Exp No: 1 **IP/Networking Commands**

Date:

AIM

COMMANDS

1) Ping: The **ping** command is used to test connectivity between two hosts. It sendsICMP echo request messages to the destination. The destination host replies with ICMP reply messages. If the ping command gets a reply from the destination host, it displays the reply along with round-trip times

```
Pinging google.com [142.250.193.110] with 32 bytes of data:
Reply from 142.250.193.110: bytes=32 time=2ms TTL=56
Reply from 142.250.193.110: bytes=32 time=9ms TTL=56
Reply from 142.250.193.110: bytes=32 time=3ms TTL=56
Reply from 142.250.193.110: bytes=32 time=3ms TTL=56

Ping statistics for 142.250.193.110:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 9ms, Average = 4ms
```

2) ipconfig: This command displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. This command is mainly used to view the IP addresses on the computers that are configured to obtain their IP address automatically.

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b2df:f0d9:48b5:4bf4%6
   IPv4 Address. . . . . . . . . . . : 172.20.105.17
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 172.20.105.1
```

3) ipconfig/all: Displays the full TCP/IP configuration for all adapters (Wired Ethernet, WiFi, Vmware adapters etc).

```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : pro-17
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Physical Address. . . . . . . . . : 48-9E-BD-9B-6C-85
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::b2df:f0d9:48b5:4bf4%6(Preferred)
   IPv4 Address. . . . . . . . . . . : 172.20.105.17(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 172.20.105.1
   DHCPv6 IAID . . . . . . . . . . . : 75556908
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-29-BB-7C-BD-48-9E-BD-9B-6C-85
   DNS Servers . . . . . . . . . . . : 8.8.8.8
                                       4.2.2.2
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

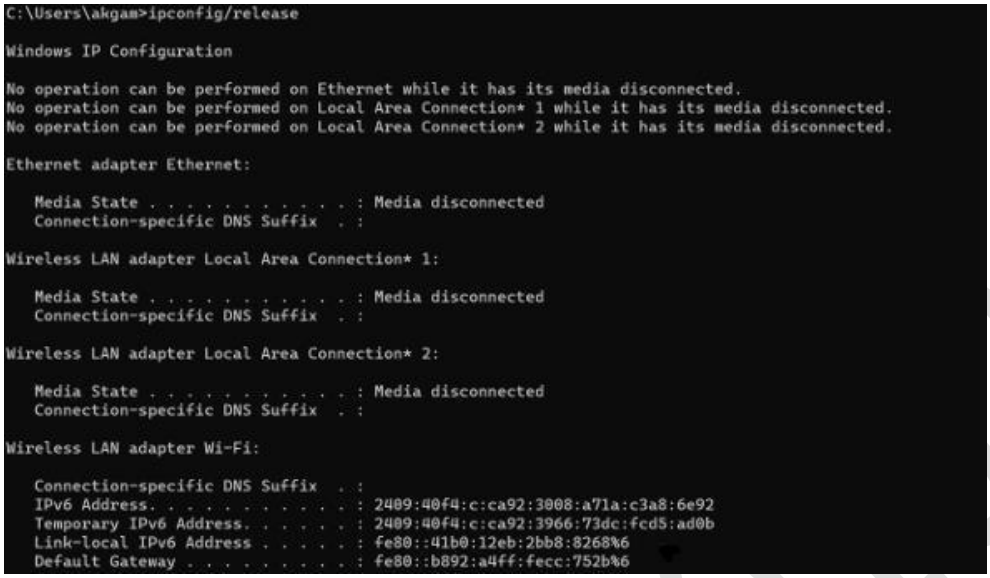
4) ipconfig/flushdns: This deletes the local DNS resolver cache of the computer. This cache stores DNS entries of frequently accessed internet resources so that the computer will not query an external DNS server every time you try to access an internet resource (website etc). This command is useful when troubleshooting DNS connection problems.

```
C:\Users\user>ipconfig/flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

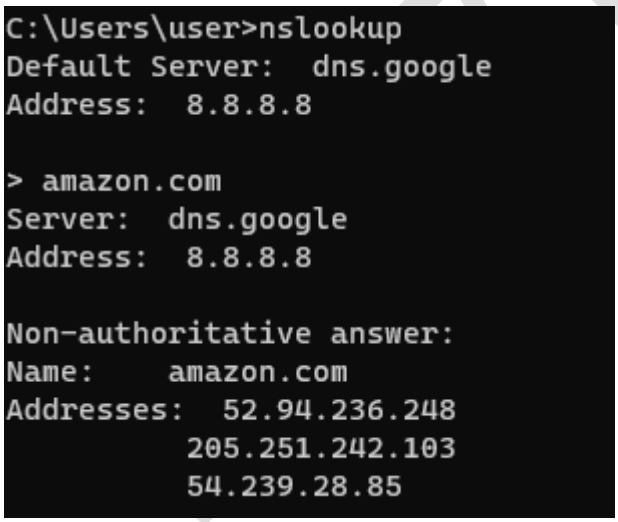
5) ipconfig/renew: The command "ipconfig /renew" is used in the Windows Command Prompt to renew the IP address of a network adapter. It's typically used to refresh the DHCP-assigned IP address of a device when it's connected to a network.

```
C:\Users\akgam>ipconfig/renew

Windows IP Configuration

No operation can be performed on Ethernet while it has its media disconnected.
No operation can be performed on Local Area Connection* 1 while it has its media disconnected.
No operation can be performed on Local Area Connection* 2 while it has its media disconnected.

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* 2:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2409:40f4:c:ca92:3008:a71a:c3a8:6e92
   Temporary IPv6 Address. . . . . . : 2409:40f4:c:ca92:3966:73dc:fcd5:ad0b
   Link-local IPv6 Address . . . . . : fe80::41b0:12eb:2bb8:8268%6
   IPv4 Address. . . . . . . . . . . : 192.168.53.77
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::b892:a4ff:fecc:752b%6
                                       192.168.53.190
```

6) ipconfig/release: The ipconfig /release command tells the server that provides the Dynamic Host Configuration Protocol (DHCP) to assign IP addresses to your computers that you no longer want to be part of the network.



7) nslookup: stands for “Name System Lookup” and is very useful in obtaining Domain Name System (DNS) related information about a domain or about an IP address (reverse DNS lookup).



8) nbtstat -a: This command helps solve problems with NetBIOS name resolution. (Nbt stands for NetBIOS over TCP/IP).

```
C:\Users\user>nbtstat -a

Displays protocol statistics and current TCP/IP connections using NBT
(NetBIOS over TCP/IP).

NBTSTAT [ [-a RemoteName] [-A IP address] [-c] [-n]
        [-r] [-R] [-RR] [-s] [-S] [interval] ]

  -a   (adapter status) Lists the remote machine's name table given its name
  -A   (Adapter status) Lists the remote machine's name table given its
                        IP address.
  -c   (cache)          Lists NBT's cache of remote [machine] names and their IP addresses
  -n   (names)          Lists local NetBIOS names.
  -r   (resolved)       Lists names resolved by broadcast and via WINS
  -R   (Reload)         Purges and reloads the remote cache name table
  -S   (Sessions)       Lists sessions table with the destination IP addresses
  -s   (sessions)       Lists sessions table converting destination IP
                        addresses to computer NETBIOS names.
  -RR  (ReleaseRefresh) Sends Name Release packets to WINS and then, starts Refresh

  RemoteName   Remote host machine name.
  IP address   Dotted decimal representation of the IP address.
  interval     Redisplays selected statistics, pausing interval seconds
               between each display. Press Ctrl+C to stop redisplaying
               statistics.
```

9) netstat: Netstat displays a variety of statistics about a computers active TCP/IP connections. This tool is most useful when you're having trouble with TCP/IP applications such as HTTP, and FTP

```
C:\Users\user>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:8080         pro-18:50617           TIME_WAIT
  TCP    127.0.0.1:8080         pro-18:50619           TIME_WAIT
  TCP    127.0.0.1:8080         pro-18:50620           TIME_WAIT
  TCP    127.0.0.1:8080         pro-18:50622           TIME_WAIT
  TCP    127.0.0.1:8080         pro-18:50624           TIME_WAIT
  TCP    127.0.0.1:8080         pro-18:50626           TIME_WAIT
  TCP    127.0.0.1:8080         pro-18:50627           TIME_WAIT
  TCP    127.0.0.1:8080         pro-18:50628           TIME_WAIT
  TCP    127.0.0.1:8080         pro-18:50629           TIME_WAIT
  TCP    127.0.0.1:8080         pro-18:50631           TIME_WAIT
  TCP    127.0.0.1:8080         pro-18:50633           TIME_WAIT
  TCP    127.0.0.1:8080         pro-18:50634           TIME_WAIT
  TCP    127.0.0.1:8080         pro-18:50635           TIME_WAIT
  TCP    127.0.0.1:8080         pro-18:50637           TIME_WAIT
  TCP    127.0.0.1:8080         pro-18:50638           TIME_WAIT
  TCP    127.0.0.1:8080         pro-18:50640           TIME_WAIT
  TCP    127.0.0.1:8080         pro-18:50642           TIME_WAIT
  TCP    127.0.0.1:8080         pro-18:50643           TIME_WAIT
  TCP    127.0.0.1:8080         pro-18:50644           TIME_WAIT
  TCP    127.0.0.1:8080         pro-18:50645           TIME_WAIT
  TCP    127.0.0.1:8080         pro-18:50646           TIME_WAIT
  TCP    127.0.0.1:8080         pro-18:50647           TIME_WAIT
  TCP    127.0.0.1:8080         pro-18:50648           TIME_WAIT
  TCP    127.0.0.1:8080         pro-18:50649           TIME_WAIT
  TCP    172.20.105.18:49707    20.198.119.143:https   ESTABLISHED
  TCP    172.20.105.18:50603    25:https               TIME_WAIT
  TCP    [::1]:8080             pro-18:50623           TIME_WAIT
  TCP    [::1]:8080             pro-18:50632           TIME_WAIT
  TCP    [::1]:8080             pro-18:50641           TIME_WAIT
```

10) arp -a: arp -a is short for address resolution protocol, It will show the IP address of your computer along with the IP address and MAC address of your router

```
C:\Users\user>arp -a

Interface: 172.20.105.18 --- 0x6
  Internet Address      Physical Address      Type
  172.20.104.11         48-9e-bd-9f-37-92     dynamic
  172.20.104.12         48-9e-bd-9f-38-52     dynamic
  172.20.104.13         48-9e-bd-9e-e7-30     dynamic
  172.20.104.14         48-9e-bd-9f-24-ab     dynamic
  172.20.104.15         48-9e-bd-9f-24-fa     dynamic
  172.20.104.17         48-9e-bd-9f-27-5a     dynamic
  172.20.104.18         48-9e-bd-9f-37-1b     dynamic
  172.20.104.19         48-9e-bd-9f-24-e2     dynamic
  172.20.104.20         48-9e-bd-9f-28-de     dynamic
  172.20.104.21         48-9e-bd-9f-35-1c     dynamic
  172.20.104.22         48-9e-bd-9e-f2-44     dynamic
  172.20.104.23         48-9e-bd-9f-21-c4     dynamic
  172.20.104.24         48-9e-bd-9f-2b-a3     dynamic
  172.20.104.26         48-9e-bd-9f-38-48     dynamic
  172.20.104.27         48-9e-bd-9f-38-61     dynamic
  172.20.104.28         48-9e-bd-9f-37-23     dynamic
  172.20.104.31         48-9e-bd-9f-26-18     dynamic
  172.20.104.32         48-9e-bd-9f-29-86     dynamic
```

11) tracert: The tracert command displays a list of all the routers that a packet has to go through to get from the computer where tracert is run to any other computer on the internet.

```
Tracing route to google.com [142.250.76.46]
over a maximum of 30 hops:

  1     *        *        *     Request timed out.
  2    <1 ms    <1 ms    <1 ms  172.20.100.1
  3     1 ms     5 ms     5 ms  14.139.188.161
  4     1 ms    <1 ms    <1 ms  10.119.236.201
  5     1 ms     3 ms     2 ms  10.163.251.21
  6     2 ms     2 ms     2 ms  10.119.73.122
  7     4 ms     5 ms     4 ms  72.14.195.128
  8     2 ms     2 ms     2 ms  216.239.43.131
  9     3 ms     3 ms     3 ms  142.250.235.105
 10     2 ms     2 ms     2 ms  maa03s36-in-f14.1e100.net [142.250.76.46]

Trace complete.
```

12) systeminfo: Systeminfo displays detailed configuration information about a computer and its operating system, including operating system configuration, security information, product ID, and hardware properties (such as RAM, disk space, and network cards).

```
Host Name:                 PRO-17
OS Name:                   Microsoft Windows 11 Pro
OS Version:                10.0.22621 N/A Build 22621
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00331-20140-00000-AA243
Original Install Date:     19-07-2023, 09:55:50
System Boot Time:          23-01-2024, 10:07:13
System Manufacturer:       HP
System Model:              HP 280 Pro G8 Microtower PC
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 165 Stepping 3 GenuineIntel ~3696 Mhz
BIOS Version:              AMI F.28, 20-02-2023
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             4009
Input Locale:              00004009
Time Zone:                 (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory:     16,099 MB
Available Physical Memory: 9,506 MB
Virtual Memory: Max Size:  17,123 MB
Virtual Memory: Available: 9,687 MB
Virtual Memory: In Use:    7,436 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\PRO-17
Hotfix(s):                 3 Hotfix(s) Installed.
                           [01]: KB5033920
                           [02]: KB5034123
                           [03]: KB5032393
Network Card(s):           1 NIC(s) Installed.
                           [01]: Realtek PCIe GbE Family Controller
                                 Connection Name: Ethernet
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 172.20.105.17
                                 [02]: fe80::b2df:f0d9:48b5:4bf4
Hyper-V Requirements:      VM Monitor Mode Extensions: Yes
                           Virtualization Enabled In Firmware: Yes
                           Second Level Address Translation: Yes
                           Data Execution Prevention Available: Yes
```

13) hostname: This is the simplest of all TCP/IP commands. It simply displays the name of your computer.

```
C:\Users\user>hostname
pro-17
```

14) pathping: Pathping is unique to Window's, and is basically a combination of the Ping and Tracert commands. Pathping traces the route to the destination address then launches a 25 second test of each router along the way, gathering statistics on the rate of data loss along each hop.

```
C:\Users\user>pathping google.com

Tracing route to google.com [142.250.76.46]
over a maximum of 30 hops:
  0  pro-17 [172.20.105.17]
  1     *        *        *
Computing statistics for 0 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           pro-17 [172.20.105.17]

Trace complete.
```

15) getmac: The 'getmac' command is a Windows command-line utility used to retrieve the media access control (MAC) address and the list of network protocols associated with each, locally or across a network.

```
C:\Users\user>getmac

Physical Address    Transport Name
=================== ============================================================
48-9E-BD-9B-6C-85   Media disconnected
```

16) route: The route command displays the computers routing table. A typical computer, with a single network interface, connected to a LAN, with a router is fairly simple and generally doesn't pose any network problems. But if you're having trouble accessing other computers on your network, you can use the route command to make sure the entries in the routing table are correct.

```
C:\Users\user>route

Manipulates network routing tables.

ROUTE [-f] [-p] [-4|-6] command [destination]
                  [MASK netmask]  [gateway] [METRIC metric]  [IF interface]

  -f           Clears the routing tables of all gateway entries.  If this is
               used in conjunction with one of the commands, the tables are
               cleared prior to running the command.

  -p           When used with the ADD command, makes a route persistent across
               boots of the system. By default, routes are not preserved
               when the system is restarted. Ignored for all other commands,
               which always affect the appropriate persistent routes.

  -4           Force using IPv4.

  -6           Force using IPv6.

  command      One of these:
                 PRINT     Prints  a route
                 ADD       Adds    a route
                 DELETE    Deletes a route
                 CHANGE    Modifies an existing route
  destination  Specifies the host.
  MASK         Specifies that the next parameter is the 'netmask' value.
  netmask      Specifies a subnet mask value for this route entry.
               If not specified, it defaults to 255.255.255.255.
  gateway      Specifies gateway.
  interface    the interface number for the specified route.
  METRIC       specifies the metric, ie. cost for the destination.

All symbolic names used for destination are looked up in the network database
file NETWORKS. The symbolic names for gateway are looked up in the host name
database file HOSTS.

If the command is PRINT or DELETE. Destination or gateway can be a wildcard,
(wildcard is specified as a star '*'), or the gateway argument may be omitted.

If Dest contains a * or ?, it is treated as a shell pattern, and only
matching destination routes are printed. The '*' matches any string,
and '?' matches any one char. Examples: 157.*.1, 157.*, 127.*, *224*.

Pattern match is only allowed in PRINT command.
Diagnostic Notes:
    Invalid MASK generates an error, that is when (DEST & MASK) != DEST.
    Example> route ADD 157.0.0.0 MASK 155.0.0.0 157.55.80.1 IF 1
             The route addition failed: The specified mask parameter is invalid. (Destination & Mask) != Destination.
```

17) netsh: Netsh is a command-line scripting utility that allows you to display or modify the network configuration of a computer that is currently running.

```
C:\Users\user>netsh interface ipv4 show addresses

Configuration for interface "Ethernet"
    DHCP enabled:                         No
    IP Address:                           172.20.105.8
    Subnet Prefix:                        172.20.0.0/16 (mask 255.255.0.0)
    Default Gateway:                      172.20.105.1
    Gateway Metric:                       256
    InterfaceMetric:                      25

Configuration for interface "Loopback Pseudo-Interface 1"
    DHCP enabled:                         No
    IP Address:                           127.0.0.1
    Subnet Prefix:                        127.0.0.0/8 (mask 255.0.0.0)
    InterfaceMetric:                      75
```

18) net share: We can use net share command from command line to create, configure and delete network shares.

```
C:\Users\user>net share

Share name   Resource                        Remark

-------------------------------------------------------------------------------
C$           C:\                             Default share
D$           D:\                             Default share
IPC$                                         Remote IPC
ADMIN$       C:\WINDOWS                      Remote Admin
The command completed successfully.
```

19) net use: Connects a computer to or disconnects a computer from a shared resource, or displays information about computer connections. The command also controls persistent net connections. Used without parameters, net use retrieves a list of network connections.

```
C:\Users\user>net use
New connections will be remembered.

There are no entries in the list.
```

20) net user: Net user command is used to Connects a computer or disconnects a computer from a shared resource, or displays information about computer connections. The command also controls persistent net connections. Used without parameters, net use retrieves a list of network connections.

```
C:\Users\user>net user

User accounts for \\PRO-08

-------------------------------------------------------------------------------
Admin                    Administrator            DefaultAccount
Guest                    user                     WDAGUtilityAccount
The command completed successfully.
```

21) netsh wlan show networks: WLAN Show All: shows detailed information about your Wi-Fi adapter including the adapter's capabilities, the Wi-Fi profiles on your PC (not including security keys or passwords), and a list of the Wi-Fi networks that were found when you ran the report.

```
C:\Users\akgam>netsh wlan show networks

Interface name : Wi-Fi
There are 1 networks currently visible.

SSID 1 : Dr. Sigma Stone
    Network type            : Infrastructure
    Authentication          : WPA3-Personal
    Encryption              : CCMP
```

22) taskkill: With the taskkill command is used to shutdown whole batches of processes at once, based on specific filters.

```
C:\WINDOWS\system32>taskkill /IM "notepad.exe" /F
SUCCESS: The process "Notepad.exe" with PID 1092 has been terminated.
```

23) netview: Netview is a command used to manage files shares, printer shares, and sessions in Windows.

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

-------------------------------------------------------------------------------
\\CODRUT-PC
\\ZENWIFI-AX           ZenWiFi_XT8
The command completed successfully.
```

24) typeperf: Windows allows you to see the network traffic easily in the *Task Manager*. However, that's a visual tool, and some users might want to get network utilization from the command line. Fortunately, there's a command for that too. It's called typeperf and lets you check the network traffic from CMD, although not in a friendly manner.

```
C:\Users\user>typeperf “\Network Interface(*)\Bytes Total/sec”


Error: No valid counters.

Note:
  In order to use typeperf, you must either be a member of the local
  Performance Log Users group, or the command must be executed from an
  elevated command window.
```

25) whoami: Displays user , group and priveleges information for the user who is currently logged on to the local system.

```
C:\Users\user>whoami
pro-17\user
```

RESULT