Ex.no:1A **Date:25/07/2024**

Roll no:231901004

AIM:

Study of various Network commands used in Windows.

BASIC COMMANDS:

- **nslookup**: (name server lookup) is a tool used to perform DNS lookups in Linux. It is used to display DNS details, such as the IP address of a particular computer, the MX records for a domain or the NS servers of a domain. nslookup can operate in two modes: interactive and non-interactive.

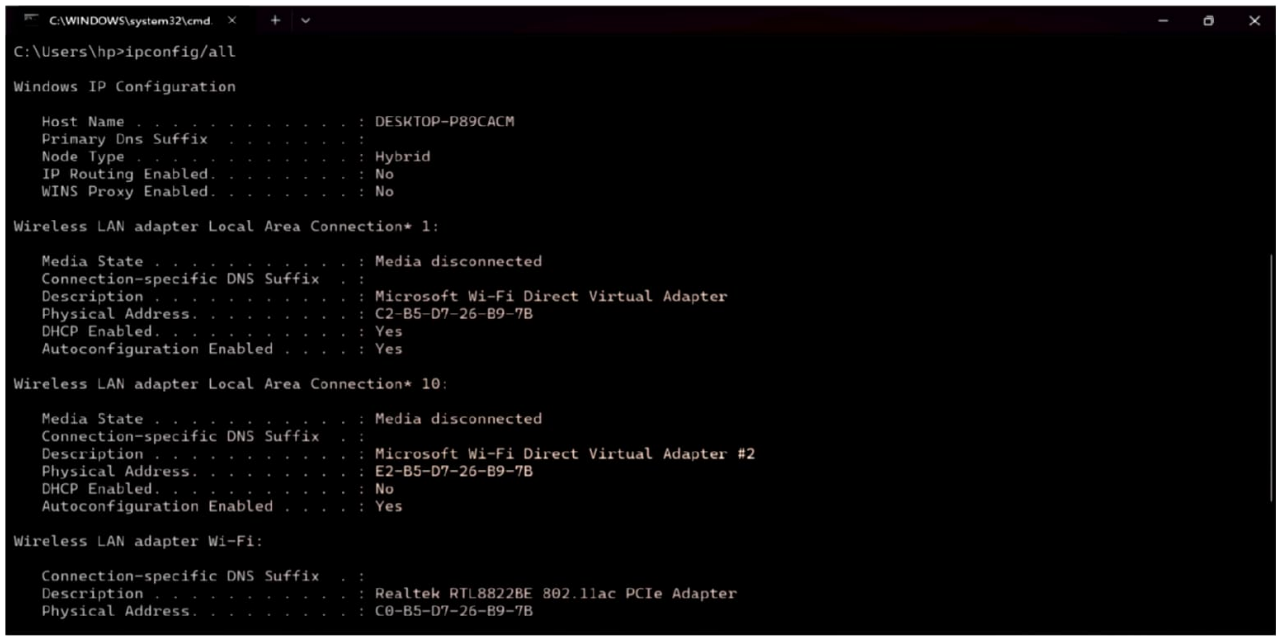
Syntax: nslookup www.google.com

```
C:\Users\hp>nslookup
Default Server:  Unknown
Address:  192.168.0.1

>
```

- **ipconfig /all:** This command displays detailed configuration information about your TCP/IP connection including Router, Gateway, DNS, DHCP, and type of Ethernet adapter in your system

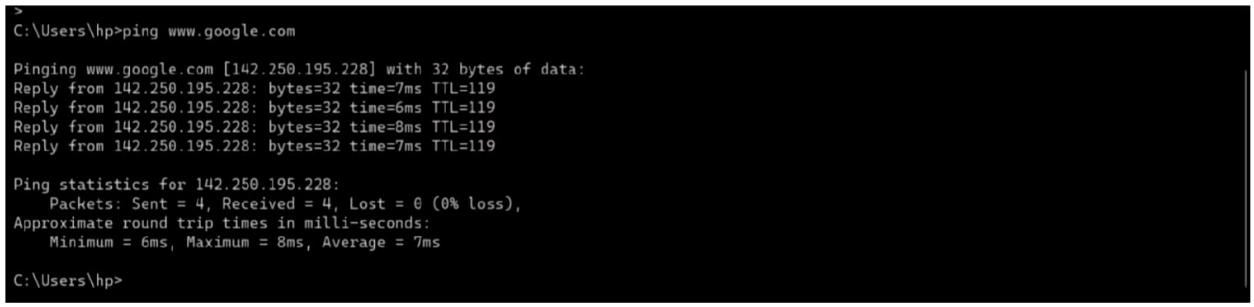
Syntax: ipconfig

```
C:\WINDOWS\system32\cmd
Microsoft Windows [Version 10.0.22631.3958]
(c) Microsoft Corporation. All rights reserved.

C:\Users\hp>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* 10:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::ba0c:98b3:6df0:cdc2%8
   IPv4 Address. . . . . . . . . . . : 192.168.0.105
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

C:\Users\hp>
```



- **ping**:(Packet INternet Groper) command is the best way to test connectivity between two nodes. Ping use ICMP (Internet Control Message Protocol) to communicate to other devices.

#ping hostname(ping localhost)
#ping ip address (ping 4.2.2.2)
#ping fully qualified domain name(ping www.facebook.com
Syntax: ping www.google.com



- **hostname:**
  This is the simplest of all TCP/IP commands. It simply displays the name of your computer.
  Syntax: hostname

```
C:\Users\hp>hostname
DESKTOP-P89CACM
```

- **Route:** route command is used to show/manipulate the IP routing table. It is primarily used to setup static routes to specific host or networks via an interface

  Syntax: tracert www.google.com

```
C:\Users\hp>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.

C:\Users\hp>tracert www.google.com

Tracing route to www.google.com [142.250.195.228]
over a maximum of 30 hops:

  1     1 ms     1 ms    <1 ms  192.168.0.1
  2    10 ms     9 ms     7 ms  10.1.0.1
  3     7 ms     7 ms     7 ms  103.88.76.2
  4     6 ms     6 ms     6 ms
```

- **arp – a**:ARP is short form of address resolution protocol, It will show the IP address of your computer along with the IP address and MAC address of your router.

  Syntax: arp

```
C:\Users\hp>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.

C:\Users\hp>tracert www.google.com

Tracing route to www.google.com [142.250.195.228]
over a maximum of 30 hops:

  1     1 ms     1 ms    <1 ms  192.168.0.1
  2    10 ms     9 ms     7 ms  10.1.0.1
  3     7 ms     7 ms     7 ms  103.88.76.2
  4     6 ms     6 ms     6 ms
```

- **netstat:** (network statistics) netstat displays a variety of statistics about a computers active TCP/IP connections. It is a command line tool for monitoring network connections both incoming and outgoing as well as viewing routing tables, interface statistics etc.

  Syntax: netstat -r

```
C:\Users\hp>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.0.105:52326    173:7506               ESTABLISHED
  TCP    192.168.0.105:52647    sl-in-f188:5228        ESTABLISHED
  TCP    192.168.0.105:61168    a23-202-229-23:https   CLOSE_WAIT
  TCP    192.168.0.105:61181    a23-202-229-22:https   CLOSE_WAIT
  TCP    192.168.0.105:61182    a23-202-229-22:https   CLOSE_WAIT
  TCP    192.168.0.105:61183    a23-202-229-22:https   CLOSE_WAIT
  TCP    192.168.0.105:61184    a23-202-229-22:https   CLOSE_WAIT
  TCP    192.168.0.105:61185    a23-202-229-22:https   CLOSE_WAIT
  TCP    192.168.0.105:61186    a23-202-229-22:https   CLOSE_WAIT
  TCP    192.168.0.105:61190    a23-202-229-22:https   CLOSE_WAIT
  TCP    192.168.0.105:61191    a23-202-229-22:https   CLOSE_WAIT
  TCP    192.168.0.105:61192    a23-202-229-22:https   CLOSE_WAIT
  TCP    192.168.0.105:61193    a23-202-229-22:https   CLOSE_WAIT
  TCP    192.168.0.105:61194    a23-202-229-22:https   CLOSE_WAIT
  TCP    192.168.0.105:61195    a23-202-229-22:https   CLOSE_WAIT
  TCP    192.168.0.105:64057    65:https               ESTABLISHED
```

RESULT:

Thus, the various basic windows commands were studied.