Name:- MOHAMMED TOUSIF
Roll No:- CB.EN.P2CYS22008

BASIC NETWORK ADMINISTRATION AND TROUBLESHOOTING USING WINDOWS COMMAND LINE UTILITIES

Date :- 03-10-2022

Aim :- To demonstrate the use of basic windows command line utilities to perform troubleshooting in network.

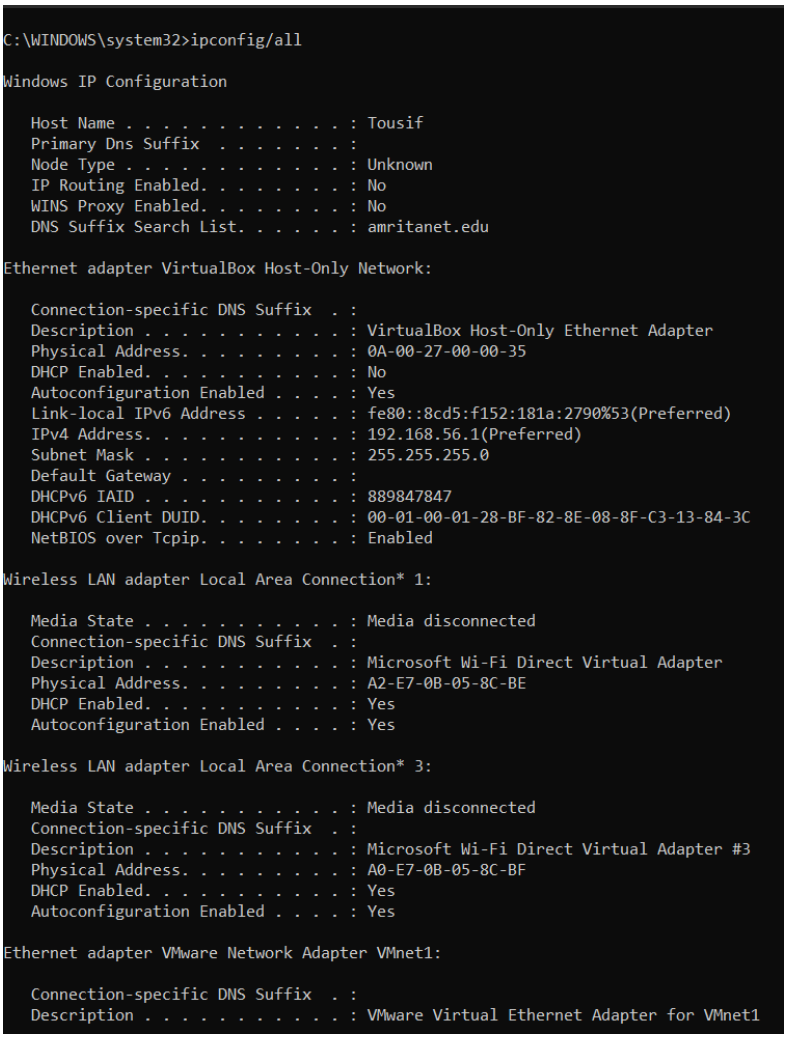
Tools Required :- Windows OS , CMD with Administrator privilege.

Procedure :-

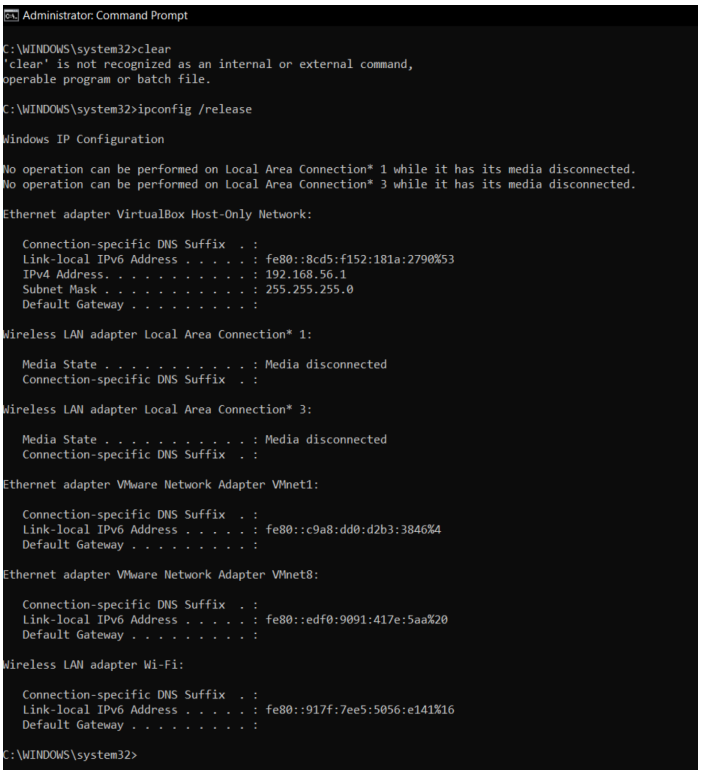
Windows command utilities allows you to administrator, diagnosis, monitor and repair network connections.

1. Open CMD by Administrator access.
2. Type **ipconfig** to verify the IP configuration settings of the machine.
3. We can use different ipconfig parameters such as:

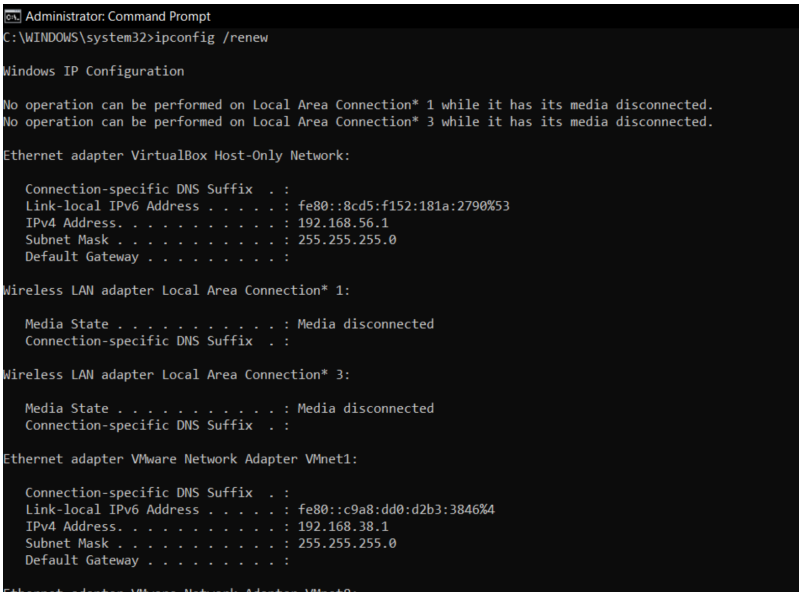
ipconfig/all : Displays IP configuration of all adapters.



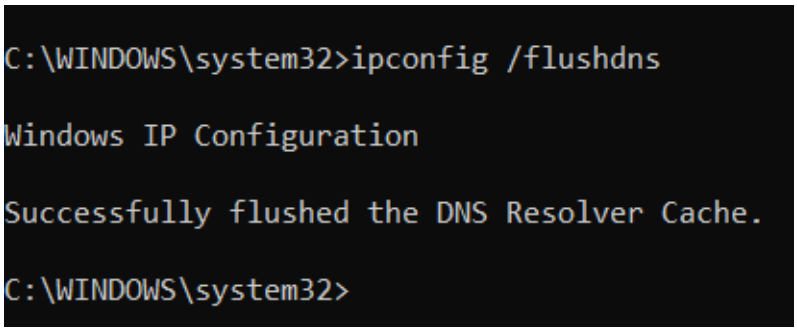
ipconfig/release : Release the current DHCP configuration.



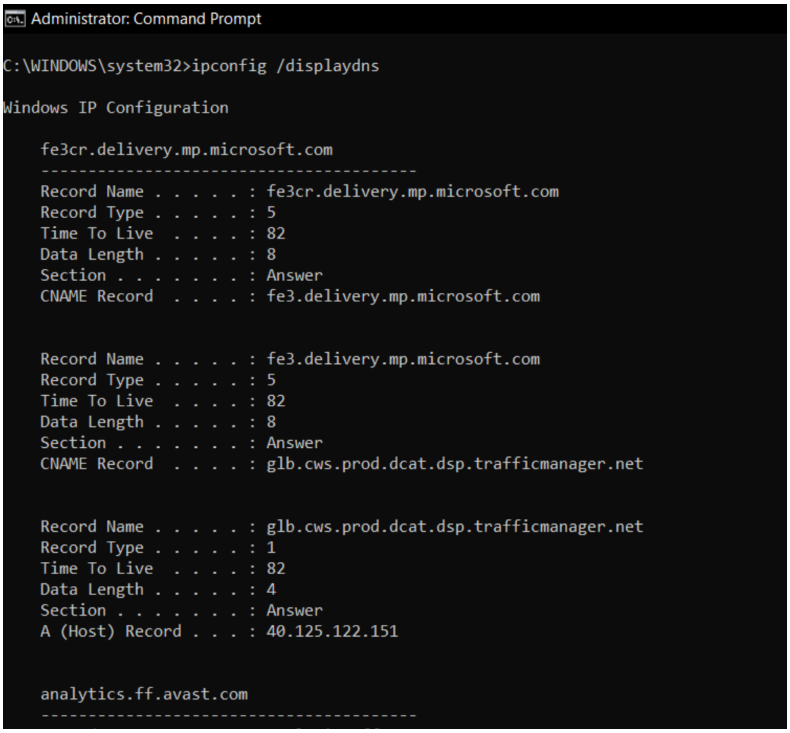
ipconfig/renew : Renews DHCP configuration for all adpaters.



ipconfig/flushdns : Flushes or removes the DNS cache and resets.



ipconfig/displaydns : Displays the contents of DNS cache.



ipconfig/registerdns : Initiates manual DNS registration.

```
C:\WINDOWS\system32>ipconfig /registerdns

Windows IP Configuration

Registration of the DNS resource records for all adapters of this computer has been initiated. Any errors will be reported in the Event Viewer in 15 minutes.
```

ipconfig showclassid Adapter : Displays DHCP class ID for specified adapter

```
C:\WINDOWS\system32>ipconfig /showclassid Wi-Fi

Windows IP Configuration


DHCPv4 Classes for Adapter "Wi-Fi":

   DHCPv4 ClassID Name . . . . . . . . : Default Routing and Remote Access Class
   DHCPv4 ClassID Description  . . . . : User class for remote access clients

   DHCPv4 ClassID Name . . . . . . . . : Default Network Access Protection Class
   DHCPv4 ClassID Description  . . . . : Default special user class for Restricted Access clients

   DHCPv4 ClassID Name . . . . . . . . : Default BOOTP Class
   DHCPv4 ClassID Description  . . . . : User class for BOOTP Clients

C:\WINDOWS\system32>
```

ipconfig/? : Displays help screen

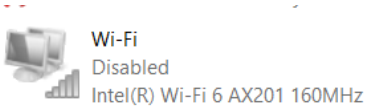
```
Administrator: Command Prompt

C:\WINDOWS\system32>ipconfig /?

USAGE:
    ipconfig [/allcompartments] [/? | /all |
                                 /renew [adapter] | /release [adapter] |
                                 /renew6 [adapter] | /release6 [adapter] |
                                 /flushdns | /displaydns | /registerdns |
                                 /showclassid adapter |
                                 /setclassid adapter [classid] |
                                 /showclassid6 adapter |
                                 /setclassid6 adapter [classid] ]

where
    adapter             Connection name
                       (wildcard characters * and ? allowed, see examples)

    Options:
       /?               Display this help message
       /all             Display full configuration information.
       /release         Release the IPv4 address for the specified adapter.
       /release6        Release the IPv6 address for the specified adapter.
       /renew           Renew the IPv4 address for the specified adapter.
       /renew6          Renew the IPv6 address for the specified adapter.
       /flushdns        Purges the DNS Resolver cache.
       /registerdns     Refreshes all DHCP leases and re-registers DNS names
       /displaydns      Display the contents of the DNS Resolver Cache.
       /showclassid     Displays all the dhcp class IDs allowed for adapter.
       /setclassid      Modifies the dhcp class id.
       /showclassid6    Displays all the IPv6 DHCP class IDs allowed for adapter.
       /setclassid6     Modifies the IPv6 DHCP class id.
```

Checking IP level connectivity using **ping** command.

Ping command is used to ensure the reachability of a host to other hosts in the Internet Protocol network. Errors such as Request timed out , Transmit failed , Destination host unreachable etc. will be faced by the network administrators.

Thus, to ensure the reachability of a host, **ping** command is used.

1. First , Wi-Fi adapter will be disabled in order to see the failure of host reachable.



2. Type **ping** in the command prompt followed the **IP** address of the Wi-Fi adapter.

```
C:\WINDOWS\system32>ping 10.11.133.72

Pinging 10.11.133.72 with 32 bytes of data:
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.

Ping statistics for 10.11.133.72:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\WINDOWS\system32>
```

As the adapter is disabled, the host is unreachable. Thus , showing an error transmit failed. General failure. upon this adapter.

3. Enable the Wi-Fi adapter. Type **ping** again followed by **IP** address of the adapter.

As it is enabled, host is reachable now.

```
C:\WINDOWS\system32>ping 10.11.133.72

Pinging 10.11.133.72 with 32 bytes of data:
Reply from 10.11.133.72: bytes=32 time<1ms TTL=128
Reply from 10.11.133.72: bytes=32 time<1ms TTL=128
Reply from 10.11.133.72: bytes=32 time<1ms TTL=128
Reply from 10.11.133.72: bytes=32 time<1ms TTL=128

Ping statistics for 10.11.133.72:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\WINDOWS\system32>
```

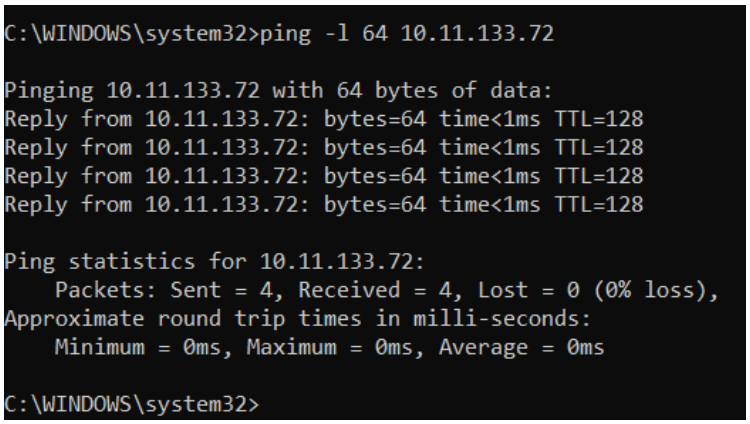
Thus the packets were transmitted and **ping** executed successfully without any loss.

ping command can accept certain options such as -n -l -w.

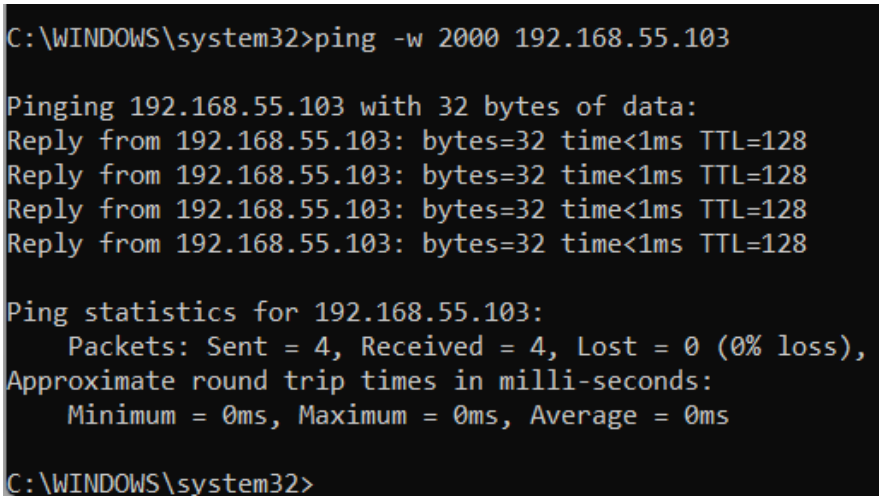
ping -n [IP address] : Determines the no of echo requests to send.

```
C:\WINDOWS\system32>ping -n 6 10.11.133.72

Pinging 10.11.133.72 with 32 bytes of data:
Reply from 10.11.133.72: bytes=32 time<1ms TTL=128
Reply from 10.11.133.72: bytes=32 time<1ms TTL=128
Reply from 10.11.133.72: bytes=32 time<1ms TTL=128
Reply from 10.11.133.72: bytes=32 time<1ms TTL=128
Reply from 10.11.133.72: bytes=32 time<1ms TTL=128
Reply from 10.11.133.72: bytes=32 time<1ms TTL=128

Ping statistics for 10.11.133.72:
    Packets: Sent = 6, Received = 6, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\WINDOWS\system32>
```

ping -l [IP address] : Determines the size of the ping packet.



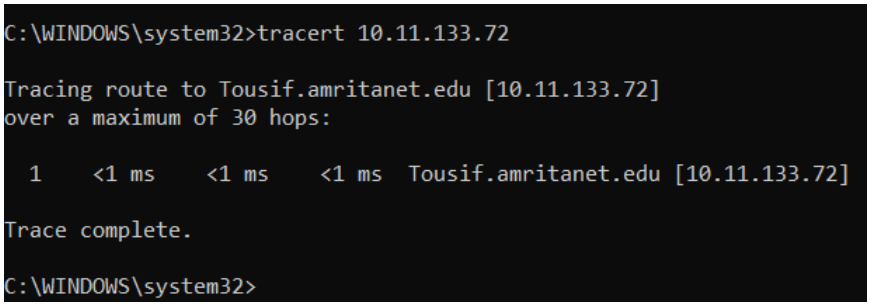
ping -w [IP address] : Determines to adjust the timeout (in milliseconds).



Tracing the route of packets using **tracert** command.

The trace route command known as **tracert** command which displays the time taken for a packet of information to travel between source and destination.

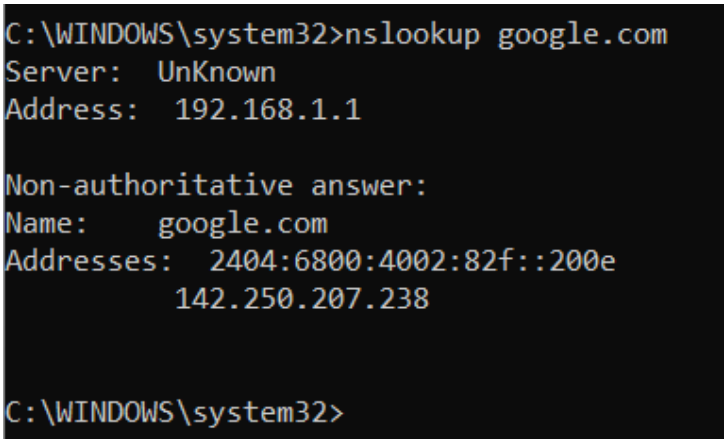
- **tracert** is useful for diagnosing large networks where several paths can lead to the same point or where many intermediate components are involved.



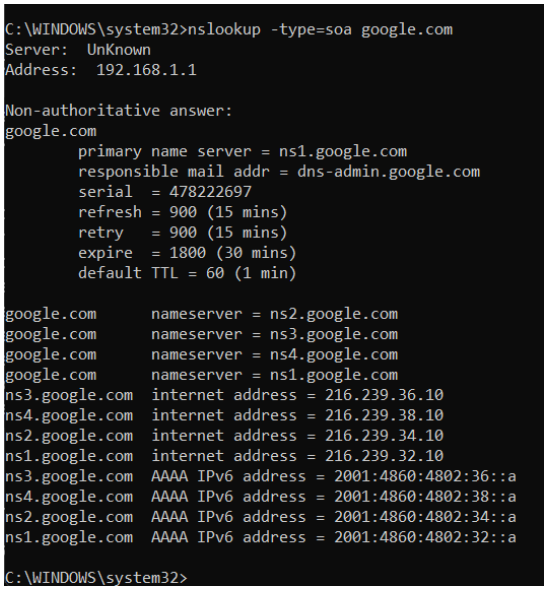
In the above picture we can see that the packet is travelled to the destination and it reached in the first hop itself.

nslookup: nslookup command stands for name server lookup.

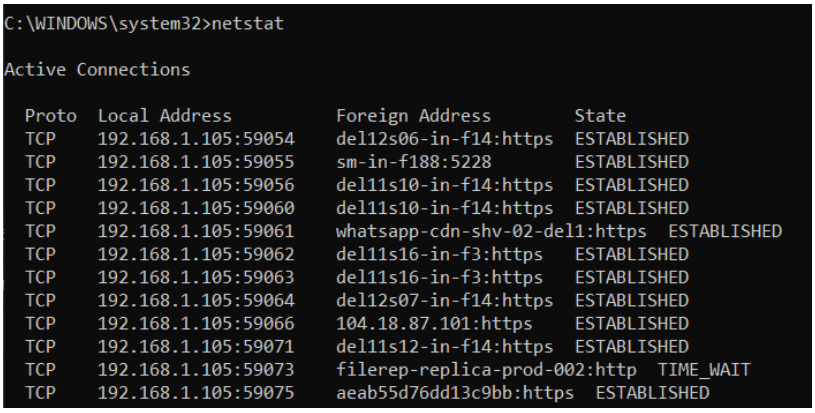
It is used to query a DNS server to obtain its domain name and associated IP address.



nslookup -type : nslookup command with -type parameter is used to get non-authorative name server information.



netstat : netstat command is used to display the contents of various network related data for active connections.



netstat -a : netstat -a displays all the TCP connections.

```
C:\WINDOWS\system32>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            Tousif:0               LISTENING
  TCP    0.0.0.0:445            Tousif:0               LISTENING
  TCP    0.0.0.0:808            Tousif:0               LISTENING
  TCP    0.0.0.0:902            Tousif:0               LISTENING
  TCP    0.0.0.0:912            Tousif:0               LISTENING
  TCP    0.0.0.0:2869           Tousif:0               LISTENING
  TCP    0.0.0.0:5040           Tousif:0               LISTENING
  TCP    0.0.0.0:7070           Tousif:0               LISTENING
  TCP    0.0.0.0:49664          Tousif:0               LISTENING
```

netstat -e : Displays ethernet statistics.

```
C:\WINDOWS\system32>netstat -e
Interface Statistics

                           Received            Sent

Bytes                    1247324448        59586734
Unicast packets             921912          430932
Non-unicast packets           1032            5346
Discards                         0               0
Errors                           0               0
Unknown protocols                0

C:\WINDOWS\system32>
```

netstat -n : Displays addresses and port numbers in numerical form.

```
C:\WINDOWS\system32>netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.1.105:59055    142.250.4.188:5228     ESTABLISHED
  TCP    192.168.1.105:59061    157.240.239.60:443     ESTABLISHED
  TCP    192.168.1.105:59196    34.193.122.215:443     ESTABLISHED
  TCP    192.168.1.105:59206    172.217.167.3:443      TIME_WAIT
  TCP    192.168.1.105:59265    34.234.57.251:443      CLOSE_WAIT
  TCP    192.168.1.105:59269    18.66.63.55:443        TIME_WAIT
  TCP    192.168.1.105:59277    99.83.135.170:443      TIME_WAIT
  TCP    192.168.1.105:59278    54.90.229.34:443       ESTABLISHED
  TCP    192.168.1.105:59281    103.217.246.161:443    ESTABLISHED
  TCP    192.168.1.105:60446    168.119.150.210:443    ESTABLISHED
```

netstat -o : Displays active TCP connections with process IDs

```
C:\WINDOWS\system32>netstat -o

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    192.168.1.105:59055    sm-in-f188:5228        ESTABLISHED     11600
  TCP    192.168.1.105:59061    whatsapp-cdn-shv-02-del1:https  ESTABLISHED     11600
  TCP    192.168.1.105:59196    ec2-34-193-122-215:https  ESTABLISHED     16688
  TCP    192.168.1.105:59206    del03s15-in-f3:https   TIME_WAIT       0
  TCP    192.168.1.105:59265    ec2-34-234-57-251:https  CLOSE_WAIT      16688
```

netstat -p : Shows connections and state for specified protocol.

```
C:\WINDOWS\system32>netstat -p tcp

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.1.105:59055    sm-in-f188:5228        ESTABLISHED
  TCP    192.168.1.105:59061    whatsapp-cdn-shv-02-del1:https  ESTABLISHED
  TCP    192.168.1.105:59196    ec2-34-193-122-215:https  ESTABLISHED
  TCP    192.168.1.105:59265    ec2-34-234-57-251:https  CLOSE_WAIT
  TCP    192.168.1.105:59278    ec2-54-90-229-34:https  CLOSE_WAIT
  TCP    192.168.1.105:59285    223:https              TIME_WAIT
  TCP    192.168.1.105:59286    223:https              TIME_WAIT
  TCP    192.168.1.105:60446    relay-dec6b013:https   ESTABLISHED
```

netstat -s : Displays statistics by protocols.

```
C:\WINDOWS\system32>netstat -s

IPv4 Statistics

  Packets Received                   = 778230
  Received Header Errors             = 0
  Received Address Errors            = 35
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 0
  Received Packets Discarded         = 17792
  Received Packets Delivered         = 813912
  Output Requests                    = 299891
  Routing Discards                   = 0
  Discarded Output Packets           = 4441
  Output Packet No Route             = 170
  Reassembly Required                = 1314
  Reassembly Successful              = 235
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 199
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 796

IPv6 Statistics

  Packets Received                   = 15606
  Received Header Errors             = 0
  Received Address Errors            = 41
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 0
```

netstat -r : Displays the contents of IP routing table.

```
C:\WINDOWS\system32>netstat -r
===========================================================================
Interface List
  6...08 8f c3 13 84 3c ......Realtek PCIe GbE Family Controller
 15...0a 00 27 00 00 0f ......VirtualBox Host-Only Ethernet Adapter
 16...a2 e7 0b 05 8c be ......Microsoft Wi-Fi Direct Virtual Adapter
  8...a0 e7 0b 05 8c bf ......Microsoft Wi-Fi Direct Virtual Adapter #3
  4...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
 21...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
 17...a0 e7 0b 05 8c be ......Intel(R) Wi-Fi 6 AX201 160MHz
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.1    192.168.1.105     55
        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
      192.168.1.0    255.255.255.0         On-link     192.168.1.105    311
```

netstat interval : Redisplays selected information every interval seconds untill user stops it.

```
C:\WINDOWS\system32>netstat -n 6

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.1.105:59055    142.250.4.188:5228     ESTABLISHED
  TCP    192.168.1.105:59061    157.240.239.60:443     ESTABLISHED
  TCP    192.168.1.105:59265    34.234.57.251:443      CLOSE_WAIT
  TCP    192.168.1.105:59290    3.214.22.3:443         CLOSE_WAIT
  TCP    192.168.1.105:59295    5.45.59.252:80         TIME_WAIT
  TCP    192.168.1.105:59296    150.107.8.152:80       TIME_WAIT
  TCP    192.168.1.105:60446    168.119.150.210:443    ESTABLISHED
  TCP    192.168.1.105:60483    20.198.119.143:443     ESTABLISHED
  TCP    192.168.1.105:60586    104.42.50.130:443      ESTABLISHED
  TCP    192.168.1.105:63925    34.225.126.187:443     CLOSE_WAIT
  TCP    192.168.1.105:64281    5.62.54.89:443         ESTABLISHED
```

netstat /? : Displays helps screen for netstat.

```
C:\WINDOWS\system32>netstat /?

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-f] [-i] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [interval]

  -a            Displays all connections and listening ports.
  -b            Displays the executable involved in creating each connection or
                listening port. In some cases well-known executables host
                multiple independent components, and in these cases the
                sequence of components involved in creating the connection
                or listening port is displayed. In this case the executable
                name is in [] at the bottom, on top is the component it called,
                and so forth until TCP/IP was reached. Note that this option
                can be time-consuming and will fail unless you have sufficient
                permissions.
  -e            Displays Ethernet statistics. This may be combined with the -s
                option.
  -f            Displays Fully Qualified Domain Names (FQDN) for foreign
                addresses.
```

arp -a : Displays ARP cache. The cache has a mapping of IP addresses with their respective MAC addresses.

```
C:\WINDOWS\system32>arp -a

Interface: 192.168.38.1 --- 0x4
  Internet Address      Physical Address      Type
  192.168.38.254        00-50-56-ee-4a-2d     dynamic
  192.168.38.255        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

Interface: 192.168.56.1 --- 0xf
  Internet Address      Physical Address      Type
  192.168.56.255        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
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

Gpresult : Tool that displays the Resultant Set of Policy

```
C:\WINDOWS\system32>Gpresult /R

Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
© Microsoft Corporation. All rights reserved.

Created on  02- 10- 2022 at 10:16:21 PM


RSOP data for TOUSIF\TOUSIF on TOUSIF : Logging Mode
-----------------------------------------------------

OS Configuration:            Standalone Workstation
OS Version:                  10.0.22000
Site Name:                   N/A
Roaming Profile:             N/A
Local Profile:               C:\Users\TOUSIF
Connected over a slow link?: No


COMPUTER SETTINGS
------------------

    Last time Group Policy was applied: 30-09-2022 at 02:11:11 PM
    Group Policy was applied from:      N/A
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        LAPTOP-N13U1A7R
    Domain Type:                        WindowsNT 4
```

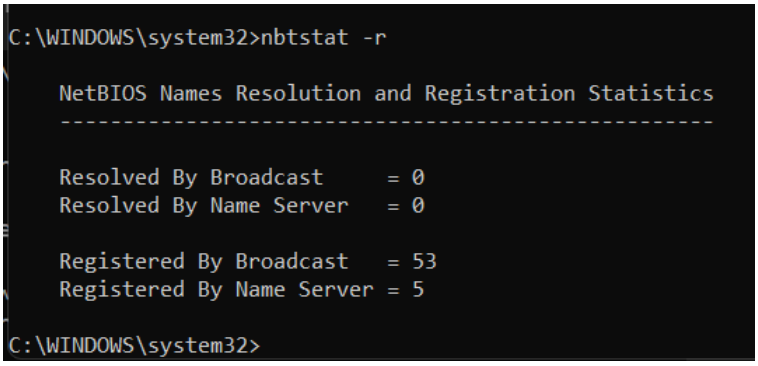
nbtstat -R : Purges and reloads the remote cache name table.

```
C:\WINDOWS\system32>nbtstat -R
    Successful purge and preload of the NBT Remote Cache Name Table.
```

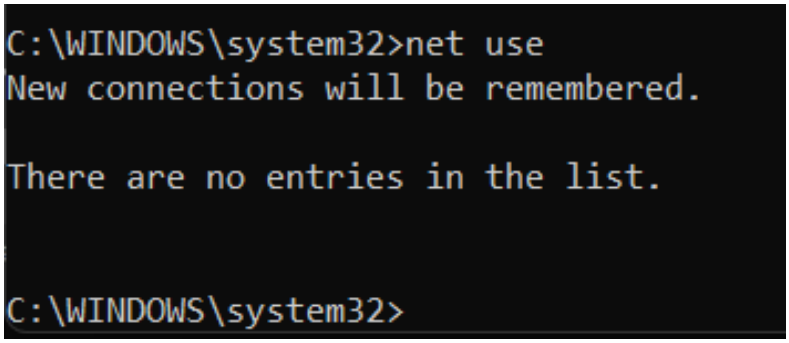
nbtstat -n : Lists local NetBIOS names.

```
C:\WINDOWS\system32>nbtstat -n

VirtualBox Host-Only Network:
Node IpAddress: [192.168.56.1] Scope Id: []

               NetBIOS Local Name Table

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

VMware Network Adapter VMnet1:
Node IpAddress: [192.168.38.1] Scope Id: []

               NetBIOS Local Name Table

      Name               Type         Status
    ---------------------------------------------
    TOUSIF         <00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered
```

nbtstat -r : Lists the names resolved by WINS(Windows Internet Name Service).

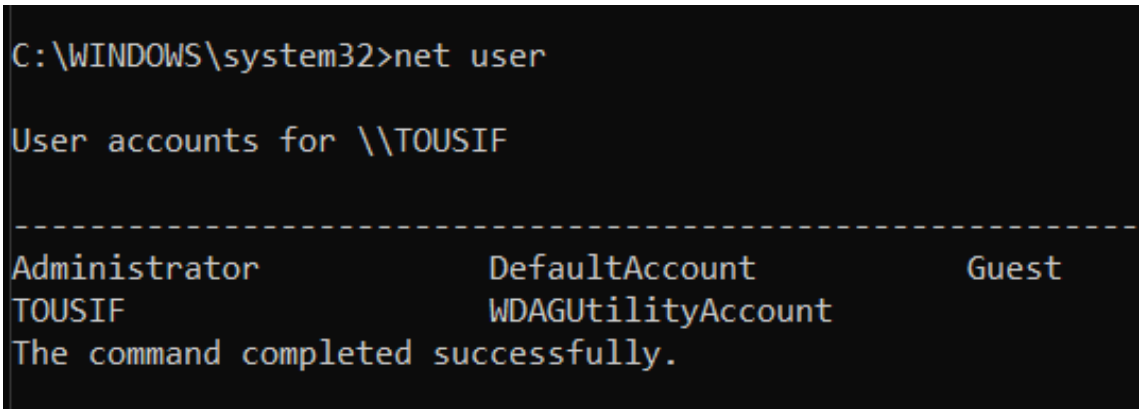


net use : Lists all shared resources currently in use under current user that logged in.



No shared resources in this example.

net user : Returns the list of all the user accounts in computer.



net user <username> : Displays details of particular user.

```
C:\WINDOWS\system32>net user TOUSIF
User name                    TOUSIF
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            16-10-2021 11:30:00 AM
Password expires             Never
Password changeable          16-10-2021 11:30:00 AM
Password required            No
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   02-10-2022 09:36:50 PM

Logon hours allowed          All
```

ping -a : Used to send ping requests to specified IP/domain.

```
C:\WINDOWS\system32>ping -a google.com

Pinging google.com [142.250.207.238] with 32 bytes of data:
Reply from 142.250.207.238: bytes=32 time=6ms TTL=117
Reply from 142.250.207.238: bytes=32 time=18ms TTL=117
Reply from 142.250.207.238: bytes=32 time=8ms TTL=117
Reply from 142.250.207.238: bytes=32 time=11ms TTL=117

Ping statistics for 142.250.207.238:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 18ms, Average = 10ms
```

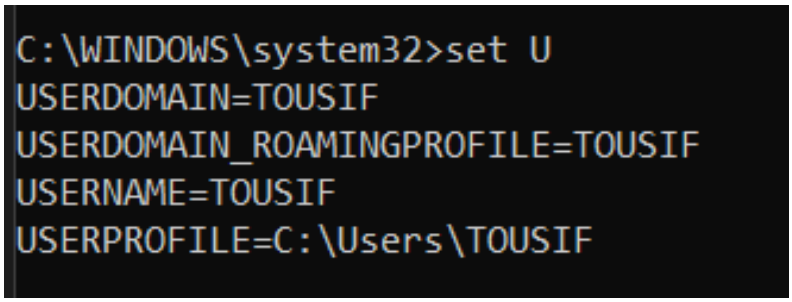
ping -t : Used to ping host untill user stops it.

```
C:\WINDOWS\system32>ping -t google.com

Pinging google.com [142.250.207.238] with 32 bytes of data:
Reply from 142.250.207.238: bytes=32 time=10ms TTL=117
Reply from 142.250.207.238: bytes=32 time=11ms TTL=117
Reply from 142.250.207.238: bytes=32 time=8ms TTL=117
Reply from 142.250.207.238: bytes=32 time=26ms TTL=117
Reply from 142.250.207.238: bytes=32 time=8ms TTL=117
Reply from 142.250.207.238: bytes=32 time=10ms TTL=117
Reply from 142.250.207.238: bytes=32 time=27ms TTL=117
Reply from 142.250.207.238: bytes=32 time=16ms TTL=117
Reply from 142.250.207.238: bytes=32 time=12ms TTL=117
Reply from 142.250.207.238: bytes=32 time=10ms TTL=117
Reply from 142.250.207.238: bytes=32 time=8ms TTL=117

Ping statistics for 142.250.207.238:
    Packets: Sent = 11, Received = 11, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 27ms, Average = 13ms
Control-C
^C
C:\WINDOWS\system32>
```

pathping : Command that combines the functionality of ping and tracert

```
C:\WINDOWS\system32>pathping google.com

Tracing route to google.com [142.250.207.238]
over a maximum of 30 hops:
  0  Tousif [192.168.1.105]
  1  192.168.1.1
  2  192.168.0.1
  3  192.168.1.1
  4  192.168.0.1
  5  10.19.128.1
  6  74.125.147.233
  7  108.170.237.85
  8  142.251.76.175
  9  del12s11-in-f14.1e100.net [142.250.207.238]

Computing statistics for 225 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           Tousif [192.168.1.105]
                                 0/ 100 =  0%   |
  1   16ms     0/ 100 =  0%     0/ 100 =  0%  192.168.1.1
                                 0/ 100 =  0%   |
  2   20ms     0/ 100 =  0%     0/ 100 =  0%  192.168.0.1
                                 0/ 100 =  0%   |
  3   21ms     0/ 100 =  0%     0/ 100 =  0%  192.168.1.1
                                 0/ 100 =  0%   |
  4   19ms     1/ 100 =  1%     1/ 100 =  1%  192.168.0.1
                                 0/ 100 =  0%   |
```

set U : Used to display environmental variables for specific user.



set L : Displays all from the set command that starts with L