BASIC NETWORK ADMINISTRATION AND TROUBLE SHOOTING USING WINDOW COMMAND LINE UTILITIES

NAME: KARTHIKA P

DATE :28|09|22 **ROLL NO**: CB.EN.P2CYS22001

AIM

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

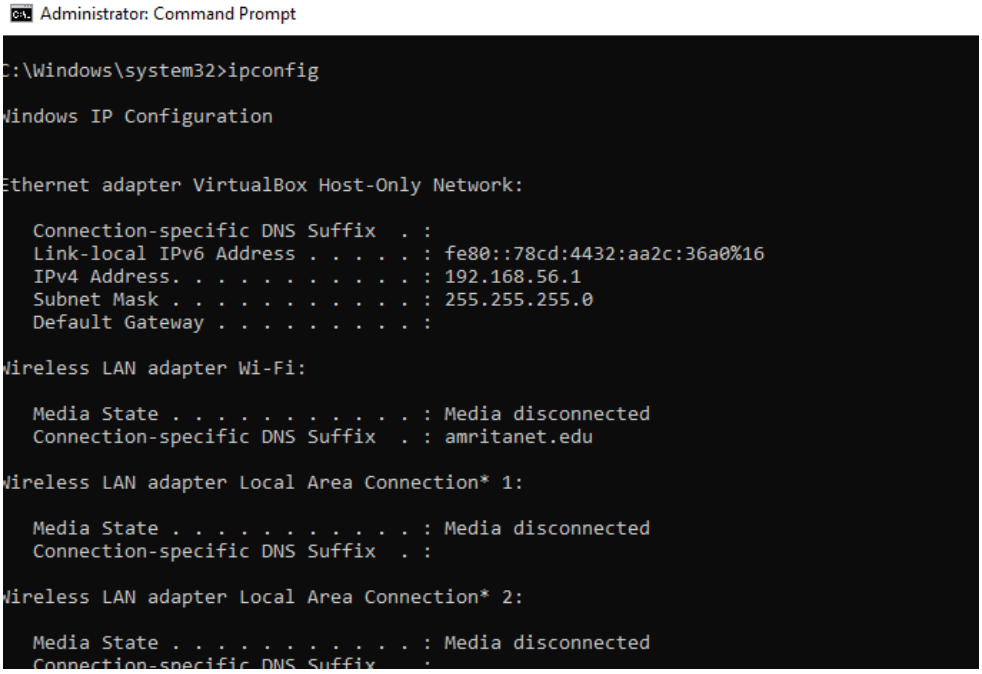
TOOLS REQUIRED

Window server and window10 VMs

Administrator privilege to run the tools

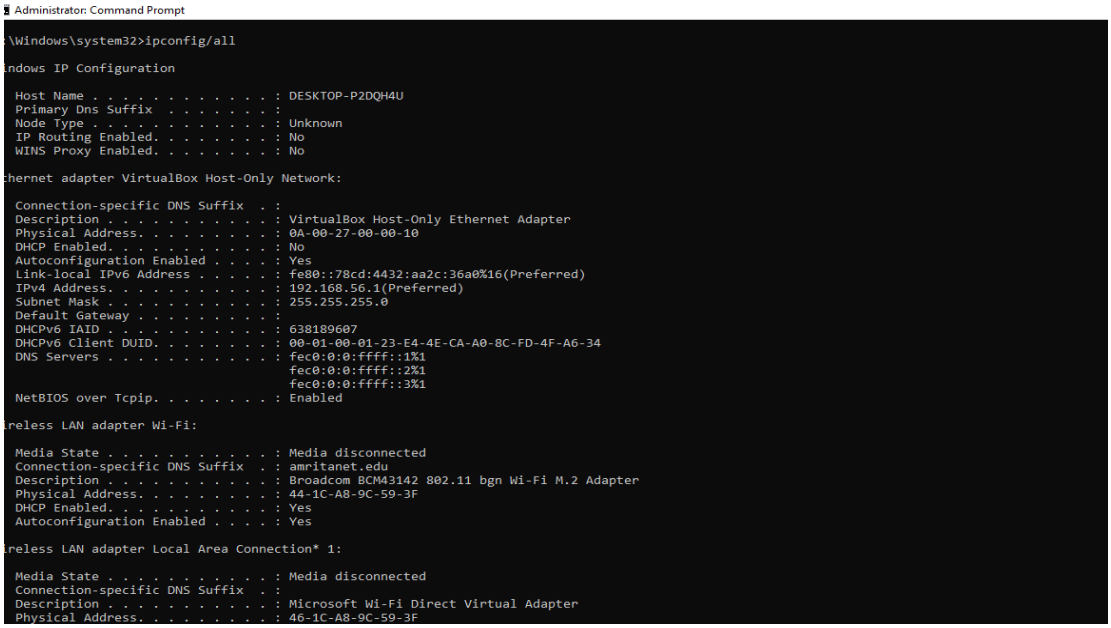
PROCEDURE

- Launch window server and login to the user name and password.
- Open the command prompt and run it as an admistrator.
- The command prompt appears on the screen and by typing all the comments the output are shown below as required.
- By typing the ipconfig in the command prompt,we can verify the ip configuration settings of the machine.

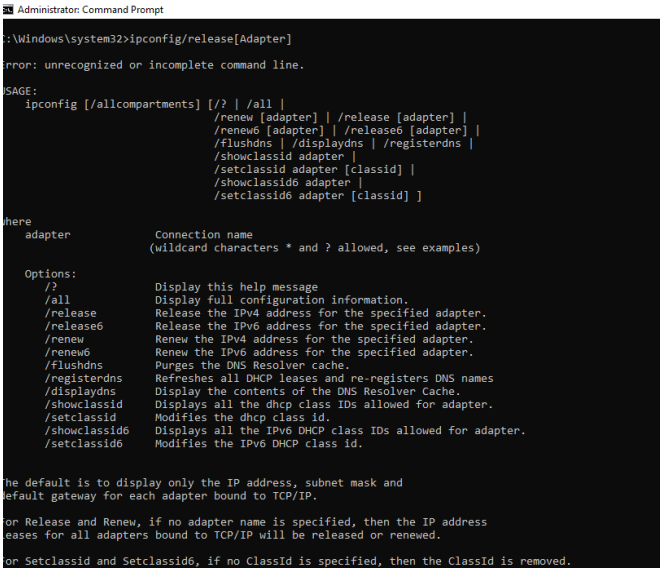


By using different ipconfig parameters to perform various network troubleshooting activities

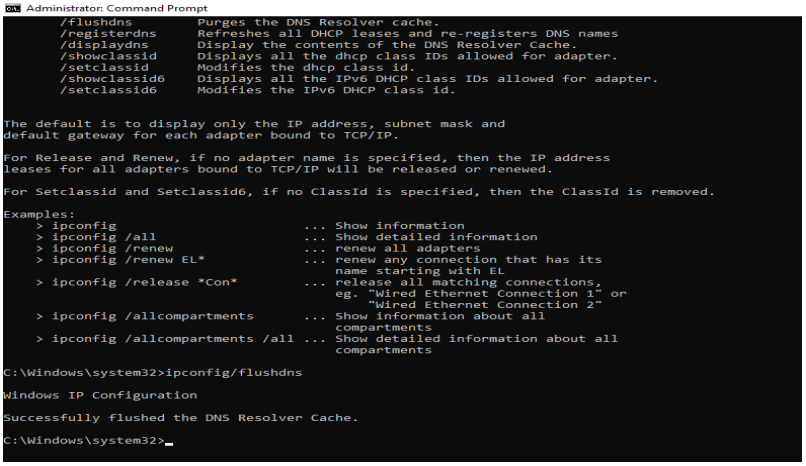
Ipconfig/all: It displays the full TCP/IP configuration for all adapters.



Ipconfig/release[adapter]: Here ,we must mention the of the IP specific address, but we entered it wrongly so the error is introduced.



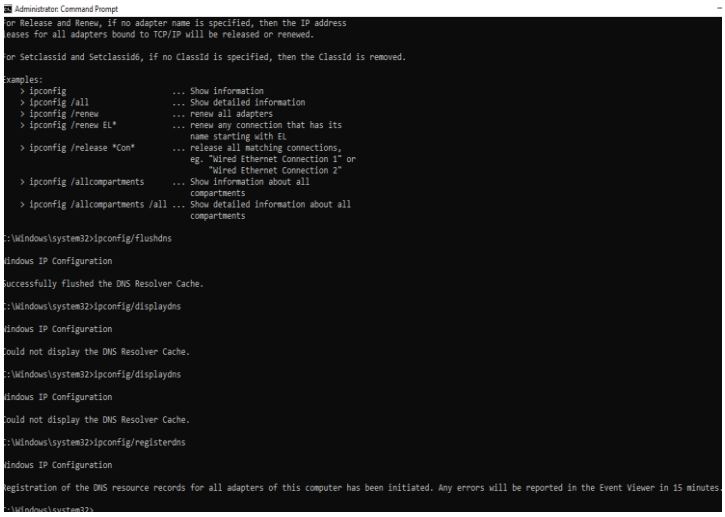
Ipconfig/flushdns: The DNS resolver cache is flushed.



Ipconfig/displaydns: Dns is not diplayed

```
C:\Windows\system32>ipconfig/flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Windows\system32>ipconfig/displaydns

Windows IP Configuration

Could not display the DNS Resolver Cache.

C:\Windows\system32>ipconfig/displaydns

Windows IP Configuration

Could not display the DNS Resolver Cache.

C:\Windows\system32>
```

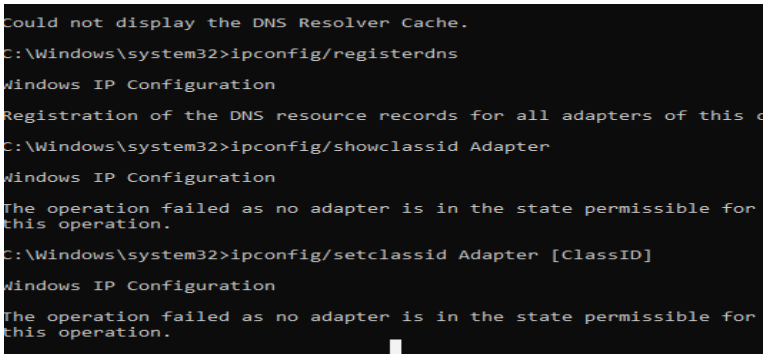
Ipconfig/registerdns: It creates or update the hostname in active directory. Here registration is updated.



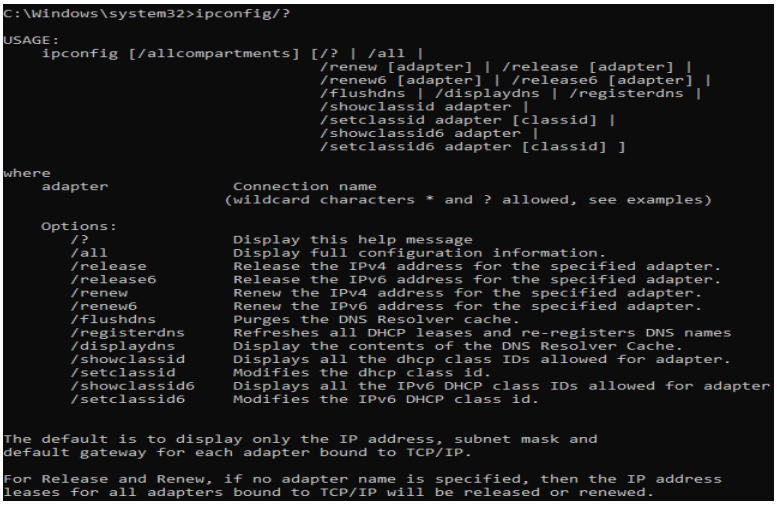
IPconfig/showclassid [Adapter]: To see the DHCP class id ,we must include (*) character in place of adapter. This parameter is available only on Computer with adapter that are configured to obtain IP adresss automatically.

```
Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Windows\system32>ipconfig/displaydns

Windows IP Configuration

Could not display the DNS Resolver Cache.

C:\Windows\system32>ipconfig/displaydns

Windows IP Configuration

Could not display the DNS Resolver Cache.

C:\Windows\system32>ipconfig/registerdns

Windows IP Configuration

Registration of the DNS resource records for all adapters of this computer has b

C:\Windows\system32>ipconfig/showclassid Adapter

Windows IP Configuration

The operation failed as no adapter is in the state permissible for
this operation.
```

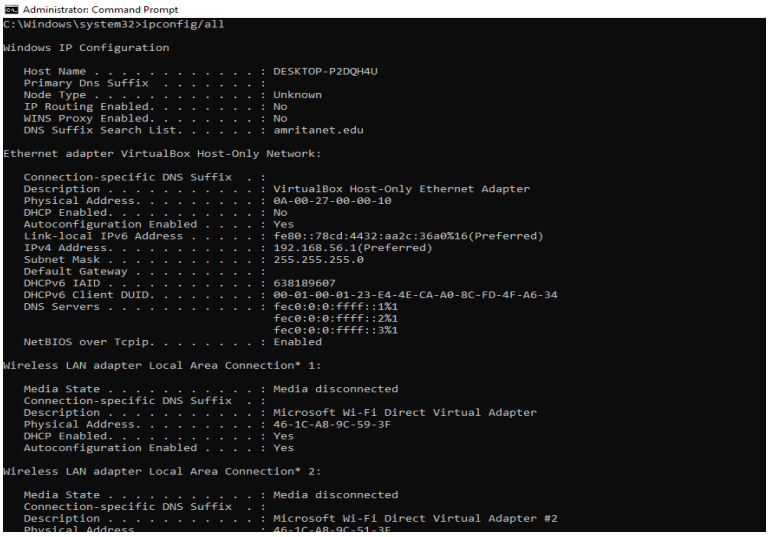
IPconfig/setclassid Adapter[classID]:The id is not specified as (*) wildcard character is not introduced here.so operation is failed here since no adapter is specified.



IPconfig/?: displays the help message of the above commands to avoid the mistakes in the syntax.



IPconfig/all: list all of your network adapters' configuration information.



Here the Ethernet is enabled and the ping command is entered, so the output

```
C:\Windows\system32>ping 10.11.136.170

Pinging 10.11.136.170 with 32 bytes of data:
Reply from 10.11.136.170: bytes=32 time<1ms TTL=128
Reply from 10.11.136.170: bytes=32 time<1ms TTL=128
Reply from 10.11.136.170: bytes=32 time<1ms TTL=128
Reply from 10.11.136.170: bytes=32 time<1ms TTL=128

Ping statistics for 10.11.136.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

The tracert command used to determine the route to a destination by sending ICMP packets to the destination, the output obtained is

```
C:\Windows\system32>ping 10.11.136.170

Pinging 10.11.136.170 with 32 bytes of data:
Reply from 10.11.136.170: bytes=32 time<1ms TTL=128
Reply from 10.11.136.170: bytes=32 time<1ms TTL=128
Reply from 10.11.136.170: bytes=32 time<1ms TTL=128
Reply from 10.11.136.170: bytes=32 time<1ms TTL=128

Ping statistics for 10.11.136.170:
    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>tracert 10.11.136.170

Tracing route to DESKTOP-P2DQH4U.amritanet.edu [10.11.136.170]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  DESKTOP-P2DQH4U.amritanet.edu [10.11.136.170]

Trace complete.
```

nslookup: It is used to query a DNS server to obtain a name and associated IP address.

```
Select Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>nslookup google.com
Server:  UnKnown
Address:  192.168.157.29

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4007:817::200e
          142.250.77.142


C:\Windows\system32>
```

To get the authoritative information ns command can be used with nslookup –type=soa google.com,the output obtained is,

```
Select Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>nslookup -type=soa google.com
Server:  UnKnown
Address:  192.168.157.29

Non-authoritative answer:
google.com
        primary name server = ns1.google.com
        responsible mail addr = dns-admin.google.com
        serial  = 478222697
        refresh = 900 (15 mins)
        retry   = 900 (15 mins)
        expire  = 1800 (30 mins)
        default TTL = 60 (1 min)
```

After using the netstat command, we can obtain network statistics as the output obtained below,

```
C:\Windows\system32>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    10.11.136.170:49710    sf-in-f188:https       ESTABLISHED
  TCP    10.11.136.170:49728    20.198.119.84:https    ESTABLISHED
  TCP    10.11.136.170:50076    147:https              ESTABLISHED
  TCP    10.11.136.170:50094    bom12s20-in-f14:https  TIME_WAIT
  TCP    10.11.136.170:50105    bom12s03-in-f22:https  TIME_WAIT
  TCP    10.11.136.170:50107    49.44.142.242:https    ESTABLISHED
  TCP    10.11.136.170:50114    maa03s46-in-f1:https   TIME_WAIT
  TCP    10.11.136.170:50116    maa03s46-in-f2:https   TIME_WAIT
  TCP    10.11.136.170:50129    bom07s29-in-f4:https   TIME_WAIT
  TCP    10.11.136.170:50133    maa05s10-in-f14:https  FIN_WAIT_1
  TCP    10.11.136.170:50137    del11s08-in-f14:https  ESTABLISHED
```

The parameters of netstat gives the output as follows:

netstat -a :displays all TCP connection and TCP and UDP Port on which computer is listening.

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

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            DESKTOP-P2DQH4U:0      LISTENING
  TCP    0.0.0.0:445            DESKTOP-P2DQH4U:0      LISTENING
  TCP    0.0.0.0:5040           DESKTOP-P2DQH4U:0      LISTENING
  TCP    0.0.0.0:7680           DESKTOP-P2DQH4U:0      LISTENING
  TCP    0.0.0.0:49664          DESKTOP-P2DQH4U:0      LISTENING
  TCP    0.0.0.0:49665          DESKTOP-P2DQH4U:0      LISTENING
  TCP    0.0.0.0:49666          DESKTOP-P2DQH4U:0      LISTENING
  TCP    0.0.0.0:49667          DESKTOP-P2DQH4U:0      LISTENING
  TCP    0.0.0.0:49668          DESKTOP-P2DQH4U:0      LISTENING
  TCP    0.0.0.0:49669          DESKTOP-P2DQH4U:0      LISTENING
  TCP    192.168.56.1:139       DESKTOP-P2DQH4U:0      LISTENING
  TCP    192.168.157.60:139     DESKTOP-P2DQH4U:0      LISTENING
  TCP    192.168.157.60:59470   20.198.119.84:https    ESTABLISHED
  TCP    192.168.157.60:63804   server-108-158-251-37:https  ESTABLISHED
  TCP    192.168.157.60:63856   server-108-158-251-117:https  ESTABLISHED
```

netstat –e: displays Ethernet statistics.

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

                           Received            Sent

Bytes                    1396400656        79989427
Unicast packets             1112468          637287
Non-unicast packets              42            2296
Discards                          0               0
Errors                            0               0
Unknown protocols                 0
```

netstat -n: displays TCP connection but address and port number is expressed numerically.

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

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.157.60:59470   20.198.119.84:443      ESTABLISHED
  TCP    192.168.157.60:64141   49.44.144.50:443       CLOSE_WAIT
  TCP    192.168.157.60:64406   142.250.182.74:443     ESTABLISHED
  TCP    192.168.157.60:64415   108.158.251.110:443    ESTABLISHED
  TCP    192.168.157.60:64425   142.250.195.67:443     ESTABLISHED
  TCP    192.168.157.60:64426   142.250.195.67:443     TIME_WAIT
  TCP    192.168.157.60:64430   165.227.168.243:443    ESTABLISHED
  TCP    192.168.157.60:64435   13.235.249.196:443     ESTABLISHED
  TCP    192.168.157.60:64440   108.158.251.106:443    ESTABLISHED
  TCP    192.168.157.60:64442   108.158.251.117:443    ESTABLISHED
  TCP    192.168.157.60:64444   216.58.196.163:443     ESTABLISHED
  TCP    192.168.157.60:64445   13.235.249.196:443     ESTABLISHED
  TCP    [2409:4073:6:3667:6c3f:bf03:97fb:e737]:59509  [2404:6800:4003:c05::bc]:443  ESTABLISHED
  TCP    [2409:4073:6:3667:6c3f:bf03:97fb:e737]:64418  [2404:6800:4007:81e::2003]:443  TIME_WAIT
  TCP    [2409:4073:6:3667:6c3f:bf03:97fb:e737]:64420  [2404:6800:4007:817::200a]:443  ESTABLISHED
  TCP    [2409:4073:6:3667:6c3f:bf03:97fb:e737]:64427  [2404:6800:4007:81f::2003]:443  TIME_WAIT
  TCP    [2409:4073:6:3667:6c3f:bf03:97fb:e737]:64429  [2404:6800:4007:81e::2003]:443  ESTABLISHED
  TCP    [2409:4073:6:3667:6c3f:bf03:97fb:e737]:64434  [2600:9000:2354:1e00:1d:1c40:1bc0:93a1]:443  ESTABLISHED
```

netstat -o: displays active TCP connections and include the processID for each connection

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

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    192.168.157.60:59470   20.198.119.84:https    ESTABLISHED     4056
  TCP    192.168.157.60:64141   49.44.144.50:https     CLOSE_WAIT      6332
  TCP    192.168.157.60:64406   maa05s20-in-f10:https  ESTABLISHED     6880
  TCP    192.168.157.60:64415   server-108-158-251-110:https  ESTABLISHED     6880
  TCP    192.168.157.60:64425   maa03s38-in-f3:https   ESTABLISHED     6880
  TCP    192.168.157.60:64430   165.227.168.243:https  TIME_WAIT       0
  TCP    192.168.157.60:64454   165.227.168.243:https  TIME_WAIT       0
```

netstat -p: it shows connections of protocol.

```
C:\Windows\system32>netstat -p

Active Connections

  Proto  Local Address          Foreign Address        State

C:\Windows\system32>netstat -p

Active Connections

  Proto  Local Address          Foreign Address        State
```

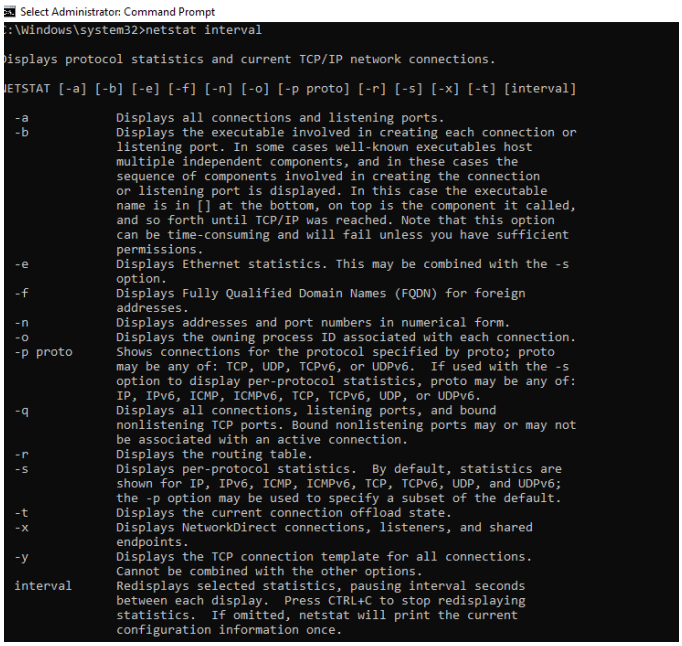
netstat -s: displays statistics by protocol.

```
Administrator: Command Prompt

:\Windows\system32>netstat -s

Pv4 Statistics

  Packets Received                   = 428118
  Received Header Errors             = 0
  Received Address Errors            = 0
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 1
  Received Packets Discarded         = 1405
  Received Packets Delivered         = 429074
  Output Requests                    = 228317
  Routing Discards                   = 0
  Discarded Output Packets           = 74
  Output Packet No Route             = 15
  Reassembly Required                = 0
  Reassembly Successful              = 0
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 0
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 0

Pv6 Statistics

  Packets Received                   = 111810
  Received Header Errors             = 0
  Received Address Errors            = 0
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 0
  Received Packets Discarded         = 888
```

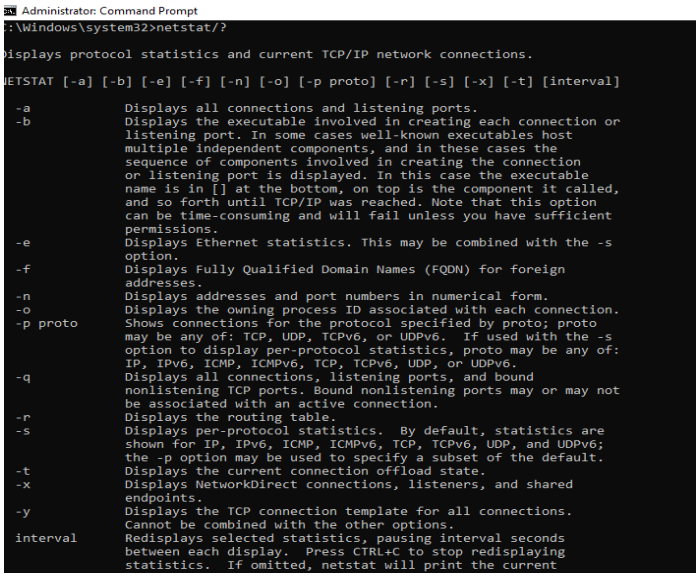
netstat -r: displays the content of IP routing table.

```
Select Administrator: Command Prompt
:\Windows\system32>netstat -r
===========================================================================
nterface List
20...a0 8c fd 4f a6 34 ......Realtek PCIe FE Family Controller
16...0a 00 27 00 00 10 ......VirtualBox Host-Only Ethernet Adapter
 6...46 1c a8 9c 59 3f ......Microsoft Wi-Fi Direct Virtual Adapter
14...46 1c a8 9c 51 3f ......Microsoft Wi-Fi Direct Virtual Adapter #2
 7...44 1c a8 9c 59 3f ......Broadcom BCM43142 802.11 bgn Wi-Fi M.2 Adapter
 1...........................Software Loopback Interface 1
===========================================================================

Pv4 Route Table
===========================================================================
ctive Routes:
etwork Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0   192.168.157.29   192.168.157.60     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
      192.168.56.0    255.255.255.0         On-link       192.168.56.1    281
      192.168.56.1  255.255.255.255         On-link       192.168.56.1    281
    192.168.56.255  255.255.255.255         On-link       192.168.56.1    281
     192.168.157.0    255.255.255.0         On-link     192.168.157.60    311
    192.168.157.60  255.255.255.255         On-link     192.168.157.60    311
   192.168.157.255  255.255.255.255         On-link     192.168.157.60    311
        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       192.168.56.1    281
        224.0.0.0        240.0.0.0         On-link     192.168.157.60    311
  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       192.168.56.1    281
  255.255.255.255  255.255.255.255         On-link     192.168.157.60    311
===========================================================================
ersistent Routes:
 None

Pv6 Route Table
===========================================================================
ctive Routes:
If Metric Network Destination      Gateway
 7     71 ::/0                     fe80::6c86:76ff:fe0f:da7e
 1    331 ::1/128                  On-link
 7     71 2409:4073:219e:9b90::/64 On-link
 7    311 2409:4073:219e:9b90:d74:f92a:b025:b01c/128
                                   On-link
```

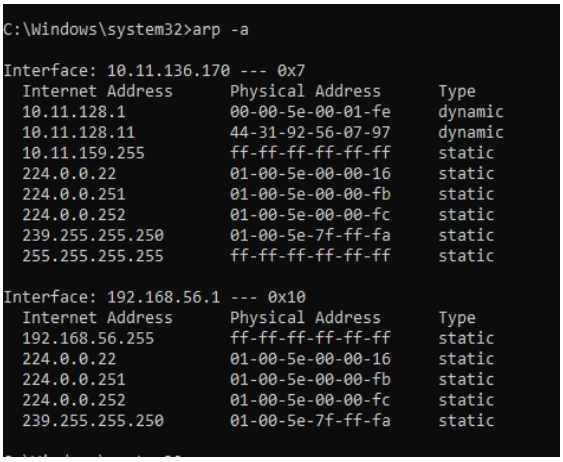
netstat interval: redisplays the selected information every internal seconds.



netstat /?: displays help at the command prompt.



The arp –a command displays ARP cache ,it has mapping of IP address with respective of MAC address.



The commands for network administration and trouble shooting are listed below

Gpresult: starts the operating system group policy result tool.

```
C:\Windows\system32>Gpresult

GPRESULT [/S system [/U username [/P [password]]]] [/SCOPE scope]
         [/USER targetusername] [/R | /V | /Z] [(/X | /H) <filename> [/F]]

Description:
    This command line tool displays the Resultant Set of Policy (RSoP)
    information for a target user and computer.

Parameter List:
    /S        system          Specifies the remote system to connect to.

    /U        [domain\]user   Specifies the user context under which the
                              command should run.
                              Can not be used with /X, /H.

    /P        [password]      Specifies the password for the given user
                              context. Prompts for input if omitted.
                              Cannot be used with /X, /H.

    /SCOPE    scope           Specifies whether the user or the
                              computer settings need to be displayed.
                              Valid values: "USER", "COMPUTER".

    /USER     [domain\]user   Specifies the user name for which the
                              RSoP data is to be displayed.

    /X        <filename>      Saves the report in XML format at the
                              location and with the file name specified
                              by the <filename> parameter. (valid in Windows
                              Vista SP1 and later and Windows Server 2008 and later)

    /H        <filename>      Saves the report in HTML format at the
                              location and with the file name specified by
                              the <filename> parameter. (valid in Windows
                              at least Vista SP1 and at least Windows Server 2008)

    /F                        Forces Gpresult to overwrite the file name
                              specified in the /X or /H command.

    /R                        Displays RSoP summary data.
```

nbtstat –a<machine name>: obtains info from WINS or LMHOST.

```
C:\Windows\system32>nbtstat -aDESKTOP-P2DQH4U

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
```

nbtstat –A<IP>: discovers who is logged on ,gets info from WINS or LMHOST.

```
C:\Windows\system32>nbtstat -A192.168.157.60

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
```

nbtstat –R: purges and preload 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
    ---------------------------------------------
    DESKTOP-P2DQH4U<20>  UNIQUE      Registered
    DESKTOP-P2DQH4U<00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered

Wi-Fi:
Node IpAddress: [192.168.157.60] Scope Id: []

               NetBIOS Local Name Table

      Name               Type         Status
    ---------------------------------------------
    DESKTOP-P2DQH4U<20>  UNIQUE      Registered
    DESKTOP-P2DQH4U<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* 2:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache
```

nbstat -r: useful for detecting errors, when browsing NETBIOS.

```
C:\Windows\system32>nbtstat -r

    NetBIOS Names Resolution and Registration Statistics
    ----------------------------------------------------

    Resolved By Broadcast     = 0
    Resolved By Name Server   = 0

    Registered By Broadcast   = 24
    Registered By Name Server = 0
```

netstat –an: shows open ports.

```
:\Windows\system32>netstat -an

ctive Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING
  TCP    192.168.56.1:139       0.0.0.0:0              LISTENING
  TCP    192.168.157.60:139     0.0.0.0:0              LISTENING
  TCP    192.168.157.60:50429   20.198.119.84:443      ESTABLISHED
  TCP    [::]:135               [::]:0                 LISTENING
  TCP    [::]:445               [::]:0                 LISTENING
  TCP    [::]:5357              [::]:0                 LISTENING
  TCP    [::]:49664             [::]:0                 LISTENING
  TCP    [::]:49665             [::]:0                 LISTENING
  TCP    [::]:49666             [::]:0                 LISTENING
  TCP    [::]:49667             [::]:0                 LISTENING
  TCP    [::]:49668             [::]:0                 LISTENING
  TCP    [::]:49669             [::]:0                 LISTENING
  TCP    [2409:4073:206:d5fd:71e4:7d86:6ed0:f72e]:50384  [2606:2800:147:120f:30c:1ba0:fc6:265a]:443  CLOSE_WAIT
  TCP    [2409:4073:206:d5fd:71e4:7d86:6ed0:f72e]:50435  [2404:6800:4003:c0f::bc]:5228  ESTABLISHED
  TCP    [2409:4073:206:d5fd:71e4:7d86:6ed0:f72e]:50451  [2404:6800:4007:81c::2005]:443  ESTABLISHED
  TCP    [2409:4073:206:d5fd:71e4:7d86:6ed0:f72e]:50465  [2404:6800:4007:81e::200e]:443  ESTABLISHED
  TCP    [2409:4073:206:d5fd:71e4:7d86:6ed0:f72e]:50471  [2404:6800:4007:808::2003]:443  ESTABLISHED
  TCP    [2409:4073:206:d5fd:71e4:7d86:6ed0:f72e]:50472  [2404:6800:4007:819::2004]:443  ESTABLISHED
  TCP    [2409:4073:206:d5fd:71e4:7d86:6ed0:f72e]:50474  [2404:6800:4007:824::200e]:443  ESTABLISHED
  UDP    0.0.0.0:3600           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:5050           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
```

netstat –ab: b switch links each used port with its application.

```
C:\Windows\system32>netstat -ab

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            DESKTOP-P2DQH4U:0      LISTENING
  RpcSs
 [svchost.exe]
  TCP    0.0.0.0:445            DESKTOP-P2DQH4U:0      LISTENING
 Can not obtain ownership information
  TCP    0.0.0.0:5040           DESKTOP-P2DQH4U:0      LISTENING
  CDPSvc
 [svchost.exe]
  TCP    0.0.0.0:5357           DESKTOP-P2DQH4U:0      LISTENING
 Can not obtain ownership information
  TCP    0.0.0.0:49664          DESKTOP-P2DQH4U:0      LISTENING
 Can not obtain ownership information
  TCP    0.0.0.0:49665          DESKTOP-P2DQH4U:0      LISTENING
  Schedule
 [svchost.exe]
  TCP    0.0.0.0:49666          DESKTOP-P2DQH4U:0      LISTENING
  EventLog
 [svchost.exe]
  TCP    0.0.0.0:49667          DESKTOP-P2DQH4U:0      LISTENING
 [spoolsv.exe]
  TCP    0.0.0.0:49668          DESKTOP-P2DQH4U:0      LISTENING
 Can not obtain ownership information
  TCP    0.0.0.0:49669          DESKTOP-P2DQH4U:0      LISTENING
 [lsass.exe]
  TCP    192.168.56.1:139       DESKTOP-P2DQH4U:0      LISTENING
 Can not obtain ownership information
  TCP    192.168.157.60:139     DESKTOP-P2DQH4U:0      LISTENING
 Can not obtain ownership information
  TCP    192.168.157.60:50429   20.198.119.84:https    ESTABLISHED
  WpnService
 [svchost.exe]
  TCP    [::]:135               DESKTOP-P2DQH4U:0      LISTENING
  RpcSs
 [svchost.exe]
  TCP    [::]:445               DESKTOP-P2DQH4U:0      LISTENING
```

netstat –an 1 |find “15868”: locates only lines with number15868 and redisplays every one second.

```
C:\Windows\system32>netstat -an1 | find "15868"

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-x] [-t] [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.
  -n            Displays addresses and port numbers in numerical form.
  -o            Displays the owning process ID associated with each connection.
  -p proto      Shows connections for the protocol specified by proto; proto
                may be any of: TCP, UDP, TCPv6, or UDPv6.  If used with the -s
                option to display per-protocol statistics, proto may be any of:
                IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
  -q            Displays all connections, listening ports, and bound
                nonlistening TCP ports. Bound nonlistening ports may or may not
                be associated with an active connection.
  -r            Displays the routing table.
  -s            Displays per-protocol statistics.  By default, statistics are
                shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6;
                the -p option may be used to specify a subset of the default.
  -t            Displays the current connection offload state.
  -x            Displays NetworkDirect connections, listeners, and shared
                endpoints.
  -y            Displays the TCP connection template for all connections.
                Cannot be combined with the other options.
  interval      Redisplays selected statistics, pausing interval seconds
                between each display.  Press CTRL+C to stop redisplaying
                statistics.  If omitted, netstat will print the current
```

netsat –an |find “LISTENING : shows open ports with LISTENING status.

netsat –an |find “LISTENING

```
C:\Windows\system32>netstat -an | find "LISTENING"
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING
  TCP    192.168.56.1:139       0.0.0.0:0              LISTENING
  TCP    192.168.157.60:139     0.0.0.0:0              LISTENING
  TCP    [::]:135               [::]:0                 LISTENING
  TCP    [::]:445               [::]:0                 LISTENING
  TCP    [::]:5357              [::]:0                 LISTENING
  TCP    [::]:49664             [::]:0                 LISTENING
  TCP    [::]:49665             [::]:0                 LISTENING
  TCP    [::]:49666             [::]:0                 LISTENING
  TCP    [::]:49667             [::]:0                 LISTENING
  TCP    [::]:49668             [::]:0                 LISTENING
  TCP    [::]:49669             [::]:0                 LISTENING
```

net use: retrieves a list of network connections.

```
C:\Windows\system32>net use
New connections will be remembered.

There are no entries in the list.
```

net user: shows user account for the computer.

```
C:\Windows\system32>net user

User accounts for \\DESKTOP-P2DQH4U

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

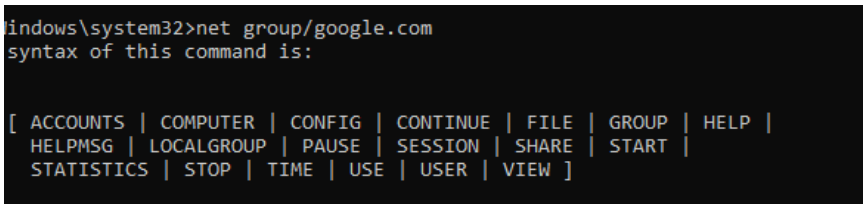
net user/domain:Displays user account for the domain.

```
C:\Windows\system32>net user/google.com
The syntax of this command is:

NET
    [ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
      HELPMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
      STATISTICS | STOP | TIME | USE | USER | VIEW ]

C:\Windows\system32>net user/google.com
The syntax of this command is:

NET
    [ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
      HELPMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
```

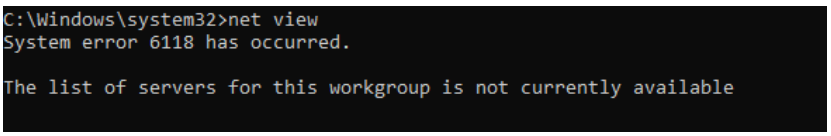
net user/domain<user name>: shows account details for specific user.

```
C:\Windows\system32>net user/google.com<karthika>
The syntax of the command is incorrect.
```

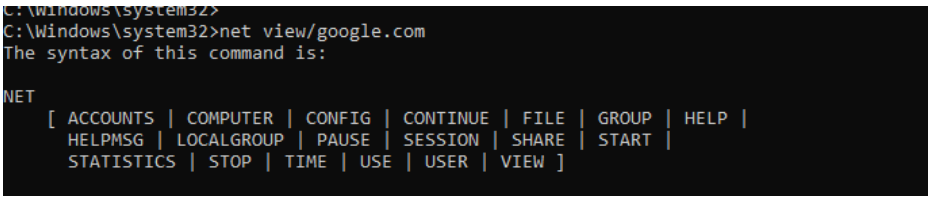
net group/domain: shows group account for domain.



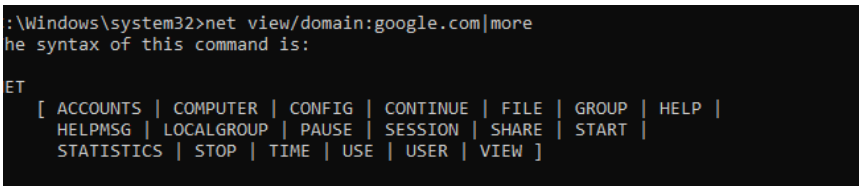
net view: since it is in workgroup,the system error has occurred.



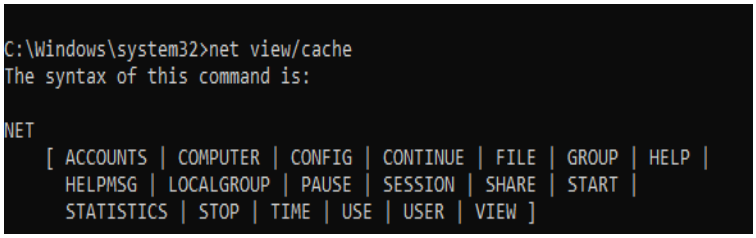
net view/domain:specifies computer available in a specific domain.



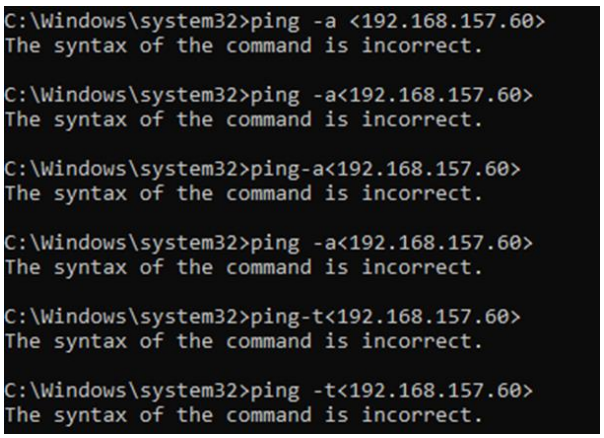
net view/domain:<domain name>|more:shows user account from specific domain.



net view/cache: shows the workstation names.



ping –a<ip> and ping –t<ip>:Ping –a resolves ip to hostname and ping-t pings host until stopped.



Pathping:It displays the route information when performing queries.it represents hostnames and maximum hops.

```
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.

C:\Windows\system32>set U
USERDOMAIN=DESKTOP-P2DQH4U
USERDOMAIN_ROAMINGPROFILE=DESKTOP-P2DQH4U
USERNAME=user
USERPROFILE=C:\Users\user
```

Set U:shows which user is logged on.

```
C:\Windows\system32>set U
USERDOMAIN=DESKTOP-P2DQH4U
USERDOMAIN_ROAMINGPROFILE=DESKTOP-P2DQH4U
USERNAME=user
USERPROFILE=C:\Users\user
```

Set L: shows the logon server.

```
C:\Windows\system32>set L
LOCALAPPDATA=C:\Users\user\AppData\Local
LOGONSERVER=\\DESKTOP-P2DQH4U
```

RESULT:

Thus, the results of various windows commands are obtained by performing the operation.