37    UDP     0.0.0.0:5353           *:*
38    UDP     0.0.0.0:5353           *:*
39    UDP     0.0.0.0:5353           *:*
40    UDP     0.0.0.0:5353           *:*
41    UDP     0.0.0.0:5353           *:*
42    UDP     0.0.0.0:5353           *:*
```

```
43   UDP     0.0.0.0:5353              *:*
44   UDP     0.0.0.0:5355              *:*
45   UDP     0.0.0.0:52533             *:*
46   UDP     0.0.0.0:53321             *:*
47   UDP     0.0.0.0:59300             *:*
48   UDP     10.1.0.118:137            *:*
49   UDP     10.1.0.118:138            *:*
50   UDP     10.1.0.118:1900           *:*
51   UDP     10.1.0.118:52419          *:*
52   UDP     127.0.0.1:1900            *:*
53   UDP     127.0.0.1:52422           *:*
54   UDP     127.0.0.1:57581           127.0.0.1:57581
55   UDP     192.168.56.1:137          *:*
56   UDP     192.168.56.1:138          *:*
57   UDP     192.168.56.1:1900         *:*
58   UDP     192.168.56.1:52421        *:*
59   UDP     192.168.119.1:137         *:*
60   UDP     192.168.119.1:138         *:*
61   UDP     192.168.119.1:1900        *:*
62   UDP     192.168.119.1:52420       *:*
63   UDP     [::]:5353                 *:*
64   UDP     [::]:5353                 *:*
65   UDP     [::]:5353                 *:*
66   UDP     [::]:5353                 *:*
67   UDP     [::]:5355                 *:*
68   UDP     [::]:52533                *:*
69   UDP     [::]:53321                *:*
70   UDP     [::]:59300                *:*
71   UDP     [::1]:1900                *:*
72   UDP     [::1]:52418               *:*
73   UDP     [fe80::3cf9:bfaa:b526:99e4%11]:1900   *:*
74   UDP     [fe80::3cf9:bfaa:b526:99e4%11]:52416   *:*
75   UDP     [fe80::4c66:bc7:e7d6:ba3e%17]:1900   *:*
76   UDP     [fe80::4c66:bc7:e7d6:ba3e%17]:52417   *:*
77   UDP     [fe80::dc48:f336:8611:fca2%16]:1900   *:*
78   UDP     [fe80::dc48:f336:8611:fca2%16]:52415   *:*
79
80   C:\Users\Student>netstat -n
81
82   Active Connections
83
84     Proto   Local Address          Foreign Address          State
85     TCP     10.1.0.118:49734       172.211.123.250:443      ESTABLISHED
86     TCP     10.1.0.118:50185       23.211.41.92:443         ESTABLISHED
87     TCP     10.1.0.118:50190       40.126.31.67:443         TIME_WAIT
88     TCP     127.0.0.1:50110        127.0.0.1:50111          ESTABLISHED
89     TCP     127.0.0.1:50111        127.0.0.1:50110          ESTABLISHED
90     TCP     [::1]:50112            [::1]:50113              ESTABLISHED
91     TCP     [::1]:50113            [::1]:50112              ESTABLISHED
92
```

11

```
93 C:\Users\Student>netstat -e
94 Interface Statistics
95
96                           Received          Sent
97
98 Bytes                   324036146      22728784
99 Unicast packets            256196        140069
100 Non-unicast packets         15825          5450
101 Discards                        0             0
102 Errors                          0             0
103 Unknown protocols               0
```

Listing 14: Netstat results.

Discussion:

- `-a`: shows all connections and listening ports.

- `-n`: skips DNS resolution.

- `-e`: Ethernet stats like sent/received packets.

3.5 ARP Table

```
1 arp -a
```

Listing 15: View ARP Table and Analyze Changes

Instructions:

1. Run `arp -a`.

2. Ping another local network machine.

3. Run `arp -a` again to observe new entry.

4. Monitor to find when the entry disappears.

Result:

```
1 C:\Users\Student>ping 10.1.0.121
2
3 Pinging 10.1.0.121 with 32 bytes of data:
4 Reply from 10.1.0.121: bytes=32 time=1ms TTL=128
5 Reply from 10.1.0.121: bytes=32 time=1ms TTL=128
6 Reply from 10.1.0.121: bytes=32 time=1ms TTL=128
7 Reply from 10.1.0.121: bytes=32 time=1ms TTL=128
8
9 Ping statistics for 10.1.0.121:
10     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
11 Approximate round trip times in milli-seconds:
12     Minimum = 1ms, Maximum = 1ms, Average = 1ms
```
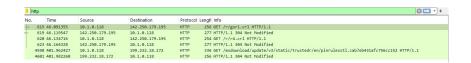
```
13
C:\Users\Student>arp -a

Interface: 10.1.0.120 --- 0x9
  Internet Address      Physical Address      Type
  10.1.0.1              00-1e-67-98-8f-83      dynamic
  10.1.0.121            44-45-6f-12-62-cd      dynamic
  10.1.0.255            ff-ff-ff-ff-ff-ff      static
  224.0.0.22            01-00-5e-00-00-16      static
  224.0.0.251           01-00-5e-00-00-fb      static
  224.0.0.252           01-00-5e-00-00-fc      static
  239.255.255.250       01-00-5e-7f-ff-fa      static
  255.255.255.255       ff-ff-ff-ff-ff-ff      static

Interface: 192.168.111.1 --- 0x10
  Internet Address      Physical Address      Type
  192.168.111.254       00-50-56-f3-cf-10      dynamic
  192.168.111.255       ff-ff-ff-ff-ff-ff      static
  224.0.0.22            01-00-5e-00-00-16      static
  224.0.0.251           01-00-5e-00-00-fb      static
  224.0.0.252           01-00-5e-00-00-fc      static
  239.255.255.250       01-00-5e-7f-ff-fa      static
  255.255.255.255       ff-ff-ff-ff-ff-ff      static

Interface: 192.168.112.1 --- 0x13
  Internet Address      Physical Address      Type
  192.168.112.254       00-50-56-f5-da-d7      dynamic
  192.168.112.255       ff-ff-ff-ff-ff-ff      static
  224.0.0.22            01-00-5e-00-00-16      static
  224.0.0.251           01-00-5e-00-00-fb      static
  224.0.0.252           01-00-5e-00-00-fc      static
  239.255.255.250       01-00-5e-7f-ff-fa      static
  255.255.255.255       ff-ff-ff-ff-ff-ff      static


C:\Users\Student>ping 10.1.0.118

Pinging 10.1.0.118 with 32 bytes of data:
Reply from 10.1.0.118: bytes=32 time=2ms TTL=128
Reply from 10.1.0.118: bytes=32 time=1ms TTL=128
Reply from 10.1.0.118: bytes=32 time=1ms TTL=128
Reply from 10.1.0.118: bytes=32 time=1ms TTL=128

Ping statistics for 10.1.0.118:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Users\Student>arp -a
```
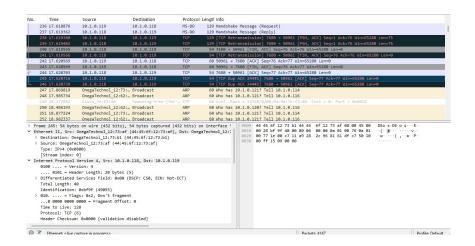
```
63  Interface: 10.1.0.120 --- 0x9
64    Internet Address      Physical Address      Type
65    10.1.0.1              00-1e-67-98-8f-83     dynamic
66    10.1.0.118            44-45-6f-12-73-af     dynamic
67    10.1.0.121            44-45-6f-12-62-cd     dynamic
68    10.1.0.255            ff-ff-ff-ff-ff-ff     static
69    224.0.0.22            01-00-5e-00-00-16     static
70    224.0.0.251           01-00-5e-00-00-fb     static
71    224.0.0.252           01-00-5e-00-00-fc     static
72    239.255.255.250       01-00-5e-7f-ff-fa     static
73    255.255.255.255       ff-ff-ff-ff-ff-ff     static
74
75  Interface: 192.168.111.1 --- 0x10
76    Internet Address      Physical Address      Type
77    192.168.111.254       00-50-56-f3-cf-10     dynamic
78    192.168.111.255       ff-ff-ff-ff-ff-ff     static
79    224.0.0.22            01-00-5e-00-00-16     static
80    224.0.0.251           01-00-5e-00-00-fb     static
81    224.0.0.252           01-00-5e-00-00-fc     static
82    239.255.255.250       01-00-5e-7f-ff-fa     static
83    255.255.255.255       ff-ff-ff-ff-ff-ff     static
84
85  Interface: 192.168.112.1 --- 0x13
86    Internet Address      Physical Address      Type
87    192.168.112.254       00-50-56-f5-da-d7     dynamic
88    192.168.112.255       ff-ff-ff-ff-ff-ff     static
89    224.0.0.22            01-00-5e-00-00-16     static
90    224.0.0.251           01-00-5e-00-00-fb     static
91    224.0.0.252           01-00-5e-00-00-fc     static
92    239.255.255.250       01-00-5e-7f-ff-fa     static
93    255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Listing 16: ARP table and ping results.

Discussion: ARP dynamically caches mappings of IP to MAC addresses. Entries expire after a short time to keep the table up to date.

3.6   Wireshark Usage

14

Discussion: Wireshark is a powerful tool for network diagnostics. By using filters and capture options, it's possible to isolate traffic by IP, MAC, or protocol. Promiscuous mode ensures all traffic is captured.

4   Conclusion

This lab session helped us gain hands-on experience with fundamental network diagnostic and monitoring tools on both Windows and Linux. Understanding these tools is essential for identifying and resolving network issues, observing packet behavior, and verifying connectivity and configurations. The skills practiced here serve as a foundation for more advanced networking topics.

5   References

1. Sloan, J.D. (2001). Network Troubleshooting Tools. O'Reilly Media, Inc.

2. Wireshark Documentation: `https://www.wireshark.org/docs/`

3. Lab Manual by Andrzej Zankiewicz, PhD