Practical: 3

AIM: Studying Windows network commands.
ping, pathping, ipconfig/ifconfig, arp, netstat, nbtstat, nslookup, route, traceroute/tracert, nmap.

Ganpat University | **U.V. Patel College of Engineering**
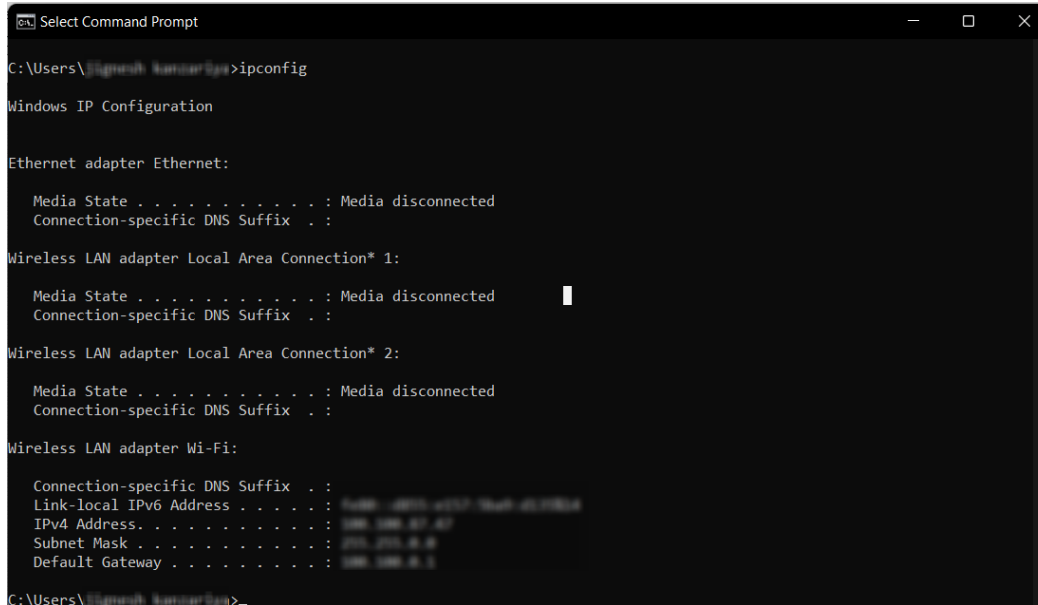|| विद्या समाजोत्कर्षः ||

Department of Computer
Engineering/Information Technology

Ipconfig :

The ipconfig command is a fast way of determining your computer's IP address and other information, such as the address of its default gateway useful if you want to know the IP address of your router's web interface.
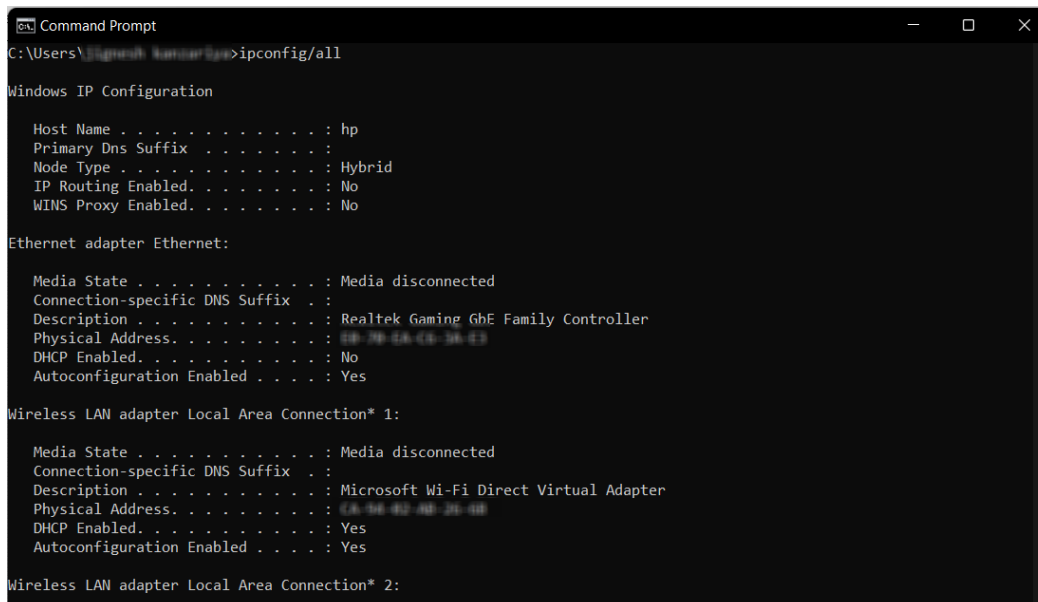
Ipconfig/all : all information about system.

Ping :

Ping is an old Unix tool that has been around for a long time but many PC users are unfamiliar with the Windows version. Ping sends out a packet to a designated internet host or network computer and measures its response time. Use ping whenever you need to verify that a host computer can connect to the TCP/IP network and network resources.

Arp –a: Displays and modifies the IP-to-Physical address translation tables used by address resolution protocol (ARP).

```
Command Prompt                                                    —    □    ✕

C:\Users\          >arp -a

Interface: 100.100.87.47 --- 0xe
  Internet Address      Physical Address      Type
  100.100.0.1           fe-ff-0a-46-10-33     dynamic
  100.100.255.255       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
  239.255.102.18        01-00-5e-7f-66-12     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\          >_
```

Netstat :

Netstat stands for network statistics. This command displays incoming and outgoing network connections as well as other network information. The netstat utility can show you the open connections on your computer, which programs are making which connections, how much data is being transmitted, and other information. The netstat command is a used to display very detailed information about how your computer is communicating with other computers or network devices.

```
Command Prompt                                                    —    □    ✕

C:\Users\          >netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    100.100.87.47:54416    49.44.8.243:https      ESTABLISHED
  TCP    100.100.87.47:54449    49.44.8.243:8443       ESTABLISHED
  TCP    100.100.87.47:54454    49.44.8.243:8443       ESTABLISHED
  TCP    100.100.87.47:54481    49.44.8.243:8443       ESTABLISHED
  TCP    100.100.87.47:54575    20.198.119.143:https   ESTABLISHED
  TCP    100.100.87.47:54631    20.189.173.6:https     ESTABLISHED
  TCP    100.100.87.47:54635    20.189.173.6:https     ESTABLISHED
  TCP    100.100.87.47:54649    relay-fcac249d:https   ESTABLISHED
  TCP    100.100.87.47:54694    a-0003:https           TIME_WAIT
  TCP    100.100.87.47:54706    a23-15-195-72:http     TIME_WAIT
  TCP    100.100.87.47:54720    a-0001:https           ESTABLISHED
  TCP    100.100.87.47:54723    a-0001:https           ESTABLISHED
  TCP    100.100.87.47:54766    13.107.4.52:http       TIME_WAIT
^C
C:\Users\          >
```

netstat –n:

```
Command Prompt                                                    —    □    ×

C:\Users\          >netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    100.100.87.47:54416    49.44.8.243:443        ESTABLISHED
  TCP    100.100.87.47:54449    49.44.8.243:8443       ESTABLISHED
  TCP    100.100.87.47:54454    49.44.8.243:8443       ESTABLISHED
  TCP    100.100.87.47:54481    49.44.8.243:8443       ESTABLISHED
  TCP    100.100.87.47:54575    20.198.119.143:443     ESTABLISHED
  TCP    100.100.87.47:54649    203.23.178.29:443      ESTABLISHED
  TCP    100.100.87.47:54859    13.107.4.52:80         TIME_WAIT
  TCP    100.100.87.47:54879    20.189.173.5:443       ESTABLISHED
  TCP    100.100.87.47:54880    20.189.173.5:443       ESTABLISHED
  TCP    127.0.0.1:54882        127.0.0.1:4843         SYN_SENT

C:\Users\          >
```
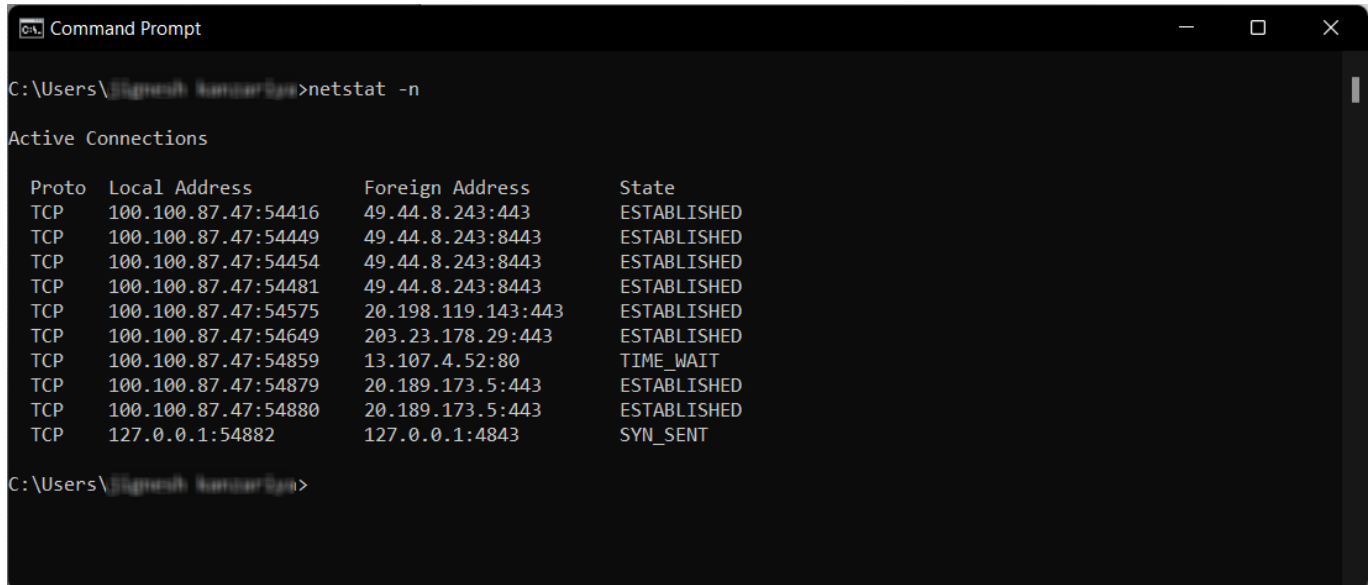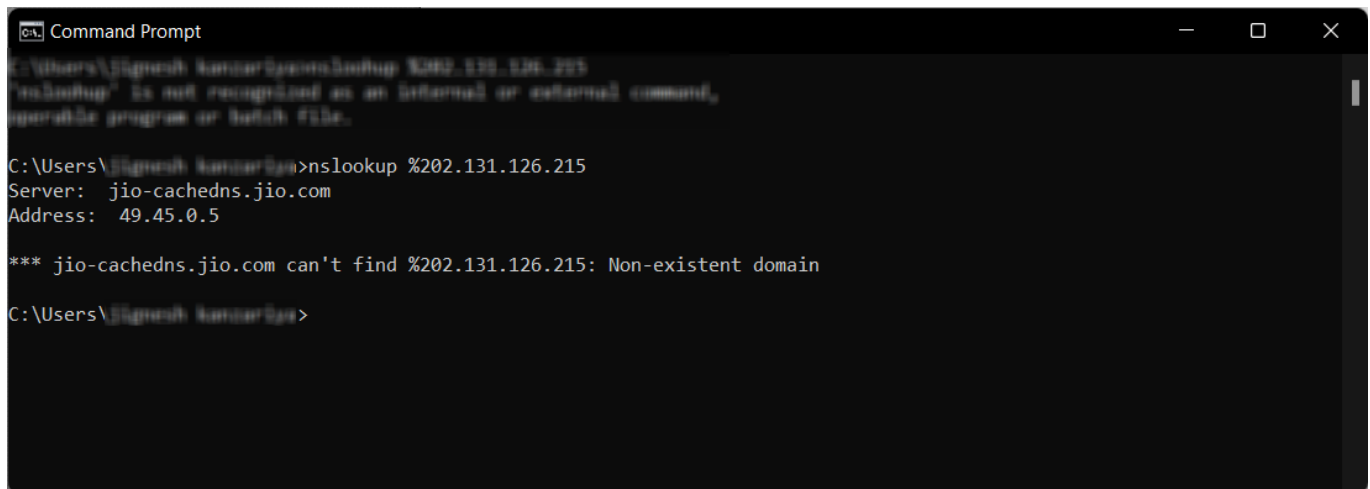
Nslookup: nslookup, which stands for "name server lookup", is a useful tool for finding out information about a domain named . This command helps diagnose the Domain Name System (DNS) infrastructure and comes with a number of sub-commands. These are mainly for systems administrators. The primary interest for average PC users is its use to find the computer name corresponding to a numeric IP.

```
Command Prompt                                                    —    □    ×

C:\Users\          >nslookup %202.131.126.215
'nslookup' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\          >nslookup %202.131.126.215
Server:  jio-cachedns.jio.com
Address:  49.45.0.5

*** jio-cachedns.jio.com can't find %202.131.126.215: Non-existent domain

C:\Users\          >
```

Tracert : A tracert is a tracking of a packet sent to a server. During its route this packet goes through several network devices (routers, firewall, etc.) and then goes finally at the server. With the tracert you can see the IP as well as the response time between each barrier.

```
Command Prompt                                                    —    □    ×

C:\Users\        >tracert 202.131.126.215

Tracing route to 202.131.126.215 over a maximum of 30 hops

  1     *        *        *      Request timed out.
  2    43 ms     7 ms     7 ms  192.168.103.14
  3    16 ms    22 ms    19 ms  172.26.109.164
  4    10 ms    12 ms     6 ms  172.26.109.178
  5   396 ms     6 ms   173 ms  192.168.38.27
  6     *        *        *      Request timed out.
  7     *        *        *      Request timed out.
  8     *        *        *      Request timed out.
  9    31 ms    41 ms    44 ms  182.79.206.229
 10     *        *        *      Request timed out.
 11   174 ms   177 ms   338 ms  59.145.238.94
 12   447 ms    83 ms    69 ms  202.131.97.241
 13    72 ms    51 ms    46 ms  202.131.97.106
 14    52 ms    42 ms    40 ms  180.211.126.2
 15     *        *        *      Request timed out.
 16    82 ms    47 ms    77 ms  202.131.126.215

Trace complete.

C:\Users\        >_
```

Route: If this is used in conjunction with one of the commands (such as add, change, or delete), the table is cleared prior to running the command. -p : When used with the add command, the specified route is added to the registry and is used to initialize the IP routing table whenever the TCP/IP protocol is started.

```
Select Command Prompt                                             —    □    ×

C:\Users\        >route print
===========================================================================
Interface List
 16...e0 70 ea c6 3a e3 ......Realtek Gaming GbE Family Controller
 17...ca 94 02 ab 26 6b ......Microsoft Wi-Fi Direct Virtual Adapter
  7...ea 94 02 ab 26 6b ......Microsoft Wi-Fi Direct Virtual Adapter #2
 14...c8 94 02 ab 26 6b ......Realtek RTL8852AE WiFi 6 802.11ax PCIe Adapter
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      100.100.0.1   100.100.87.47     50
      100.100.0.0      255.255.0.0         On-link    100.100.87.47    306
    100.100.87.47  255.255.255.255         On-link    100.100.87.47    306
   100.100.255.255  255.255.255.255         On-link    100.100.87.47    306
        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
        224.0.0.0        240.0.0.0         On-link    100.100.87.47    306
  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    100.100.87.47    306
===========================================================================
```

Ipconfig –flushdns : To ensure Windows is getting addresses from the new DNS servers instead of using old, cached entries, run the ipconfig /flushdns command after changing your DNS server.

Hostname: Useful to know machine name.
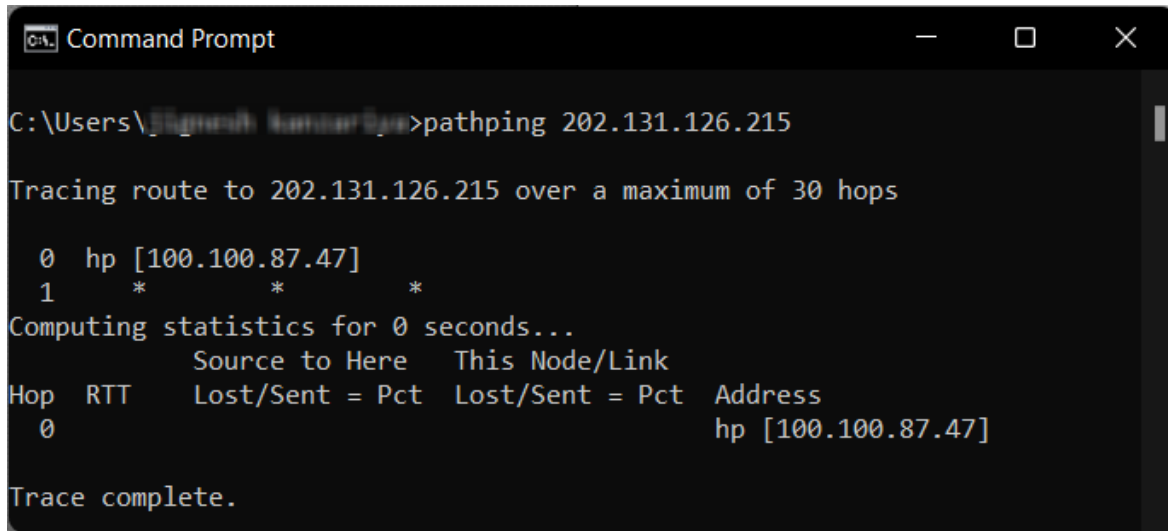
Pathping: The pathping command is a route tracing tool that combines features of the ping and tracert commands with additional information that neither of those tools provides. The pathping command sends packets to each router on the way to a final destination over a period of time, and then computes results based on the packets returned from each hop. Since the command shows the degree of packet loss at any given router or link, it is easy to determine which routers or links might be causing network problems.

getmac: using this command we can get MAC address.
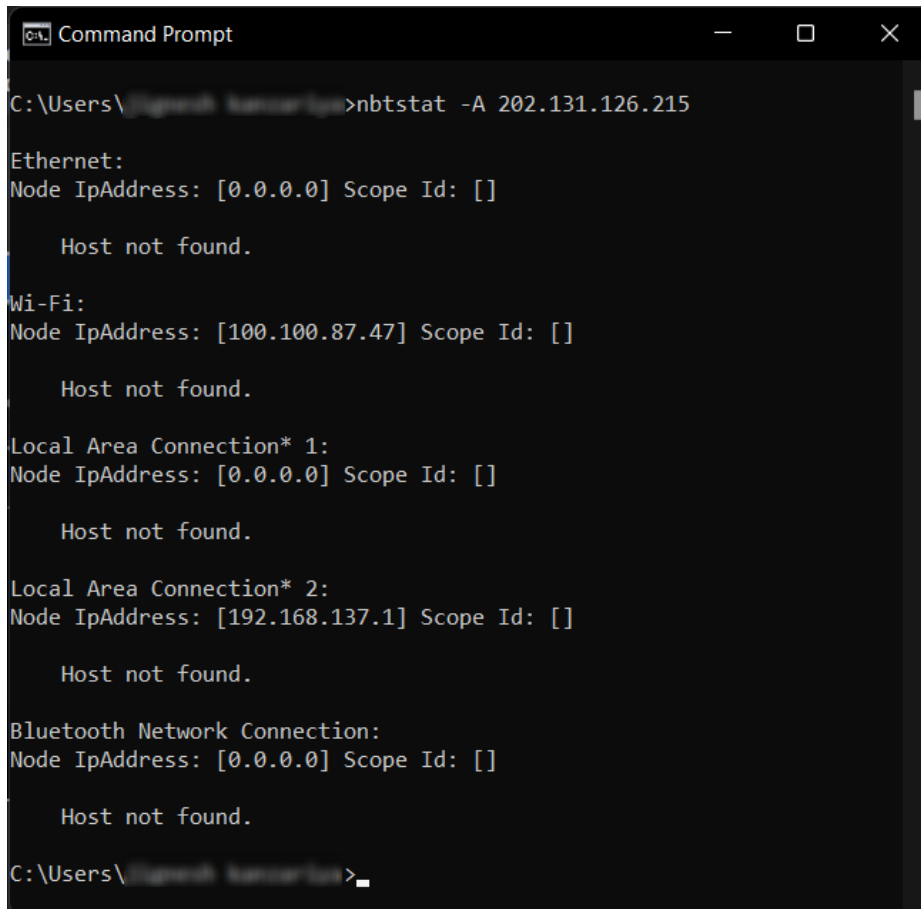
Nbtstat : Displays protocol statistics and current TCP/IP connections using NBT(NetBIOS over TCP/IP). Lists the remote machine's name table given its name.
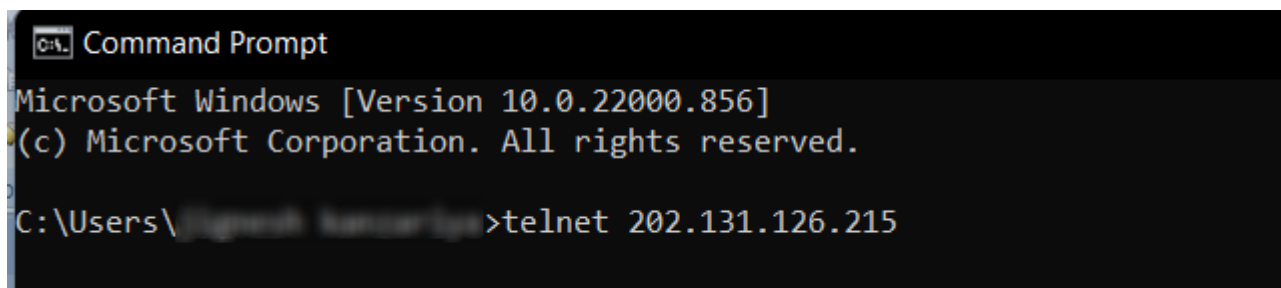
telnet : The telnet command to access to a remote host in Terminal mode (passive screen) .

net view: There may be a time where you want to see what devices are connected to your network. This is where the net view command comes in.

```
C:\Users\                >net view
Server Name              Remark

-------------------------------------------------------------------------------
\\HP
The command completed successfully.


C:\Users\                >_
```