INTERNET PROTOCOL LAB ASSIGNEMNET -1

Name: **Siriparapu Sparshika**

Roll No: **CYS22006**

Date: **28-08-2022**

BASIC NETWORK ADMINISTRATION AND TROUBLESHOOTING USING WINDOWS COMMAND UTILITIES.

AIM:

To perform troubleshooting in the network using basic Windows command-line utilities

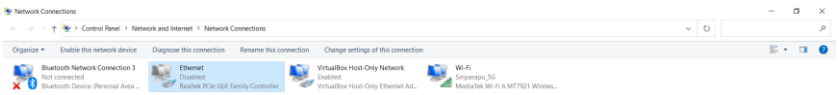
TOOLS REQUIRED:

- Windows Server 2012 and Windows 10VMs
- Administrator privileges to run the tools

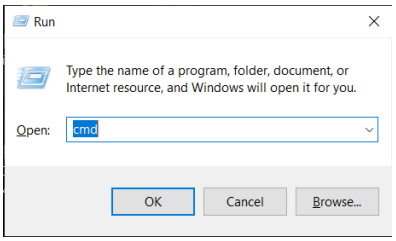
PROCEDURE:

- Login to Windows 10 VM and disable the network adapter:

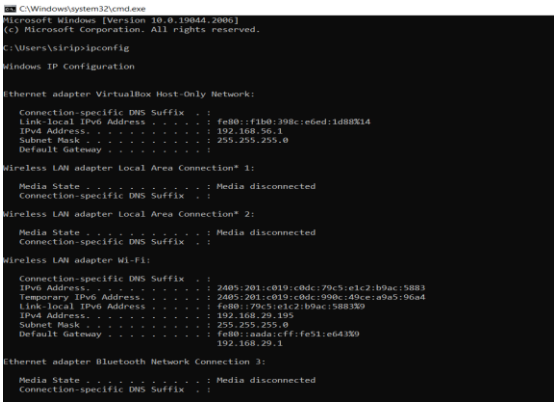
  Go to Control Panel then to Network and Internet then to Network and Sharing Center, and click Change adapter settings. Disable the network adapter before performing the tasks



- Next Open command prompt from Start button or Win + R and enter cmd.

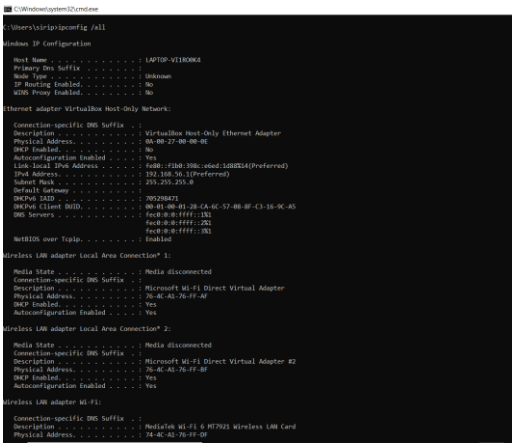


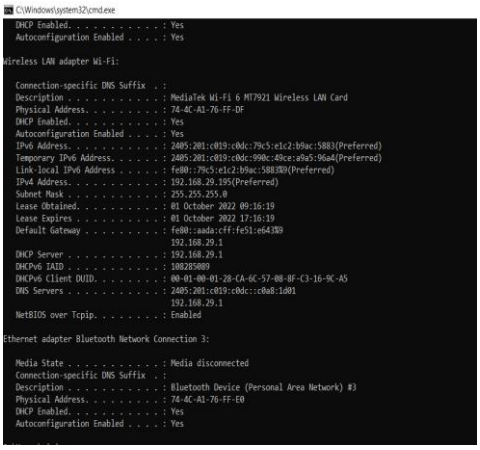
- In command prompt, enter ipconfig and click Enter. This will show the IP configurations of the system that's been connected to the same network.



- **ipconfig /all Command**

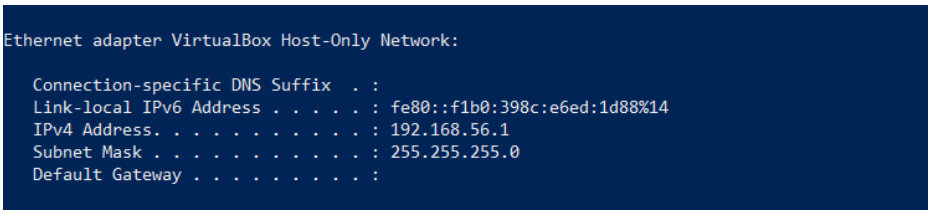
  Displays the entire network information for all the adapters.





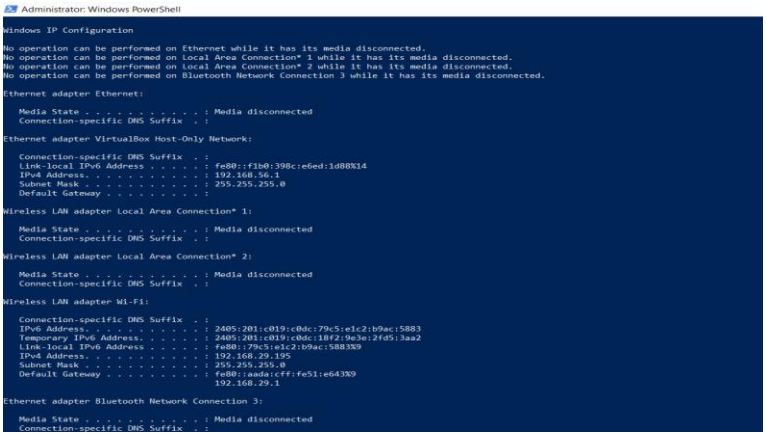
- **ipconfig /release Command**

  The command will release the IP Addresses for all network adapters and also specify a single network adapter.



- **ipconfig /renew Command**

The command request a new Ip from DHCP where we get same output as ipconfig cmd but new Ip address, subnet, mask and gateway.

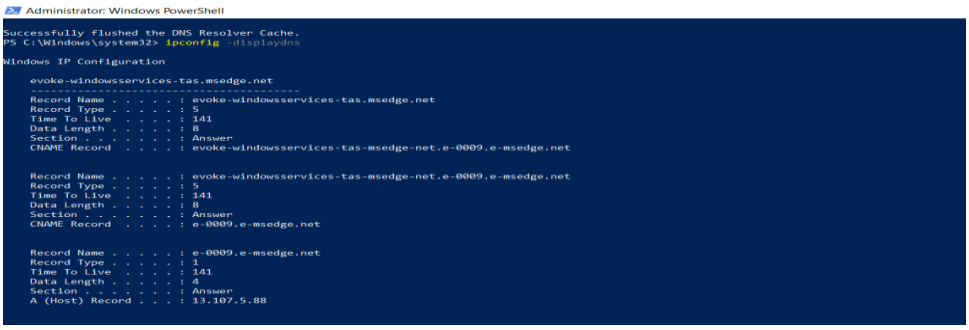


- **ipconfig /flushdns Command**

flushdns clears out DNS cache, simply request new and update dns record from dns servers.

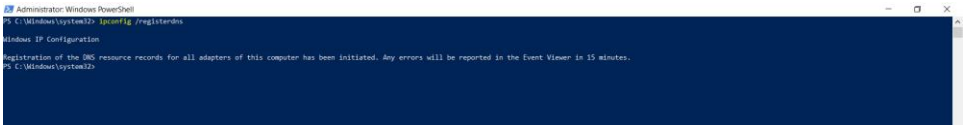
- **ipconfig /displaydns Command**

Local cache of all DNS records which is visited used to quickly translate the domain names to the correct Ip address



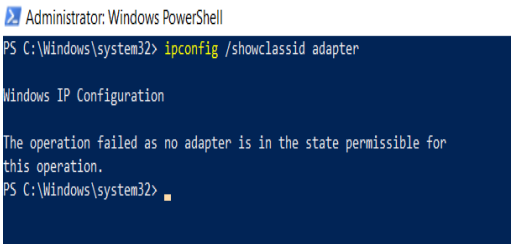
- **ipconfig /registerdns Command**

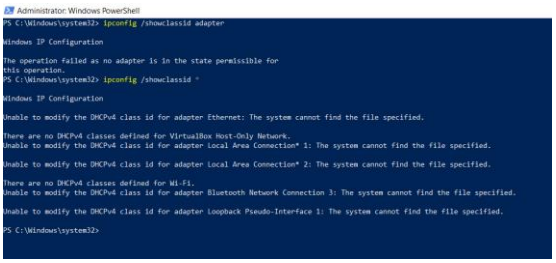
-We need to manually initiate dynamic DNS registration and refresh DHCP releases, and also use it for troubleshooting DNS name registration issues without rebooting the system



- **ipconfig /showclassid adapter Command**

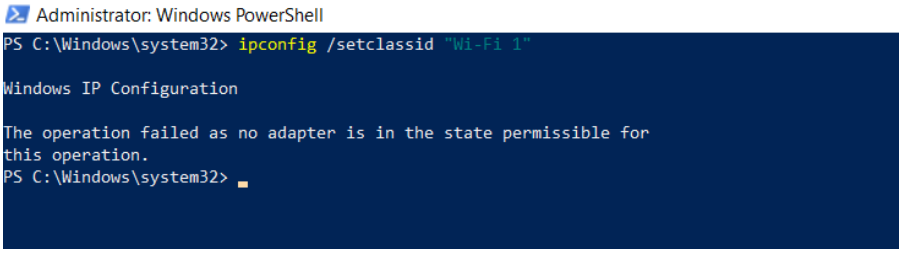
-Display DHCP (Dynamic Host Configuration Protocol) class ID for a specified Adapter





- **ipconfig /setclassid adapter [ClassID] Command**

-Configure DHCP class ID for a specified adapter, if DHCP is not specified then class ID is removed.



- **Ipconfig /? Command**

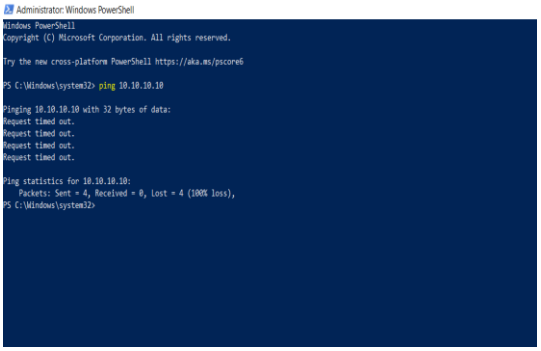
Help

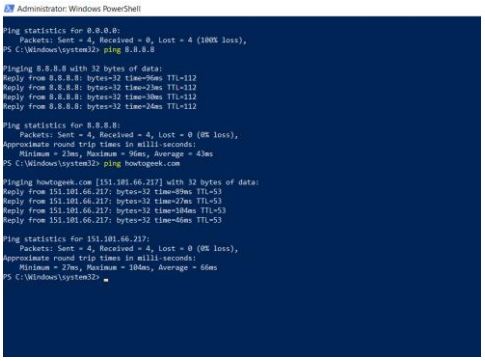
```
C:\Windows\system32\cmd.exe
C:\Users\siripsipconfig /?

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.


The default is to display only the IP address, subnet mask and
default gateway for each adapter bound to TCP/IP.

For Release and Renew, if no adapter name is specified, then the IP address
leases for all adapters bound to TCP/IP will be released or renewed.

For Setclassid and Setclassid6, if no ClassId is specified, then the ClassId is removed.

Examples:
    > ipconfig                       ... Show information
    > ipconfig /all                  ... Show detailed information
    > ipconfig /renew                ... renew all adapters
    > ipconfig /renew EL*            ... renew any connection that has its
                                         name starting with EL
    > ipconfig /release *Con*        ... release all matching connections,
                                         eg. "Wired Ethernet Connection 1" or
                                             "Wired Ethernet Connection 2"
    > ipconfig /allcompartments      ... Show information about all
                                         compartments
    > ipconfig /allcompartments /all ... Show detailed information about all
```

>>PING COMMANDS: (Packet Internet Groper)

-Used to check if a network device is reachable or not, sends request over the network in response from computer that was pinged back to the original computer.

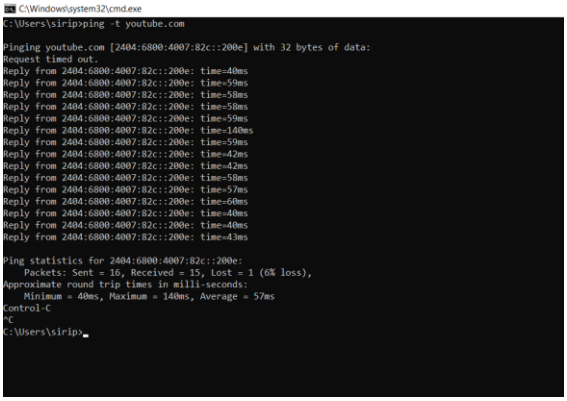
-sends and echo request and gets an echo reply





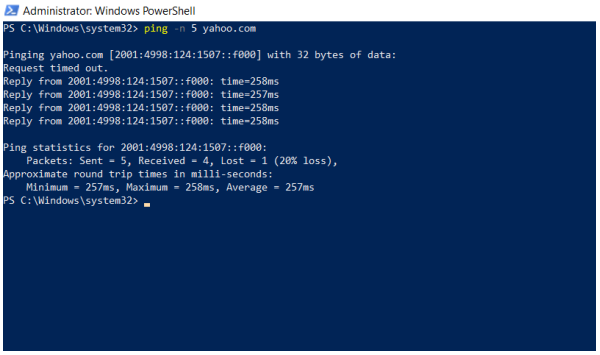
- ping –t

-Pings the specified host until stopped by using ctrl+c



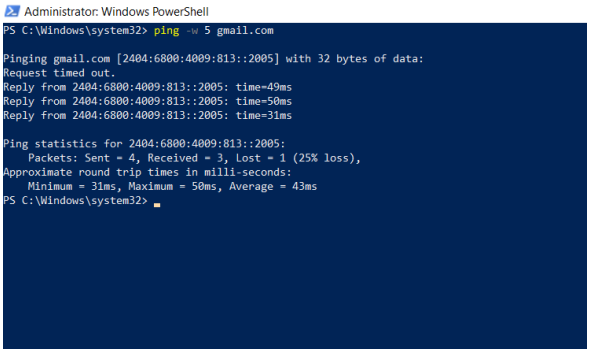
- ping -n:

Determines number of ICMP echo request to send from 1 to 4294967295



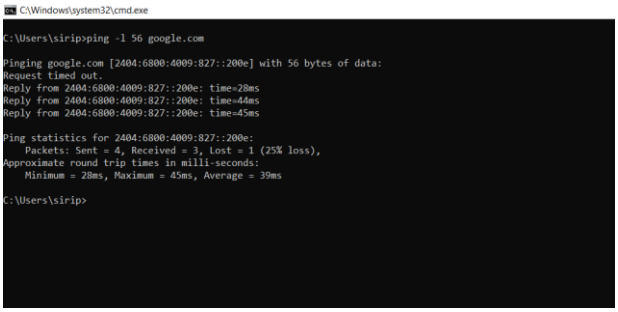
- ping -w

Command used to check Timeout in milliseconds to wait for each reply.



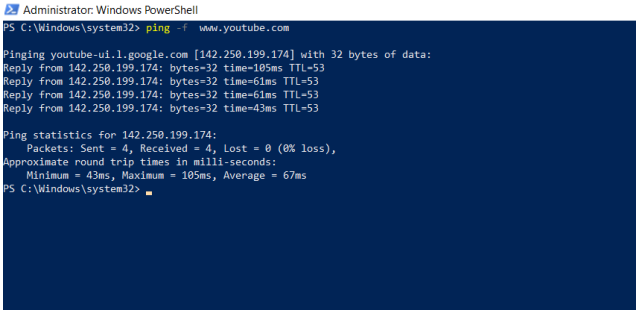
- ping -l

Command is used to set the size in the bytes of echo request packet from 32 to 65,529



- Ping -f

Command used to prevent ICMP echo requests from being fragmented by routers between our system and the target, often used to troubleshoot path maximum transmission unit (PMTU) issues.

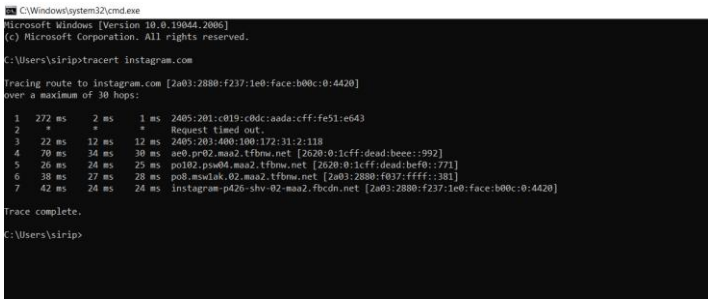


>> Tracert

-Tool that determines the route to destination by sending ICMP packets to the destination.

-Entry or a hoop is a location that the packet passes through to reach its final destination

- It shows a different way to reach a particular destination



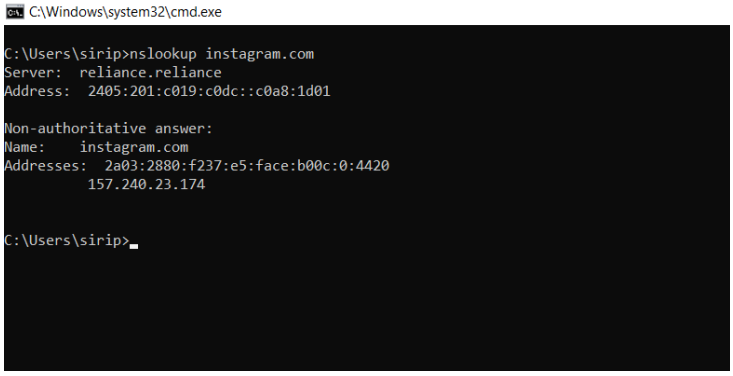
```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19044.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\sirip>tracert instagram.com

Tracing route to instagram.com [2a03:2880:f237:1e0:face:b00c:0:4420]
over a maximum of 30 hops:

  1   272 ms     2 ms     1 ms  2405:201:c019:c0dc:aada:cff:fe51:e643
  2     *        *        *    Request timed out.
  3    22 ms    12 ms    12 ms  2405:203:400:100:172:31:2:118
  4    70 ms    34 ms    30 ms  ae0.pr02.maa2.tfbnw.net [2620:0:1cff:dead:beee::992]
  5    26 ms    24 ms    25 ms  po102.psw04.maa2.tfbnw.net [2620:0:1cff:dead:bef0::771]
  6    38 ms    27 ms    28 ms  po8.msw1ak.02.maa2.tfbnw.net [2a03:2880:f037:ffff::381]
  7    42 ms    24 ms    24 ms  instagram-p426-shv-02-maa2.fbcdn.net [2a03:2880:f237:1e0:face:b00c:0:4420]

Trace complete.

C:\Users\sirip>
```

- **nslookup**

-Used for getting information from the DNS Server.

-network admin tool for querying the DNS to obtain domain name or Ip address mapping or any other specified DNS record

-Also, we can do reverse lookup, that is by giving the Ip address and then finding domain



```
C:\Windows\system32\cmd.exe

C:\Users\sirip>nslookup instagram.com
Server:  reliance.reliance
Address:  2405:201:c019:c0dc::c0a8:1d01

Non-authoritative answer:
Name:    instagram.com
Addresses:  2a03:2880:f237:e5:face:b00c:0:4420
          157.240.23.174


C:\Users\sirip>_
```

- **nslookup -type=a any option**

View all available DNS records for a particular record

```
[10/02/22]seed@VM:~$ nslookup -type=a redhat.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   redhat.com
Address: 34.235.198.240
Name:   redhat.com
Address: 52.200.142.250

[10/02/22]seed@VM:~$
```

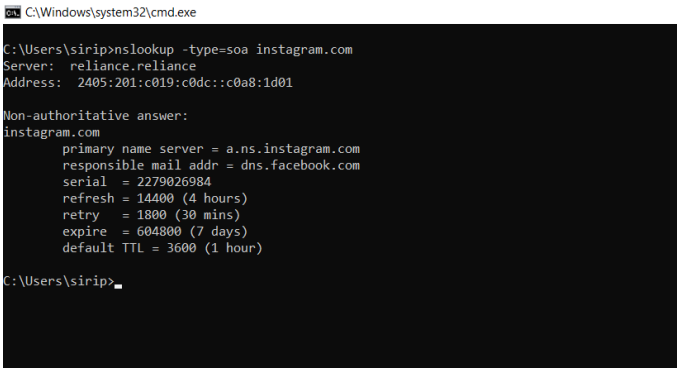
- **nslookup -type=any option**

Lookup for any record, available DNS records

```
[10/02/22]seed@VM:~$ nslookup -type=any google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.192.46
Name:   google.com
Address: 2404:6800:4007:813::200e
google.com
        origin = ns1.google.com
        mail addr = dns-admin.google.com
        serial = 478222697
        refresh = 900
        retry = 900
        expire = 1800
        minimum = 60
google.com      nameserver = ns4.google.com.
google.com      nameserver = ns1.google.com.
google.com      nameserver = ns2.google.com.
google.com      nameserver = ns3.google.com.

Authoritative answers can be found from:
```

- **nslookup –type=soa**

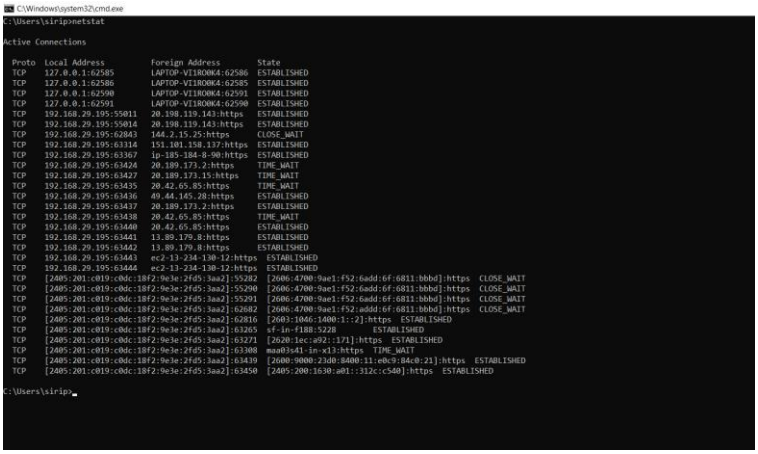
Start of authority, provides authority information about the domain, e-mail of the domain admin, domain serial number etc.



```
C:\Windows\system32\cmd.exe

C:\Users\sirip>nslookup -type=soa instagram.com
Server:  reliance.reliance
Address:  2405:201:c019:c0dc::c0a8:1d01

Non-authoritative answer:
instagram.com
        primary name server = a.ns.instagram.com
        responsible mail addr = dns.facebook.com
        serial  = 2279026984
        refresh = 14400 (4 hours)
        retry   = 1800 (30 mins)
        expire  = 604800 (7 days)
        default TTL = 3600 (1 hour)

C:\Users\sirip>
```

- **netstat**

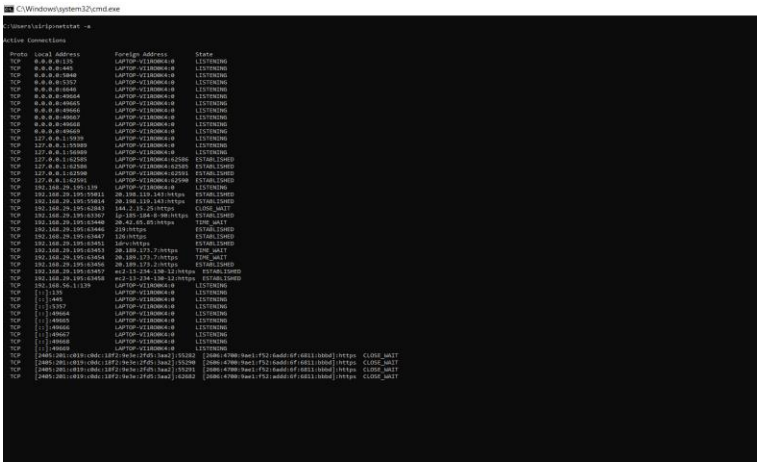
network statistics used to display very detailed information about how our computer is communication with other computers or network devices.



```
C:\Windows\system32\cmd.exe
C:\Users\sirip>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:62585        LAPTOP-VI1ROOK4:62586  ESTABLISHED
  TCP    127.0.0.1:62586        LAPTOP-VI1ROOK4:62585  ESTABLISHED
  TCP    127.0.0.1:62590        LAPTOP-VI1ROOK4:62591  ESTABLISHED
  TCP    127.0.0.1:62591        LAPTOP-VI1ROOK4:62590  ESTABLISHED
  TCP    192.168.29.195:55011   20.198.119.143:https   ESTABLISHED
  TCP    192.168.29.195:55014   20.198.119.143:https   ESTABLISHED
  TCP    192.168.29.195:62843   144.2.15.25:https      CLOSE_WAIT
  TCP    192.168.29.195:63314   151.101.158.137:https  ESTABLISHED
  TCP    192.168.29.195:63367   ip-185-184-8-90:https  ESTABLISHED
  TCP    192.168.29.195:63424   20.189.173.2:https     TIME_WAIT
  TCP    192.168.29.195:63427   20.189.173.15:https    TIME_WAIT
  TCP    192.168.29.195:63435   20.42.65.85:https      TIME_WAIT
  TCP    192.168.29.195:63436   40.44.165.20:https     ESTABLISHED
  TCP    192.168.29.195:63437   20.189.173.2:https     ESTABLISHED
  TCP    192.168.29.195:63438   20.42.65.85:https      TIME_WAIT
  TCP    192.168.29.195:63440   20.42.65.85:https      ESTABLISHED
  TCP    192.168.29.195:63441   13.89.179.8:https      ESTABLISHED
  TCP    192.168.29.195:63442   13.89.179.8:https      ESTABLISHED
  TCP    192.168.29.195:63443   ec2-13-234-130-12:https  ESTABLISHED
  TCP    192.168.29.195:63444   ec2-13-234-130-12:https  ESTABLISHED
  TCP    [2405:201:c019:c0dc:18f2:9e3e:2fd5:3aa2]:55282  [2606:4700:9ae1:f52:6add:6f:6811:bbbd]:https  CLOSE_WAIT
  TCP    [2405:201:c019:c0dc:18f2:9e3e:2fd5:3aa2]:55290  [2606:4700:9ae1:f52:6add:6f:6811:bbbd]:https  CLOSE_WAIT
  TCP    [2405:201:c019:c0dc:18f2:9e3e:2fd5:3aa2]:55291  [2606:4700:9ae1:f52:6add:6f:6811:bbbd]:https  CLOSE_WAIT
  TCP    [2405:201:c019:c0dc:18f2:9e3e:2fd5:3aa2]:62802  [2606:4700:9ae1:f52:add4:6f:6811:bbbd]:https  CLOSE_WAIT
  TCP    [2405:201:c019:c0dc:18f2:9e3e:2fd5:3aa2]:62816  [2603:1046:1400:1::2]:https  ESTABLISHED
  TCP    [2405:201:c019:c0dc:18f2:9e3e:2fd5:3aa2]:63265  sf-in-f188:5228      ESTABLISHED
  TCP    [2405:201:c019:c0dc:18f2:9e3e:2fd5:3aa2]:63271  [2620:1ec:a92::171]:https  ESTABLISHED
  TCP    [2405:201:c019:c0dc:18f2:9e3e:2fd5:3aa2]:63308  maa03s41-in-x13:https  TIME_WAIT
  TCP    [2405:201:c019:c0dc:18f2:9e3e:2fd5:3aa2]:63439  [2600:9000:23d0:8400:11:e0c9:84c0:21]:https  ESTABLISHED
  TCP    [2405:201:c019:c0dc:18f2:9e3e:2fd5:3aa2]:63450  [2405:200:1630:a01::312c:c540]:https  ESTABLISHED

C:\Users\sirip>
```

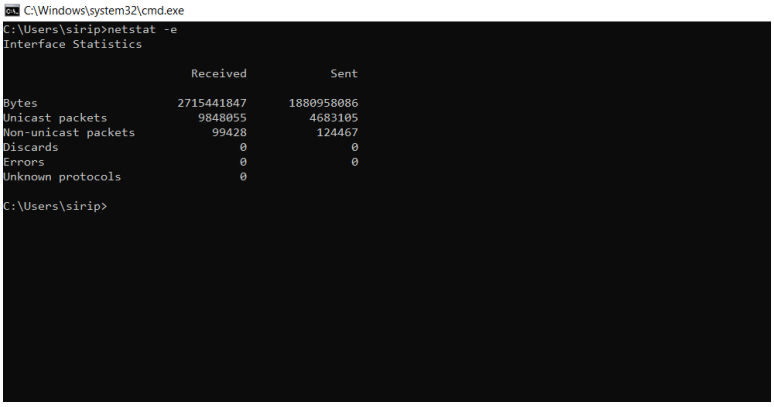
- **netstat –a**

Displays all active Tcp conversations and tcp,udp ports on which computer is listening



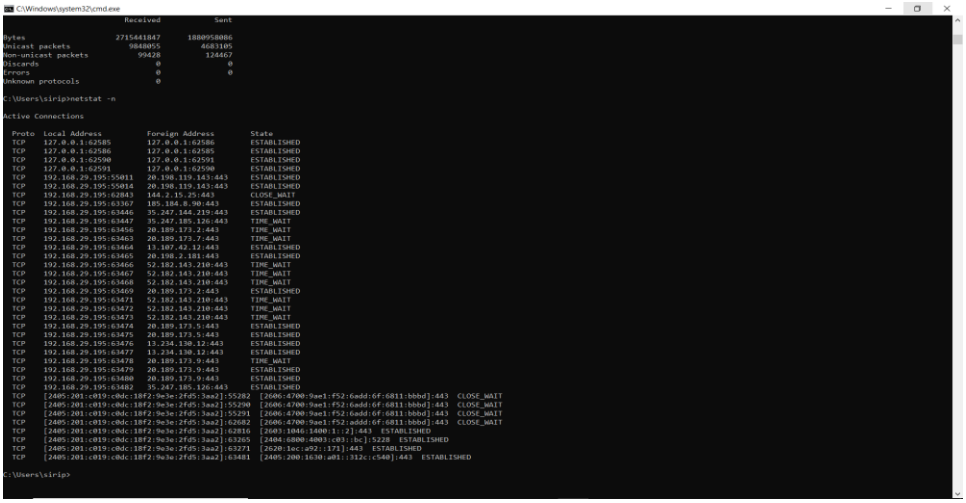
- **netstat –e**

Shows statistics about network connection data



- **netstat-n**

prevent from attempting to determine the host names for the foreign IP address



```
C:\Windows\system32\cmd.exe

                           Received            Sent

Bytes                    2715441847      1880958086
Unicast packets             9840055         4683185
Non-unicast packets           99428          124467
Discards                          0               0
Errors                            0               0
Unknown protocols                 0

C:\Users\sirip>netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:62585        127.0.0.1:62586        ESTABLISHED
  TCP    127.0.0.1:62586        127.0.0.1:62585        ESTABLISHED
  TCP    127.0.0.1:62590        127.0.0.1:62591        ESTABLISHED
  TCP    127.0.0.1:62591        127.0.0.1:62590        ESTABLISHED
  TCP    192.168.29.195:55011   20.198.119.143:443     ESTABLISHED
  TCP    192.168.29.195:55014   20.198.119.143:443     ESTABLISHED
  TCP    192.168.29.195:62843   144.2.15.25:443        CLOSE_WAIT
  TCP    192.168.29.195:63367   185.184.8.90:443       ESTABLISHED
  TCP    192.168.29.195:63446   35.247.144.219:443     ESTABLISHED
  TCP    192.168.29.195:63447   35.247.185.126:443     TIME_WAIT
  TCP    192.168.29.195:63456   20.189.173.2:443       TIME_WAIT
  TCP    192.168.29.195:63463   20.189.173.7:443       TIME_WAIT
  TCP    192.168.29.195:63464   13.107.42.12:443       ESTABLISHED
  TCP    192.168.29.195:63465   20.198.2.101:443       ESTABLISHED
  TCP    192.168.29.195:63466   52.182.143.210:443     TIME_WAIT
  TCP    192.168.29.195:63467   52.182.143.210:443     TIME_WAIT
  TCP    192.168.29.195:63468   52.182.143.210:443     TIME_WAIT
  TCP    192.168.29.195:63469   20.189.173.2:443       ESTABLISHED
  TCP    192.168.29.195:63471   52.182.143.210:443     TIME_WAIT
  TCP    192.168.29.195:63472   52.182.143.210:443     TIME_WAIT
  TCP    192.168.29.195:63473   52.182.143.210:443     TIME_WAIT
  TCP    192.168.29.195:63474   20.189.173.5:443       ESTABLISHED
  TCP    192.168.29.195:63475   20.189.173.5:443       ESTABLISHED
  TCP    192.168.29.195:63476   13.234.130.12:443      ESTABLISHED
  TCP    192.168.29.195:63477   13.234.130.12:443      ESTABLISHED
  TCP    192.168.29.195:63478   20.189.173.9:443       TIME_WAIT
  TCP    192.168.29.195:63479   20.189.173.9:443       ESTABLISHED
  TCP    192.168.29.195:63480   20.189.173.9:443       ESTABLISHED
  TCP    192.168.29.195:63482   35.247.185.126:443     ESTABLISHED
  TCP    [2405:201:c019:c0dc:18f2:9e3e:2fd5:3aa2]:55282  [2606:4700:9ae1:f52:6add:6f:6811:bbbd]:443  CLOSE_WAIT
  TCP    [2405:201:c019:c0dc:18f2:9e3e:2fd5:3aa2]:55290  [2606:4700:9ae1:f52:6add:6f:6811:bbbd]:443  CLOSE_WAIT
  TCP    [2405:201:c019:c0dc:18f2:9e3e:2fd5:3aa2]:55291  [2606:4700:9ae1:f52:6add:6f:6811:bbbd]:443  CLOSE_WAIT
  TCP    [2405:201:c019:c0dc:18f2:9e3e:2fd5:3aa2]:62682  [2606:4700:9ae1:f52:6add:6f:6811:bbbd]:443  CLOSE_WAIT
  TCP    [2405:201:c019:c0dc:18f2:9e3e:2fd5:3aa2]:62816  [2603:1046:1400:1::2]:443  ESTABLISHED
  TCP    [2405:201:c019:c0dc:18f2:9e3e:2fd5:3aa2]:63205  [2404:6800:4003:c03::bc]:5228  ESTABLISHED
  TCP    [2405:201:c019:c0dc:18f2:9e3e:2fd5:3aa2]:63271  [2620:1ec:a92::171]:443  ESTABLISHED
  TCP    [2405:201:c019:c0dc:18f2:9e3e:2fd5:3aa2]:63481  [2405:200:1630:a01::312c:c540]:443  ESTABLISHED

C:\Users\sirip>
```

- **netstat-o**

Displays the PID associated with each displayed connection

```
[10/02/22]seed@VM:~$ netstat -o
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       Timer
udp        0      0 VM:bootpc               10.0.2.3:bootps         ESTABLISHED off (0.00/0/0)
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    32573    /run/user/1000/systemd/notify
unix  2      [ ]         DGRAM                    13355    /run/systemd/journal/syslog
unix  16     [ ]         DGRAM                    13365    /run/systemd/journal/dev-log
unix  11     [ ]         DGRAM                    13369    /run/systemd/journal/socket
unix  3      [ ]         DGRAM                    13341    /run/systemd/notify
unix  3      [ ]         STREAM     CONNECTED     37240
unix  3      [ ]         STREAM     CONNECTED     35956    @/tmp/.ICE-unix/2030
unix  3      [ ]         STREAM     CONNECTED     33543
unix  3      [ ]         STREAM     CONNECTED     30077
unix  3      [ ]         STREAM     CONNECTED     37382    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     36739
unix  3      [ ]         STREAM     CONNECTED     36005    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     33475
unix  3      [ ]         STREAM     CONNECTED     31241
unix  3      [ ]         STREAM     CONNECTED     30203
```

- **netstat- p**

shows connection on statistics only for a particular protocol

Can't define more than one protocol at once

```
[10/02/22]seed@VM:~$ netstat -s -p tcp
Ip:
    Forwarding: 1
    272 total packets received
    0 forwarded
    0 incoming packets discarded
    269 incoming packets delivered
    275 requests sent out
    20 outgoing packets dropped
Icmp:
    40 ICMP messages received
    0 input ICMP message failed
    ICMP input histogram:
        destination unreachable: 40
    40 ICMP messages sent
    0 ICMP messages failed
    ICMP output histogram:
        destination unreachable: 40
IcmpMsg:
        InType3: 40
        OutType3: 40
Tcp:
    6 active connection openings
    0 passive connection openings
    4 failed connection attempts
    0 connection resets received
    0 connections established
    19 segments received
    19 segments sent out
    0 segments retransmitted
    0 bad segments received
    4 resets sent
Udp:
    170 packets received
    40 packets to unknown port received
    0 packet receive errors
```

```
    4 resets sent
Udp:
    170 packets received
    40 packets to unknown port received
    0 packet receive errors
    214 packets sent
    0 receive buffer errors
    0 send buffer errors
    IgnoredMulti: 4
UdpLite:
TcpExt:
    2 packet headers predicted
    4 acknowledgments not containing data payload received
    IPReversePathFilter: 1
    TCPOrigDataSent: 4
    TCPDelivered: 6
IpExt:
    InMcastPkts: 71
    OutMcastPkts: 75
    InBcastPkts: 4
    OutBcastPkts: 4
    InOctets: 23788
    OutOctets: 22569
    InMcastOctets: 6911
    OutMcastOctets: 7087
    InBcastOctets: 310
    OutBcastOctets: 310
    InNoECTPkts: 272
[10/02/22]seed@VM:~$
```

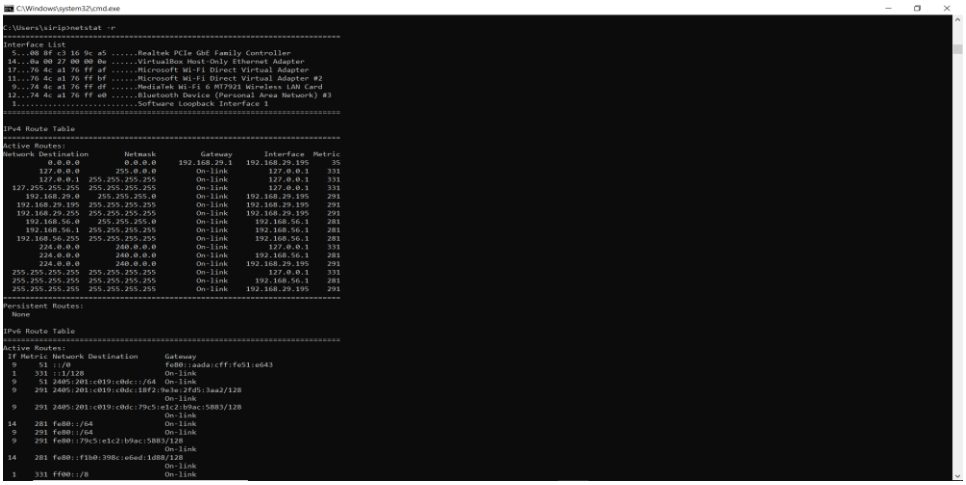
- **netstat-s**

Detailed statistical by protocol

```
C:\Windows\system32\cmd.exe
C:\Users\sirip>netstat -s

IPv4 Statistics

  Packets Received                   = 799859
  Received Header Errors             = 0
  Received Address Errors            = 2042
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 1
  Received Packets Discarded         = 4717
  Received Packets Delivered         = 890858
  Output Requests                    = 574809
  Routing Discards                   = 0
  Discarded Output Packets           = 3014
  Output Packet No Route             = 339
  Reassembly Required                = 0
  Reassembly Successful              = 0
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 0
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 0

IPv6 Statistics

  Packets Received                   = 622973
  Received Header Errors             = 0
  Received Address Errors            = 2963
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 0
  Received Packets Discarded         = 568
  Received Packets Delivered         = 628492
  Output Requests                    = 305596
  Routing Discards                   = 0
  Discarded Output Packets           = 25
  Output Packet No Route             = 5
  Reassembly Required                = 0
  Reassembly Successful              = 0
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 0
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 0

ICMPv4 Statistics

                             Received    Sent
  Messages                   2277        3052
  Errors                     0           0
  Destination Unreachable    1312        2036
  Time Exceeded              15          0
  Parameter Problems         0           0
  Source Quenches            0           0
  Redirects                  0           0
  Echo Replies               489         461
  Echos                      461         555
  Timestamps                 0           0
```

- **netstat-r**

Ip routing table similar to route print command



```
C:\Windows\system32\cmd.exe
C:\Users\sirip>netstat -r
===========================================================================
Interface List
  5...08 8f c3 16 9c a5 ......Realtek PCIe GbE Family Controller
 14...0a 00 27 00 00 0e ......VirtualBox Host-Only Ethernet Adapter
 17...76 4c a1 76 ff af ......Microsoft Wi-Fi Direct Virtual Adapter
 11...76 4c a1 76 ff bf ......Microsoft Wi-Fi Direct Virtual Adapter #2
  9...74 4c a1 76 ff df ......MediaTek Wi-Fi 6 MT7921 Wireless LAN Card
 12...74 4c a1 76 ff e0 ......Bluetooth Device (Personal Area Network) #3
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     192.168.29.1  192.168.29.195     35
        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
     192.168.29.0    255.255.255.0         On-link    192.168.29.195    291
   192.168.29.195  255.255.255.255         On-link    192.168.29.195    291
   192.168.29.255  255.255.255.255         On-link    192.168.29.195    291
     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
        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    192.168.29.195    291
  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    192.168.29.195    291
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  9     51 ::/0                     fe80::aada:cff:fe51:e643
  1    331 ::1/128                  On-link
  9     51 2405:201:c019:c0dc::/64  On-link
  9    291 2405:201:c019:c0dc:18f2:9e3e:2fd5:3aa2/128
                                    On-link
  9    291 2405:201:c019:c0dc:79c5:e1c2:b9ac:5883/128
                                    On-link
 14    281 fe80::/64               On-link
  9    291 fe80::/64               On-link
  9    291 fe80::79c5:e1c2:b9ac:5883/128
                                    On-link
 14    281 fe80::f1b0:398c:e6ed:1d88/128
                                    On-link
  1    331 ff00::/8                On-link
```

- **netstat/time_interval**

Used to measure time in seconds, and also to re-execute automatically

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19044.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\sirip>netstat -o

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    127.0.0.1:49670        LAPTOP-VI1RO0K4:49671  ESTABLISHED     7552
  TCP    127.0.0.1:49671        LAPTOP-VI1RO0K4:49670  ESTABLISHED     7552
  TCP    127.0.0.1:49674        LAPTOP-VI1RO0K4:49675  ESTABLISHED     7552
  TCP    127.0.0.1:49675        LAPTOP-VI1RO0K4:49674  ESTABLISHED     7552
  TCP    127.0.0.1:50304        LAPTOP-VI1RO0K4:50305  ESTABLISHED     16936
  TCP    127.0.0.1:50305        LAPTOP-VI1RO0K4:50304  ESTABLISHED     16936
  TCP    127.0.0.1:50306        LAPTOP-VI1RO0K4:50307  ESTABLISHED     16936
  TCP    127.0.0.1:50307        LAPTOP-VI1RO0K4:50306  ESTABLISHED     16936
  TCP    127.0.0.1:50308        LAPTOP-VI1RO0K4:50309  ESTABLISHED     16936
  TCP    127.0.0.1:50309        LAPTOP-VI1RO0K4:50308  ESTABLISHED     16936
  TCP    127.0.0.1:50310        LAPTOP-VI1RO0K4:50311  ESTABLISHED     16936
  TCP    127.0.0.1:50311        LAPTOP-VI1RO0K4:50310  ESTABLISHED     16936
  TCP    127.0.0.1:50312        LAPTOP-VI1RO0K4:50313  ESTABLISHED     16936
  TCP    127.0.0.1:50313        LAPTOP-VI1RO0K4:50312  ESTABLISHED     16936
  TCP    192.168.29.195:50288   20.198.118.190:https   ESTABLISHED     10116
  TCP    192.168.29.195:50927   192.168.29.11:8009     ESTABLISHED     14924
^C
C:\Users\sirip>
```

- **netstat/ ?**

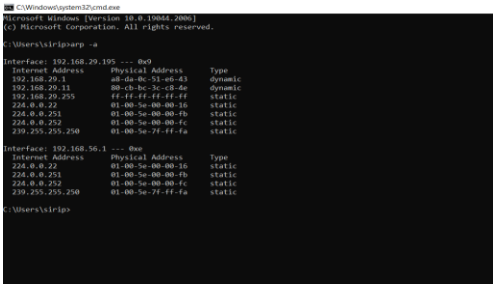
Help command

```
C:\Windows\system32\cmd.exe

C:\Users\sirip>netstat /?

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-f] [-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.
  -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
                configuration information once.


C:\Users\sirip>
```

>>Arp-Address Resolution Protocol

- **arp –a**

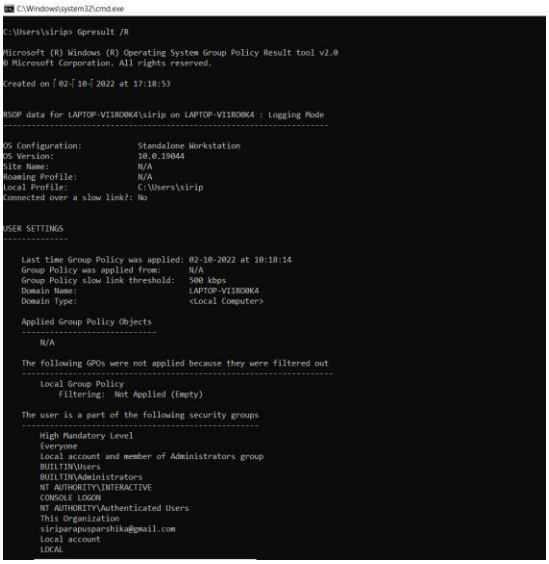
Used for mapping Ip address to physical MAC address on LAN.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19044.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\sirip>arp -a

Interface: 192.168.29.195 --- 0x9
  Internet Address      Physical Address      Type
  192.168.29.1          a8-da-0c-51-e6-43     dynamic
  192.168.29.11         80-cb-bc-3c-c8-4e     dynamic
  192.168.29.255        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

Interface: 192.168.56.1 --- 0xe
  Internet Address      Physical Address      Type
  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

C:\Users\sirip>
```

- **Gpresult**

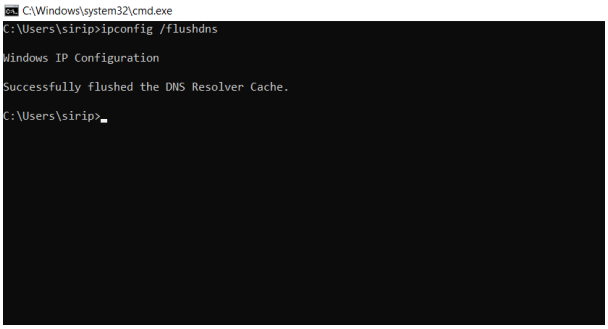
Displays RSOP information for a remote user and uses it to report remotely targeted computer through firewall.



```
C:\Windows\system32\cmd.exe
C:\Users\sirip> Gpresult /R

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

Created on 02-10-2022 at 17:18:53


RSOP data for LAPTOP-VI1RO0K4\sirip on LAPTOP-VI1RO0K4 : Logging Mode
---------------------------------------------------------------------------

OS Configuration:            Standalone Workstation
OS Version:                  10.0.19044
Site Name:                   N/A
Roaming Profile:             N/A
Local Profile:               C:\Users\sirip
Connected over a slow link?: No


USER SETTINGS
--------------

    Last time Group Policy was applied: 02-10-2022 at 10:18:14
    Group Policy was applied from:      N/A
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        LAPTOP-VI1RO0K4
    Domain Type:                        <Local Computer>

    Applied Group Policy Objects
    ----------------------------
        N/A

    The following GPOs were not applied because they were filtered out
    -------------------------------------------------------------------
        Local Group Policy
            Filtering:  Not Applied (Empty)

    The user is a part of the following security groups
    ---------------------------------------------------
        High Mandatory Level
        Everyone
        Local account and member of Administrators group
        BUILTIN\Users
        BUILTIN\Administrators
        NT AUTHORITY\INTERACTIVE
        CONSOLE LOGON
        NT AUTHORITY\Authenticated Users
        This Organization
        siripurapuspparshika@gmail.com
        Local account
        LOCAL
```

- **ipconfig/ flushdns**

Flushing Dns is the useful in removal of bad caches since the flush completely removes all the info stored with in the cache

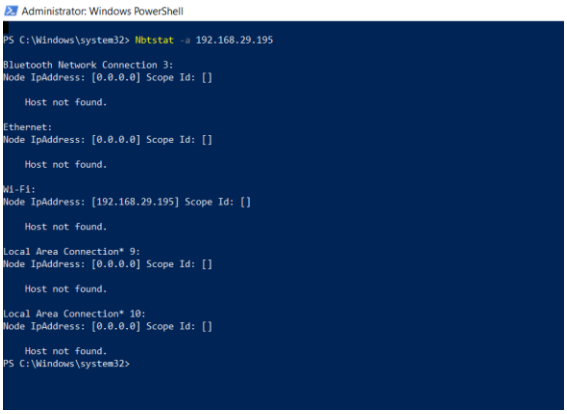


- **nbstat-a**

  Displays the NetBIOS name table of a remote computer, where *remotename* is the NetBIOS computer name of the remote computer.

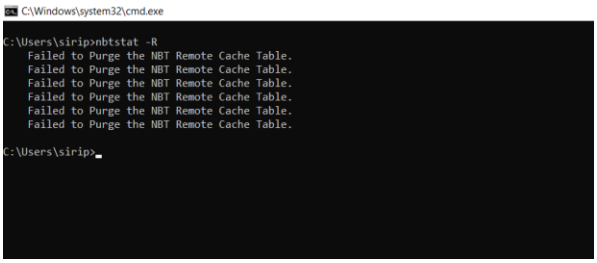
- **nbtstat-A**

  Displays the NetBIOS name table of a remote computer, specified by the IP address (in dotted decimal notation) of the remote computer.



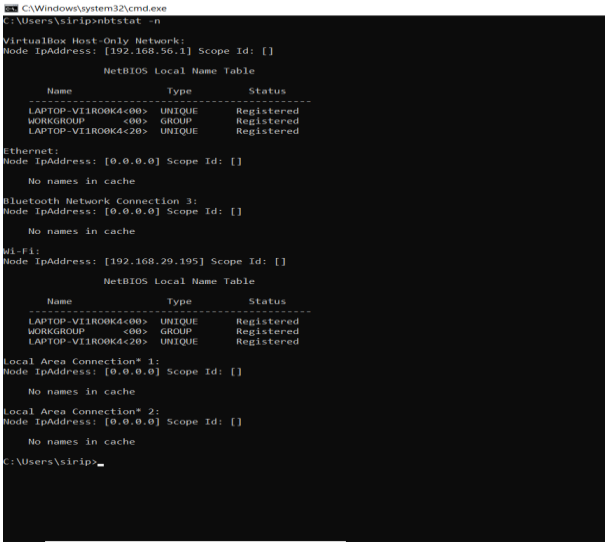
- **nbtstat -R**

Purges and reload the cached name from table to the LMHOST(text file that maps Ip address to the NetBios) file



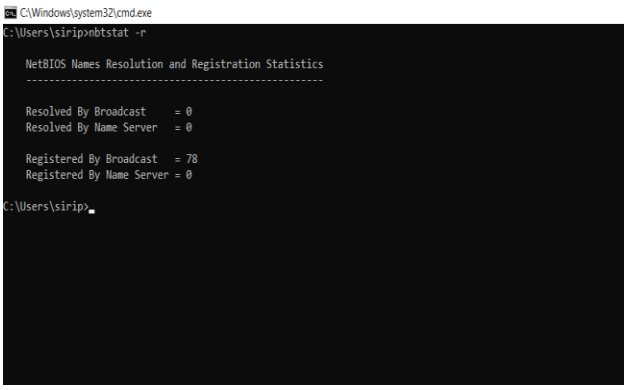
- **nbtstat -n**

List locally registered NetBios names



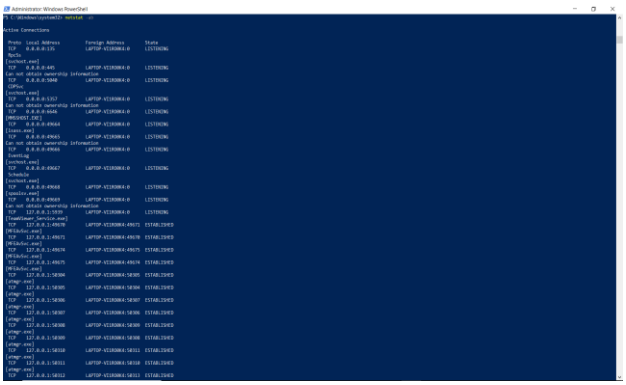
- **nbtstat-r**

Displays a count of the name resolved by broadcast and via WINS



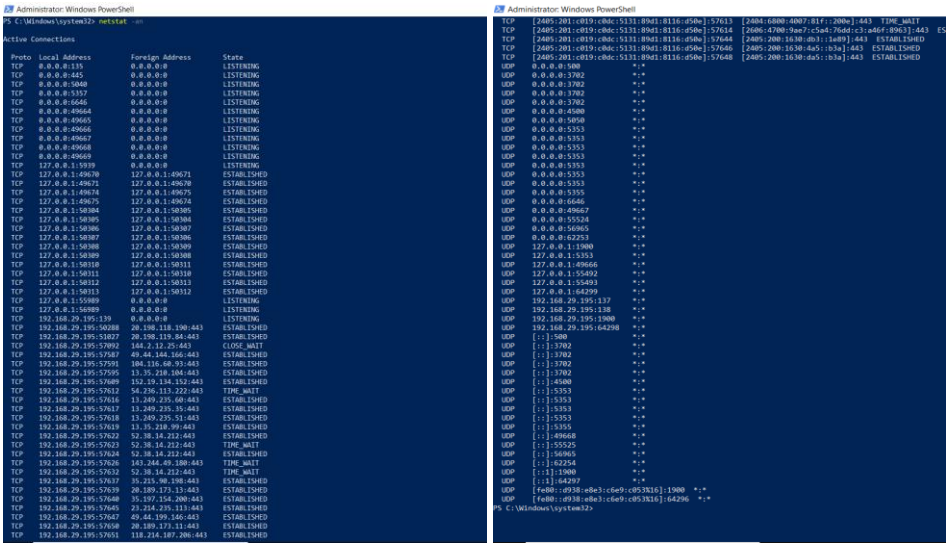
- **netstat –ab**

Executable involved in creating each connection or listening port



- **netstat-an**

Displays all the active TCP connections, address, and port numbers are expressed numerically and no attempt is made to determine name.

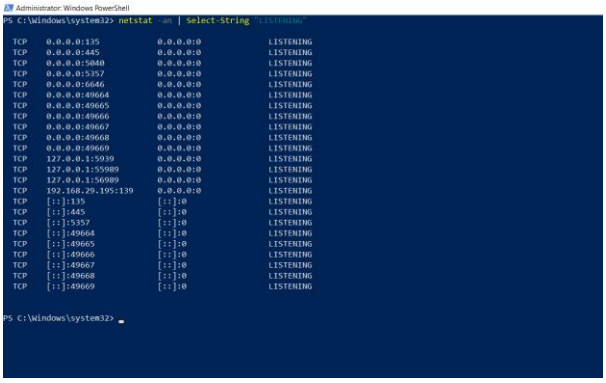


- **netstat-an1|find “15868”**

Displays all the strings that contain 15868 and redisplays every minute.

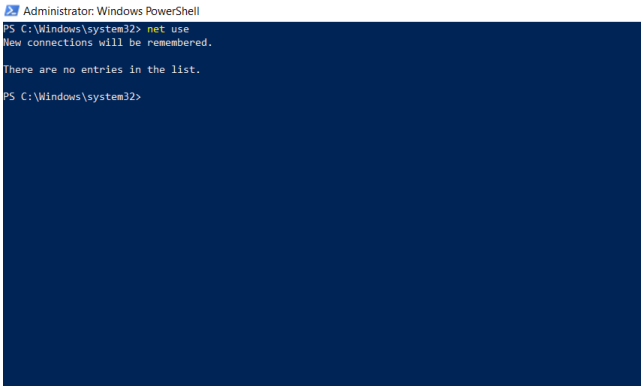
- **netstat-an1|find “listening”**

Displays all the strings that contain “listening”



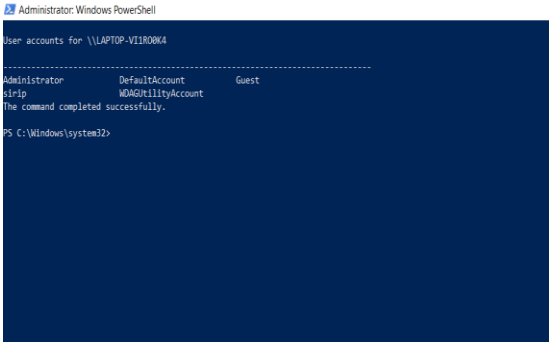
- **netuse:**

Used to connect and disconnect from a network resource and view current connection to the network resources.

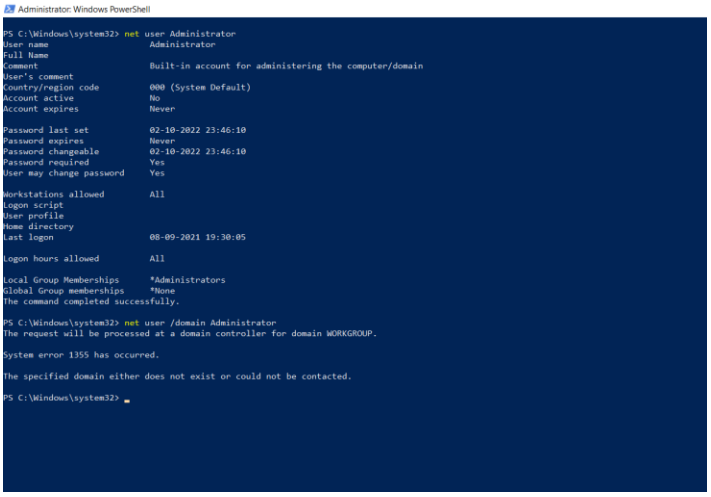


- **net user**

Displays list of the user's accounts on the computer

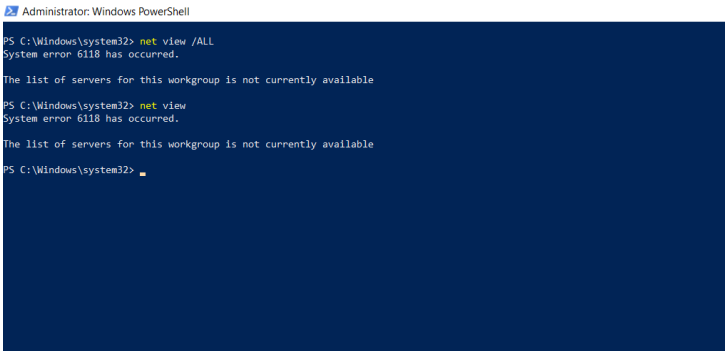


- **net user /domain <username>**



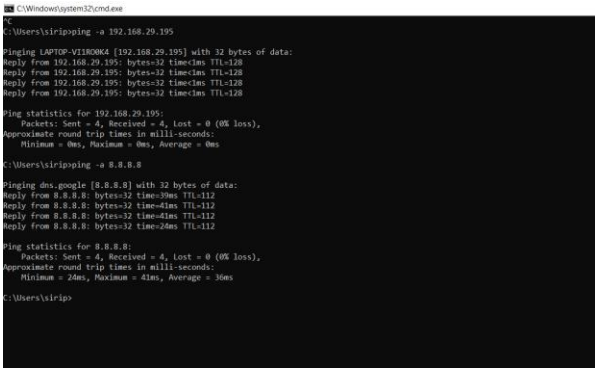
- **net view/cache**

Displays the list of Domains, computers, resources being shared by specified computer.



- **ping-a<ip>**

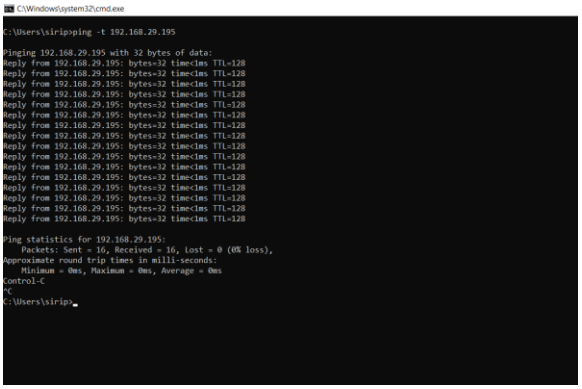
specifies reverse name resolution to be performed on the destination Ip address, if success ping will display the corresponding host name



```
^C
C:\Users\sirip>ping -a 192.168.29.195

Pinging LAPTOP-VI1RO0K4 [192.168.29.195] with 32 bytes of data:
Reply from 192.168.29.195: bytes=32 time<1ms TTL=128
Reply from 192.168.29.195: bytes=32 time<1ms TTL=128
Reply from 192.168.29.195: bytes=32 time<1ms TTL=128
Reply from 192.168.29.195: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.29.195:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\sirip>ping -a 8.8.8.8

Pinging dns.google [8.8.8.8] with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=39ms TTL=112
Reply from 8.8.8.8: bytes=32 time=41ms TTL=112
Reply from 8.8.8.8: bytes=32 time=41ms TTL=112
Reply from 8.8.8.8: bytes=32 time=24ms TTL=112

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 24ms, Maximum = 41ms, Average = 36ms

C:\Users\sirip>
```

- **ping-t <ip>**

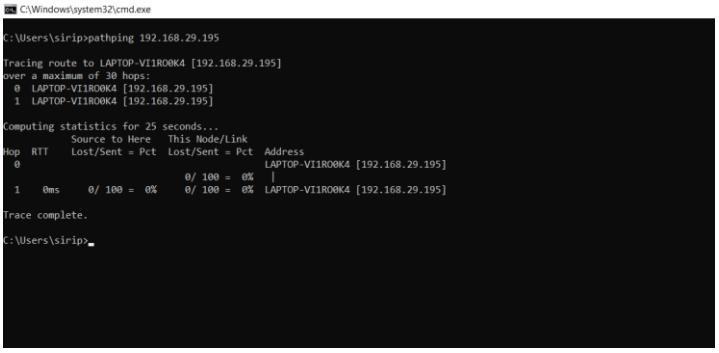
Ip ping service sends several ICMP packets to domain or IP and returns detailed output and keeps on printing until we enter Ctrl+C to stop



```
C:\Users\sirip>ping -t 192.168.29.195

Pinging 192.168.29.195 with 32 bytes of data:
Reply from 192.168.29.195: bytes=32 time<1ms TTL=128
Reply from 192.168.29.195: bytes=32 time<1ms TTL=128
Reply from 192.168.29.195: bytes=32 time<1ms TTL=128
Reply from 192.168.29.195: bytes=32 time<1ms TTL=128
Reply from 192.168.29.195: bytes=32 time<1ms TTL=128
Reply from 192.168.29.195: bytes=32 time<1ms TTL=128
Reply from 192.168.29.195: bytes=32 time<1ms TTL=128
Reply from 192.168.29.195: bytes=32 time<1ms TTL=128
Reply from 192.168.29.195: bytes=32 time<1ms TTL=128
Reply from 192.168.29.195: bytes=32 time<1ms TTL=128
Reply from 192.168.29.195: bytes=32 time<1ms TTL=128
Reply from 192.168.29.195: bytes=32 time<1ms TTL=128
Reply from 192.168.29.195: bytes=32 time<1ms TTL=128
Reply from 192.168.29.195: bytes=32 time<1ms TTL=128
Reply from 192.168.29.195: bytes=32 time<1ms TTL=128
Reply from 192.168.29.195: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.29.195:
    Packets: Sent = 16, Received = 16, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\Users\sirip>_
```

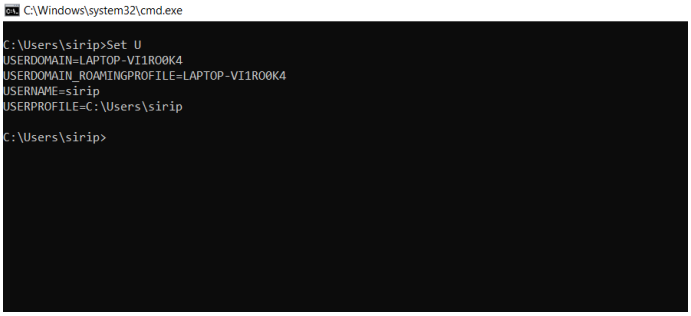
- **Pathping:**

It explains about the number of hops between user and destination, 1st trace is the router showing route for every node and Next it calculates latency and packet loss for each hop in the route



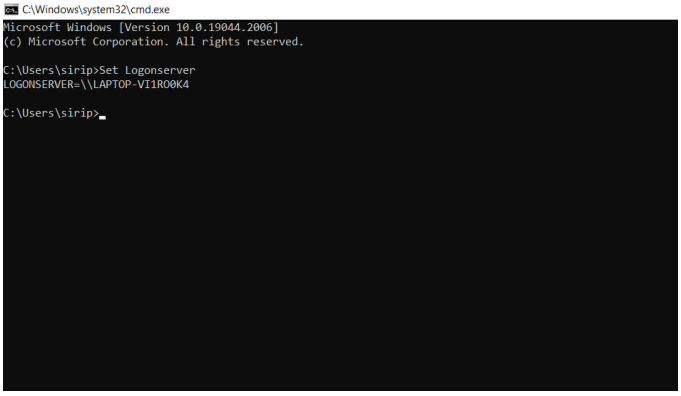
- **set-U**

shows which user is logged in



- **set-logonserver:**

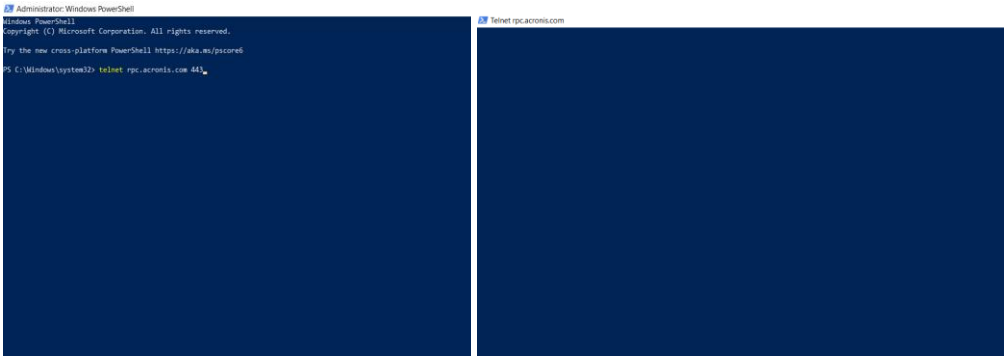
It's an environment variable, shows what user used as a logon server.



- **telnet <IP><port>**

-Computer protocols that were built for interacting with remote computers

-Test connectivity to remote machine and issues commands through the keyboard.



<u>RESULT:</u>

Studied and performed basic network administration and troubleshooting using Windows command line utilities.