Study of Network Diagnostics Tools Part-1
Experiment No: AV-341-2025-Lab-1

Saurabh Kumar
SC22B146

January 27, 2025

Date and Time of experiment: January 20, 2025, 14:45 IST

Objectives

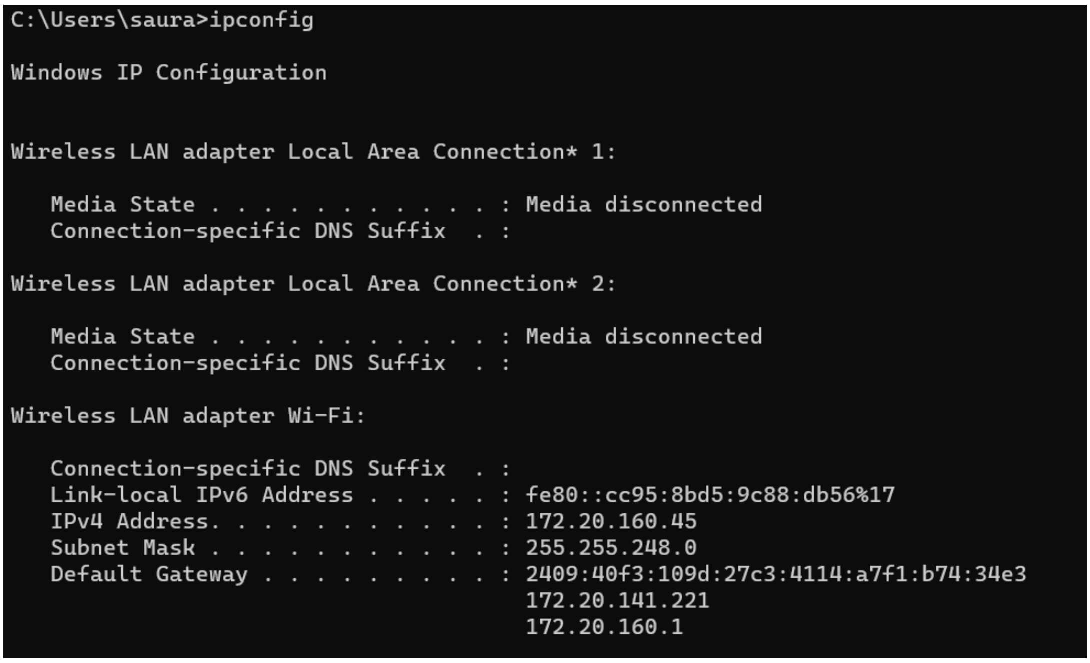
- To study the network diagnostic tools: `ping`, `ipconfig/ifconfig`, and `tracert`.
- Use the network diagnostic tools in your network and understand the various options.

Tools Used

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

Procedure

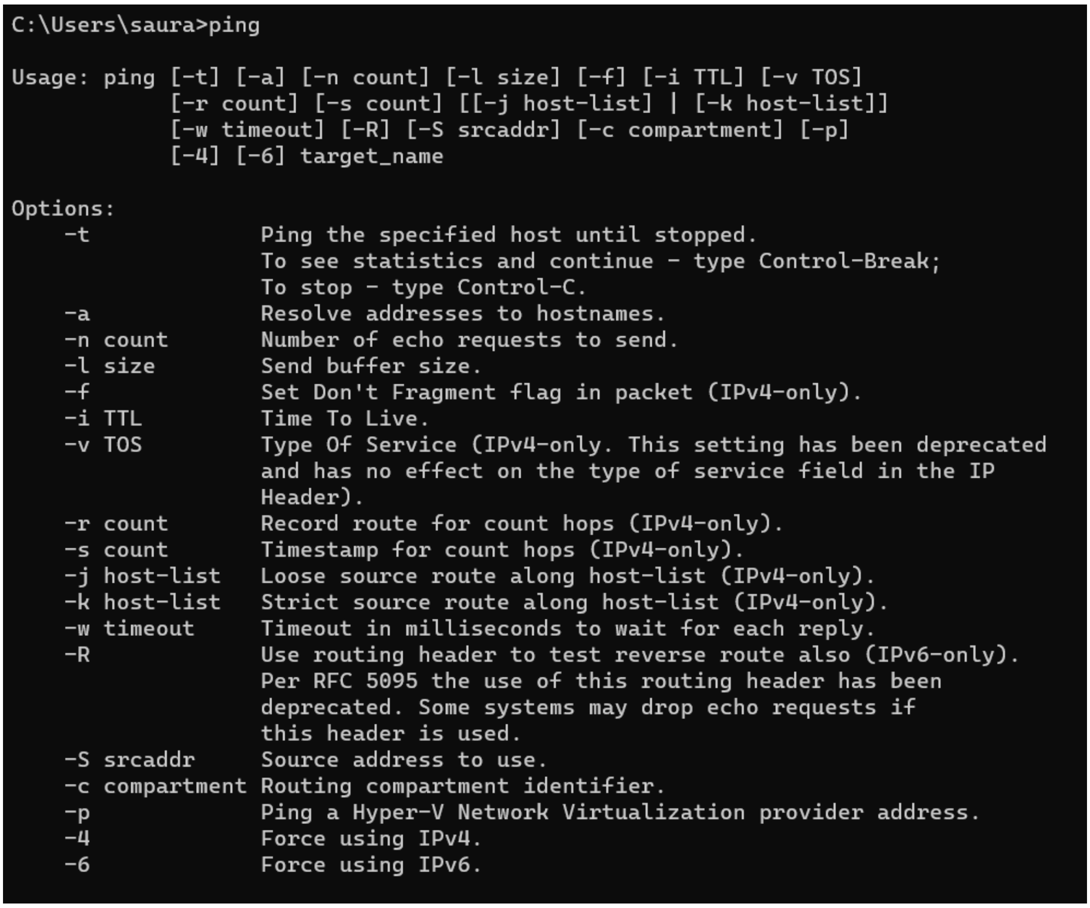
1. Open the Command Prompt on Windows PC.
2. Use the `ipconfig` (`ifconfig` for Linux) command to check the network configuration of the system.



```
C:\Users\saura>ipconfig

Windows IP Configuration


Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::cc95:8bd5:9c88:db56%17
   IPv4 Address. . . . . . . . . . . : 172.20.160.45
   Subnet Mask . . . . . . . . . . . : 255.255.248.0
   Default Gateway . . . . . . . . . : 2409:40f3:109d:27c3:4114:a7f1:b74:34e3
                                       172.20.141.221
                                       172.20.160.1
```

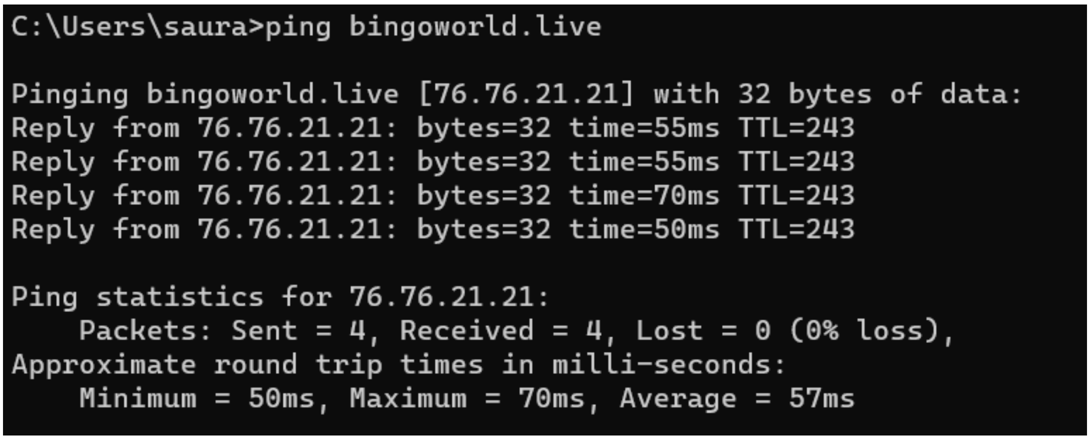
Figure 1: `ipconfig` command on Command Prompt

3. Use the `ping` command to test connectivity with a specific IP address or domain.



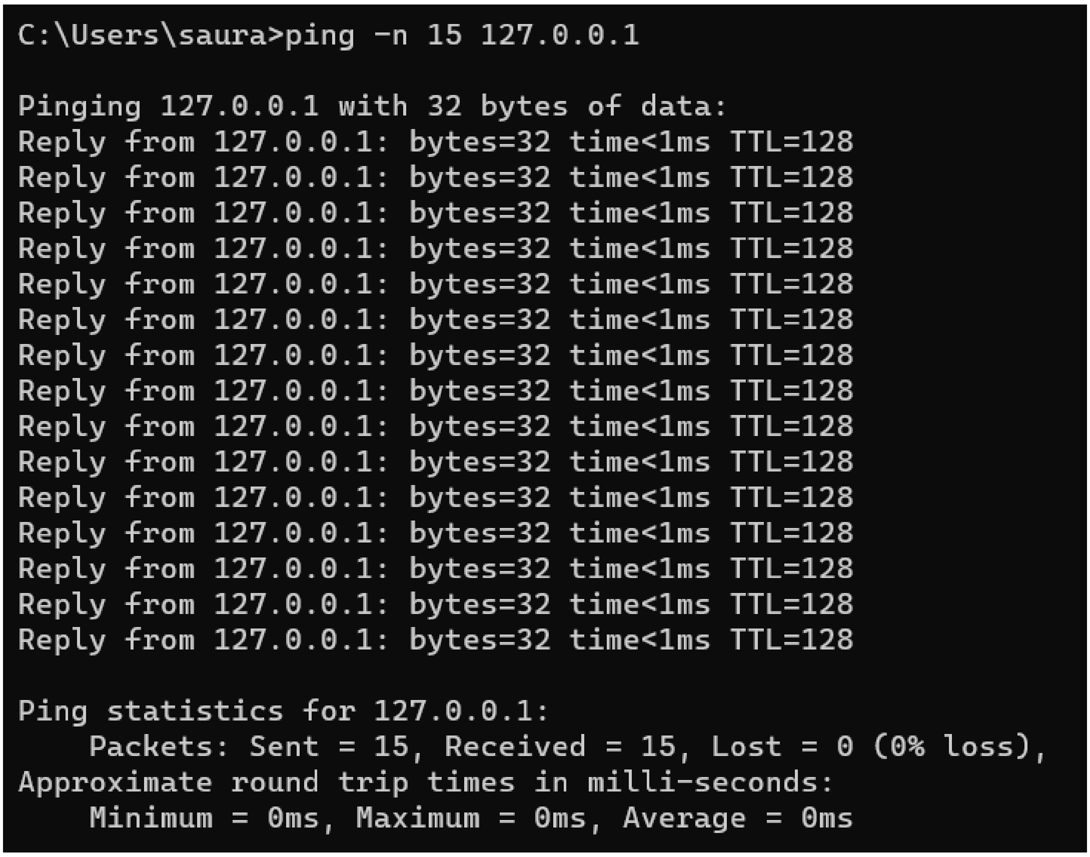
```
C:\Users\saura>ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
            [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
                   and has no effect on the type of service field in the IP
                   Header).
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
                   Per RFC 5095 the use of this routing header has been
                   deprecated. Some systems may drop echo requests if
                   this header is used.
    -S srcaddr     Source address to use.
    -c compartment Routing compartment identifier.
    -p             Ping a Hyper-V Network Virtualization provider address.
    -4             Force using IPv4.
    -6             Force using IPv6.
```

Figure 2: `ping` command options



```
C:\Users\saura>ping bingoworld.live

Pinging bingoworld.live [76.76.21.21] with 32 bytes of data:
Reply from 76.76.21.21: bytes=32 time=55ms TTL=243
Reply from 76.76.21.21: bytes=32 time=55ms TTL=243
Reply from 76.76.21.21: bytes=32 time=70ms TTL=243
Reply from 76.76.21.21: bytes=32 time=50ms TTL=243

Ping statistics for 76.76.21.21:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 50ms, Maximum = 70ms, Average = 57ms
```

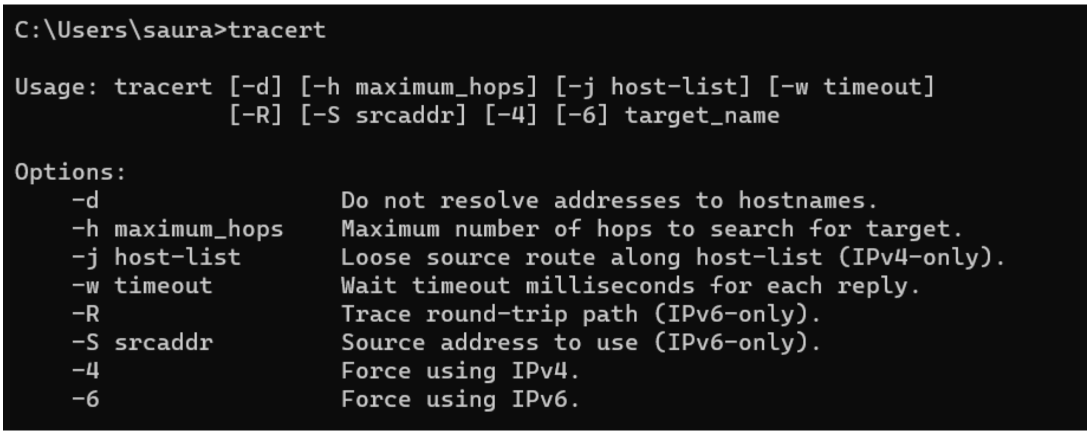
Figure 3: Pinging a domain



```
C:\Users\saura>ping -n 15 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 15, Received = 15, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

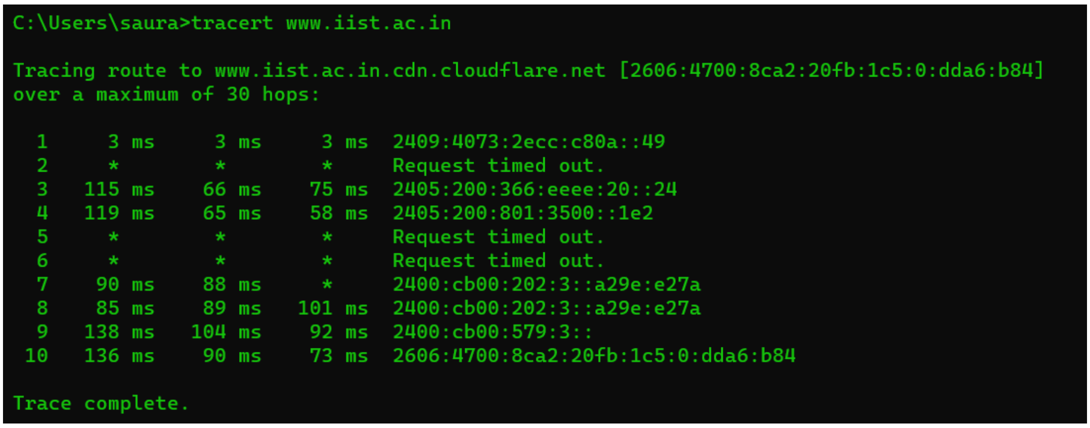
Figure 4: Self pinging with a specific no. of echo

4. Use the `tracert` command to trace the route packets took to reach the destination.



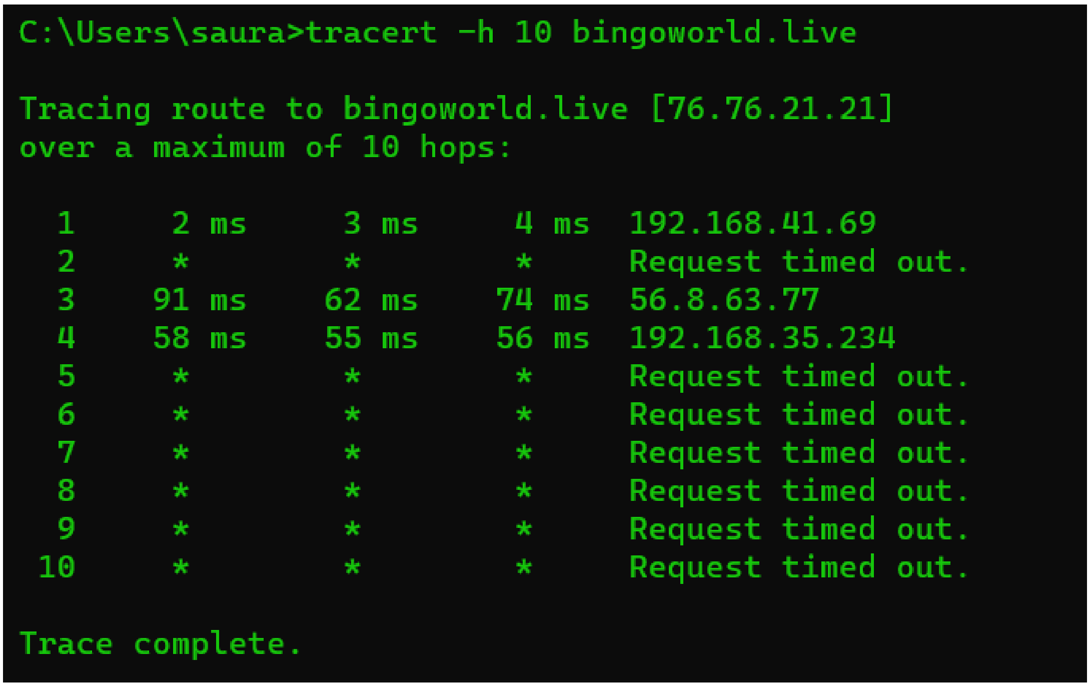
```
C:\Users\saura>tracert

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.
```

Figure 5: `tracert` command options



```
C:\Users\saura>tracert www.iist.ac.in

Tracing route to www.iist.ac.in.cdn.cloudflare.net [2606:4700:8ca2:20fb:1c5:0:dda6:b84]
over a maximum of 30 hops:

  1     3 ms     3 ms     3 ms  2409:4073:2ecc:c80a::49
  2     *        *        *     Request timed out.
  3   115 ms    66 ms    75 ms  2405:200:366:eeee:20::24
  4   119 ms    65 ms    58 ms  2405:200:801:3500::1e2
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7    90 ms    88 ms     *     2400:cb00:202:3::a29e:e27a
  8    85 ms    89 ms   101 ms  2400:cb00:202:3::a29e:e27a
  9   138 ms   104 ms    92 ms  2400:cb00:579:3::
 10   136 ms    90 ms    73 ms  2606:4700:8ca2:20fb:1c5:0:dda6:b84

Trace complete.
```

Figure 6: Tracing packets to a domain



```
C:\Users\saura>tracert -h 10 bingoworld.live

Tracing route to bingoworld.live [76.76.21.21]
over a maximum of 10 hops:

  1     2 ms     3 ms     4 ms  192.168.41.69
  2     *        *        *     Request timed out.
  3    91 ms    62 ms    74 ms  56.8.63.77
  4    58 ms    55 ms    56 ms  192.168.35.234
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.

Trace complete.
```

Figure 7: Tracing packets to a domain with a specific no. of hops

Observations

- The `ipconfig` command showed the IP address (unique identifier), subnet mask, and gateway of the device.
  - `IPv4` Address is the IP address of the device on a network.
  - `IPv6` Address is used for for modern networks with larger address spaces.
  - `Subnet Mask` identifies the network and the host.
  - `Default Gateway` is the address of the device which connects the our local network to the internet.
- The `ping` command displayed the latency and packet loss for the target IP address.
  - Use options like `-n count` along with `ping` to send specific no. of packets.

    - Other options can be checked by commanding `ping`.

- The `tracert` command displayed the hops and latency for each router the packets passed through.
    - Use options like `-h maximum_hops` to specify the maximum no. of hops to search for target.

Conclusions

- The network diagnostic tools like `ping`, `ipconfig`, and `tracert` can be used for troubleshooting network connectivity issues.
- Each tool provides unique and valuable information to understand the state and performance of the network.