

# LAB 2: Network commands for testing and trouble shooting

## Objectives

- To learn and understand various network commands used for testing and troubleshooting network connectivity.
- To study the working and output of basic network diagnostic commands in the Windows operating system.

## Theory

### Requirement – Windows Operating System

Network commands are essential utilities used for testing, monitoring, and troubleshooting computer networks. These commands assist network administrators and users in identifying connectivity problems, IP configuration issues, routing errors, and communication failures. In the Windows Operating System, network commands are executed through the **Command Prompt (CMD)**.

Some network commands are:

1. Ping
2. tracert
3. ipconfig
4. nslookup
5. netstat-a
6. pathping
7. route
8. arp-a
9. hostname
10. getmac
11. nbstat

## 1. Ping

Ping is used to test the connectivity between the local computer and a remote host. It sends ICMP echo requests and measures the response time to check whether the destination is reachable.

Syntax: ping<ip address domain>

```
C:\Windows\System32>ping www.google.com

Pinging www.google.com [2404:6800:4002:829::2004] with 32 bytes of data:
Reply from 2404:6800:4002:829::2004: time=23ms
Reply from 2404:6800:4002:829::2004: time=26ms
Reply from 2404:6800:4002:829::2004: time=26ms
Reply from 2404:6800:4002:829::2004: time=26ms

Ping statistics for 2404:6800:4002:829::2004:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 23ms, Maximum = 26ms, Average = 25ms
```

## 2. Tracert

Tracert traces the route taken by data packets from the source to the destination. It helps identify network delays or failures at specific hops along the path.

Syntax: tracert Domain\_name

```
C:\Windows\System32>tracert google.com

Tracing route to google.com [2404:6800:4002:817::200e]
over a maximum of 30 hops:

  0  1 ms    1 ms    1 ms    2405:acc0:1200::d4b7
  1  5 ms    4 ms    4 ms    2001:def:8000::169
  2  8 ms    7 ms    6 ms    2405:acc0::a6
  3  8 ms    9 ms    6 ms    2405:acc0::9a
  4  25 ms   25 ms   23 ms   2401:5760::210:87:106:0
  5  25 ms   23 ms   24 ms   2404:6800:81e2:300::1
  6  26 ms   24 ms   23 ms   2404:6800:81e2:300::1
  7  26 ms   25 ms   25 ms   2001:4860:0:1::53a4
  8  27 ms   25 ms   25 ms   2001:4860:0:1::168f
  9  25 ms   23 ms   23 ms   tzdelb-bf-in-x0e.1e100.net [2404:6800:4002:817::200e]

Trace complete.
```

### 3. ipconfig

Ipconfig displays the current IP configuration of the system, including IP address, subnet mask, and default gateway. It is useful for diagnosing network configuration issues.

Syntax :ipconfig

```
C:\Windows\System32>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

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

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 10:

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

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . :
    IPv6 Address. . . . . : 2405:acc0:1207:66f5::2
    IPv6 Address. . . . . : 2405:acc0:1207:66f5:28e9:326a:ab61:152e
    Temporary IPv6 Address. . . . . : 2405:acc0:1207:66f5:c5d1:a36d:c35d:b6ff
    Link-local IPv6 Address . . . . . : fe80::5084:d3b3:a0e0:11ae%4
    IPv4 Address. . . . . : 192.168.18.7
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::1%4
                                192.168.18.1
```

### 4. nslookup

Nslookup is used to query DNS servers to obtain information about domain names and their corresponding IP addresses. It helps in troubleshooting DNS-related problems.

Syntax: nslookup domain\_name

```
C:\Windows\System32>nslookup google.com
Server: dev.opt
Address: 192.168.18.1

Non-authoritative answer:
Name: google.com
Addresses: 2404:6800:4002:817::200e
           142.250.183.14
```

## 5. netstat -a

Netstat -a shows all active TCP connections and listening ports on the computer. It is useful for monitoring network activity and detecting unauthorized connections.

Syntax: netstat - a

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

Active Connections

Proto Local Address           Foreign Address         State
TCP   0.0.0.0:135              SS:0                   LISTENING
TCP   0.0.0.0:445              SS:0                   LISTENING
TCP   0.0.0.0:5040             SS:0                   LISTENING
TCP   0.0.0.0:7070             SS:0                   LISTENING
TCP   0.0.0.0:49664            SS:0                   LISTENING
TCP   0.0.0.0:49665            SS:0                   LISTENING
TCP   0.0.0.0:49666            SS:0                   LISTENING
TCP   0.0.0.0:49667            SS:0                   LISTENING
TCP   0.0.0.0:49668            SS:0                   LISTENING
TCP   0.0.0.0:49672            SS:0                   LISTENING
TCP   0.0.0.0:52698            SS:0                   LISTENING
TCP   0.0.0.0:57621            SS:0                   LISTENING
TCP   127.0.0.1:5354           SS:0                   LISTENING
TCP   127.0.0.1:5354           SS:49670              ESTABLISHED
TCP   127.0.0.1:5354           SS:49671              ESTABLISHED
TCP   127.0.0.1:7768           SS:0                   LISTENING
TCP   127.0.0.1:8884           SS:0                   LISTENING
TCP   127.0.0.1:27015          SS:0                   LISTENING
TCP   127.0.0.1:27017          SS:0                   LISTENING
TCP   127.0.0.1:45112          SS:0                   LISTENING
TCP   127.0.0.1:49670          SS:5354               ESTABLISHED
TCP   127.0.0.1:49671          SS:5354               ESTABLISHED
TCP   127.0.0.1:58613          SS:58614              ESTABLISHED
TCP   127.0.0.1:58614          SS:58613              ESTABLISHED
TCP   127.0.0.1:58615          SS:58616              ESTABLISHED
TCP   127.0.0.1:58616          SS:58615              ESTABLISHED
TCP   127.0.0.1:62847          SS:62848              ESTABLISHED
TCP   127.0.0.1:62848          SS:62847              ESTABLISHED
TCP   127.0.0.1:62849          SS:62850              ESTABLISHED
TCP   127.0.0.1:62850          SS:62849              ESTABLISHED
TCP   192.168.18.7:139         SS:0                   LISTENING
```

## 6. Pathping

Pathping combines the features of ping and tracert to analyze network performance. It provides detailed statistics about packet loss at each router along the path.

Syntax: pathping destination

```
C:\Windows\System32>pathping

Usage: pathping [-g host-list] [-h maximum_hops] [-i address] [-n]
               [-p period] [-q num_queries] [-w timeout]
               [-4] [-6] target_name

Options:
  -g host-list      Loose source route along host-list.
  -h maximum_hops   Maximum number of hops to search for target.
  -i address        Use the specified source address.
  -n               Do not resolve addresses to hostnames.
  -p period         Wait period milliseconds between pings.
  -q num_queries    Number of queries per hop.
  -w timeout        Wait timeout milliseconds for each reply.
  -4               Force using IPv4.
  -6               Force using IPv6.
```

## 7. route

The route command displays and modifies the IP routing table. It helps control how network packets are forwarded to different destinations.

Syntax: route print

```
C:\Windows\System32>route print
=====
Interface List
 5...60 18 95 21 37 31 .....Realtek PCIe GbE Family Controller
12...e0 2b e9 de bd aa .....Microsoft Wi-Fi Direct Virtual Adapter
 9...e2 2b e9 de bd a9 .....Microsoft Wi-Fi Direct Virtual Adapter #2
 4...e0 2b e9 de bd a9 .....Intel(R) Wireless-AC 9462
 1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway           Interface         Metric
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
224.0.0.0                  240.0.0.0        On-link           127.0.0.1          331
255.255.255.255            255.255.255.255  On-link           127.0.0.1          331
=====
Persistent Routes:
None

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
1    331  ::1/128         On-link
1    331  ff00::/8        On-link
=====
Persistent Routes:
None
```

## 8. arp -a

Arp -a displays the ARP table, which maps IP addresses to MAC addresses. It is useful for identifying devices connected to the local network.

Syntax : arp -a

```
C:\Windows\System32>arp -a

Interface: 192.168.18.7 --- 0x4
 Internet Address      Physical Address      Type
192.168.18.1           0c-84-08-65-73-fc    dynamic
224.0.0.22             01-00-5e-00-00-16    static
224.0.0.252            01-00-5e-00-00-fc    static
255.255.255.255        ff-ff-ff-ff-ff-ff    static
```

9. hostname

The hostname command displays the name of the current computer on the network. It helps identify the system within a local or domain network.

Syntax : hostname

```
C:\Windows\System32>hostname
SS
```

10. getmac

Getmac displays the MAC addresses of all network adapters on the system. It is helpful for network identification and troubleshooting.

Syntax: getmac

```
C:\Windows\System32>getmac

Physical Address    Transport Name
=====
60-18-95-21-37-31  Media disconnected
E0-2B-E9-DE-BD-A9  \Device\Tcpip_{125A3DAD-F4C9-429C-8491-F533384C631F}
```

11. nbstat

Nbtstat displays NetBIOS over TCP/IP statistics and name tables. It is used to diagnose NetBIOS name resolution problems on a network.

Syntax: nbstat-n

```
C:\Windows\System32>nbtstat -n

Ethernet:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache

Wi-Fi:
Node IpAddress: [192.168.18.7] Scope Id: []

    NetBIOS Local Name Table

        Name                Type                Status
    -----
        SS                   <20>               UNIQUE             Registered
        SS                   <00>               UNIQUE             Registered
        WORKGROUP             <00>               GROUP              Registered

Local Area Connection* 1:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache

Local Area Connection* 10:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache
```

## **Discussion**

In this laboratory exercise, various network commands available in the Windows Operating System were studied and executed using the Command Prompt. Commands such as ping, tracert, ipconfig, and nslookup were used to test connectivity, analyze network paths, and verify IP and DNS configurations. Monitoring commands like netstat, arp, and getmac helped in observing active connections, IP-to-MAC mappings, and hardware addresses. Through this experiment, it was observed that each command serves a specific role in network troubleshooting. Some commands focus on connectivity testing, while others provide routing, name resolution, and interface information. The practical use of these commands improved understanding of how data flows through a network and how common network problems can be identified efficiently.

## **Conclusion**

In conclusion, Windows network commands were successfully studied and demonstrated using the Command Prompt.