

INTERNET PROTOCOL LAB ASSIGNMENT -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

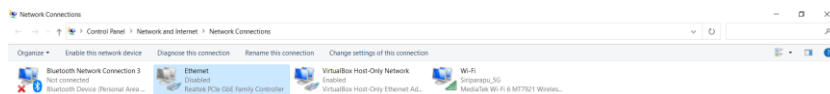
TOOLS REQUIRED:

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

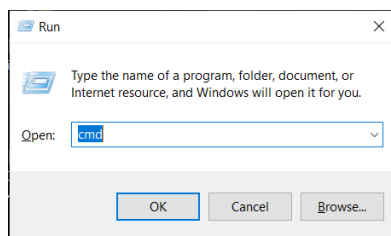
PROCEDURE:

- 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.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19044.2000]
(c) Microsoft Corporation. All rights reserved.

C:\Users\slr\ipconfig
Windows IP Configuration

Ethernet adapter VirtualBox Host-Only Network:

    Connection-specific DNS Suffix . : 
    Link-local IPv6 Address . . . . . : fe80::f1b0:398c:e6ed:1d88%14
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 2:

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

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix . : 
    IPv6 Address. . . . . : 2405:201:c019:c0dc:79c5:e1c2:b9ac:5883
    Temporary IPv6 Address. . . . . : 2405:201:c019:c0dc:990c:40ce:a9a5:96a4
    Link-local IPv6 Address . . . . . : fe80::79c5:e1c2:b9ac:5883%30
    IPv4 Address. . . . . : 192.168.29.195
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::adaa:eff:fe51:e643%30
    . . . . . : 192.168.29.1

Ethernet adapter Bluetooth Network Connection 3:

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

- **ipconfig /all Command**

Displays the entire network information for all the adapters.

```
C:\Windows\system32\cmd.exe
C:\Users\slr\ipconfig /all
Windows IP Configuration

Host Name . . . . . : LAPTOP-VI180661
Primary DNS Suffix . : 
Node Type . . . . . : Unknown
IP Routing Enabled . . . . . : No
WINS Proxy Enabled . . . . . : No

Ethernet adapter VirtualBox Host-Only Network:

    Connection-specific DNS Suffix . : 
    Description . . . . . : VirtualBox Host-Only Ethernet Adapter
    Physical Address. . . . . : 08-00-27-00-00-02
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::f1b0:398c:e6ed:1d88%14(Preferred)
    IPv4 Address. . . . . : 192.168.56.1(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 
    DHCPv6 DAD . . . . . : No
    DHCPv6 Client DUID. . . . . : 00-01-00-01-20-CA-AC-57-00-0F-C3-16-9C-A5
    DNS Servers . . . . . : fe80::b:ffff::32
    NetBIOS over Tcpip. . . . . : Enabled

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : 
    Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
    Physical Address. . . . . : 8E-4E-A2-76-FF-4F
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : 
    Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
    Physical Address. . . . . : 8E-4E-A2-76-FF-4F
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix . : 
    Description . . . . . : MediaTek Wi-Fi 6 MT7921 Wireless LAN Card
    Physical Address. . . . . : 74-4C-A1-76-FF-DF

Ethernet adapter Bluetooth Network Connection 3:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : 
    Description . . . . . : Bluetooth Device (Personal Area Network) #3
    Physical Address. . . . . : 74-4C-A1-76-FF-E0
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
```

- **ipconfig /release Command**

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

```
Ethernet adapter VirtualBox Host-Only Network:

    Connection-specific DNS Suffix . : 
    Link-local IPv6 Address . . . . . : fe80::f1b0:398c:e6ed:1d88%14
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :
```

▪ **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.

```
Administrator: Windows PowerShell

Windows IP Configuration

No operation can be performed on Ethernet while it has its media disconnected.
No operation can be performed on Local Area Connection* 1 while it has its media disconnected.
No operation can be performed on Local Area Connection* 2 while it has its media disconnected.
No operation can be performed on Bluetooth Network Connection 3 while it has its media disconnected.

Ethernet adapter Ethernet:

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

Ethernet adapter VirtualBox Host-Only Network:

    Connection-specific DNS Suffix . :
    Link-Local IPv6 Address . . . . : fe80::f3b0:398c:e6ed:1d80%14
    IPv4 Address. . . . . : 192.168.255.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 2:

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

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix . :
    IPv6 Address. . . . . : 2405:201:c019:c0dc:79c5:e1c2:b9ac:5883
    Temporary IPv6 Address. . . . : 2405:201:c019:c0dc:10f2:9e3e:2fd5:3aa2
    Link-Local IPv6 Address. . . . : fe80:79c5:e1c2:b9ac:5883%0
    IPv4 Address. . . . . : 192.168.29.195
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::aada:cff:fe51:e643%0
    192.168.29.1

Ethernet adapter Bluetooth Network Connection 3:

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

▪ **ipconfig /flushdns Command**

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

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

Connection-specific DNS Suffix . :

C:\Users\sirip>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\sirip>
```

▪ **ipconfig /displaydns Command**

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

```
Administrator: Windows PowerShell

Successfully flushed the DNS Resolver Cache.
PS C:\Windows\system32> ipconfig /displaydns

Windows IP Configuration


evolve-windowservices-tas.msedge.net
-----
Record Name . . . . . : evolve-windowservices-tas.msedge.net
Record Type . . . . . : 5
Time To Live . . . . . : 141
Data Length . . . . . : 8
Section . . . . . : Answer
CNAME Record . . . . : evolve-windowservices-tas.msedge.net.e-0009.e-msedge.net

Record Name . . . . . : evolve-windowservices-tas.msedge.net.e-0009.e-msedge.net
Record Type . . . . . : 5
Time To Live . . . . . : 141
Data Length . . . . . : 8
Section . . . . . : Answer
CNAME Record . . . . : e-0009.e-msedge.net

Record Name . . . . . : e-0009.e-msedge.net
Record Type . . . . . : 1
Time To Live . . . . . : 141
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 13.107.5.88
```

- **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



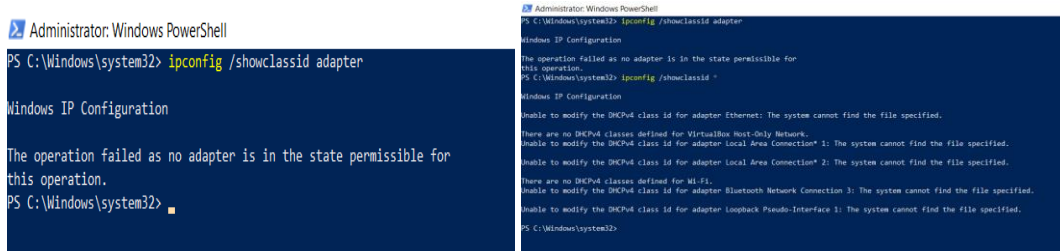
```
Administrator: Windows PowerShell
PS C:\Windows\system32> ipconfig /registerdns

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.
PS C:\Windows\system32>
```

- **ipconfig /showclassid adapter Command**

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



```
Administrator: Windows PowerShell
PS C:\Windows\system32> ipconfig /showclassid adapter

Windows IP Configuration

The operation failed as no adapter is in the state permissible for this operation.
PS C:\Windows\system32>

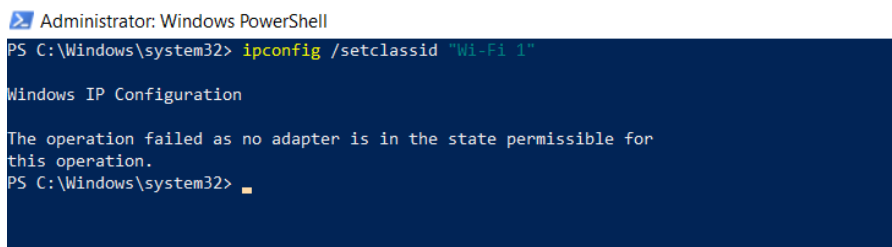
Administrator: Windows PowerShell
PS C:\Windows\system32> ipconfig /showclassid *

Windows IP Configuration

Unable to modify the DHCPv4 class id for adapter Ethernet: The system cannot find the file specified.
There are no DHCPv4 classes defined for VirtualBox Host-Only Network.
Unable to modify the DHCPv4 class id for adapter Local Area Connection* 1: The system cannot find the file specified.
Unable to modify the DHCPv4 class id for adapter Local Area Connection* 2: The system cannot find the file specified.
There are no DHCPv4 classes defined for Wi-Fi.
Unable to modify the DHCPv4 class id for adapter Bluetooth Network Connection 3: The system cannot find the file specified.
Unable to modify the DHCPv4 class id for adapter Loopback Pseudo-Interface 1: The system cannot find the file specified.
PS C:\Windows\system32>
```

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

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



```
Administrator: Windows PowerShell
PS C:\Windows\system32> ipconfig /setclassid "Wi-Fi 1"

Windows IP Configuration

The operation failed as no adapter is in the state permissible for this operation.
PS C:\Windows\system32>
```

■ Ipconfig /? Command Help

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

USAGE:
    ipconfig [/allcompartment] [/? | /all |
        /renew [adapter] | /release [adapter] |
        /renew {adapter} | /release {adapter} |
        /flushdns | /displaydns | /registerdns |
        /flushdns {adapter} |
        /setclassid adapter [classid] |
        /showclassid adapter |
        /setclassid6 adapter [classid] |
        /showclassid6 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 IP address for the specified adapter.
    /release     Release the IPv6 address for the specified adapter.
    /renew       Renew the IP address for the specified adapter.
    /renew       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 {L*} ... renew any connection that has its
                        name starting with L
> ipconfig /release *Con* ... release all matching connections,
                        eg. "Wired Ethernet Connection 1" or
                        "Wired Ethernet Connection 2"
> ipconfig /allcompartment ... Show information about all
                        compartments
> ipconfig /allcompartment /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

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/powershell

PS C:\Windows\system32> ping 10.10.10.10

Pinging 10.10.10.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Windows\system32>
```

```
Administrator: Windows PowerShell

Ping statistics for 0.0.0.0:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Windows\system32> ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=5ms TTL=112
Reply from 8.8.8.8: bytes=32 time=2ms TTL=112
Reply from 8.8.8.8: bytes=32 time=0ms TTL=112
Reply from 8.8.8.8: bytes=32 time=0ms 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 = 2ms, Maximum = 5ms, Average = 4ms
PS C:\Windows\system32> ping howtogeek.com

Pinging howtogeek.com [151.101.66.217] with 32 bytes of data:
Reply from 151.101.66.217: bytes=32 time=0ms TTL=53
Reply from 151.101.66.217: bytes=32 time=2ms TTL=53
Reply from 151.101.66.217: bytes=32 time=0ms TTL=53
Reply from 151.101.66.217: bytes=32 time=0ms TTL=53

Ping statistics for 151.101.66.217:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 10ms, Average = 6ms
PS C:\Windows\system32>
```

- ping -t

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

```
C:\Windows\system32\cmd.exe
C:\Users\sirip> ping -t youtube.com

Pinging youtube.com [2404:6800:4007:82c::200e] with 32 bytes of data:
Request timed out.
Reply from 2404:6800:4007:82c::200e: time=40ms
Reply from 2404:6800:4007:82c::200e: time=59ms
Reply from 2404:6800:4007:82c::200e: time=58ms
Reply from 2404:6800:4007:82c::200e: time=59ms
Reply from 2404:6800:4007:82c::200e: time=59ms
Reply from 2404:6800:4007:82c::200e: time=140ms
Reply from 2404:6800:4007:82c::200e: time=59ms
Reply from 2404:6800:4007:82c::200e: time=42ms
Reply from 2404:6800:4007:82c::200e: time=42ms
Reply from 2404:6800:4007:82c::200e: time=58ms
Reply from 2404:6800:4007:82c::200e: time=57ms
Reply from 2404:6800:4007:82c::200e: time=50ms
Reply from 2404:6800:4007:82c::200e: time=40ms
Reply from 2404:6800:4007:82c::200e: time=43ms

Ping statistics for 2404:6800:4007:82c::200e:
    Packets: Sent = 16, Received = 15, Lost = 1 (6% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 40ms, Maximum = 140ms, Average = 57ms
Control-C
^C
C:\Users\sirip>
```

- ping -n:

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

```
Administrator: Windows PowerShell
PS C:\Windows\system32> ping -n 5 yahoo.com

Pinging yahoo.com [2001:4998:124:1507::f000] with 32 bytes of data:
Request timed out.
Reply from 2001:4998:124:1507::f000: time=258ms
Reply from 2001:4998:124:1507::f000: time=257ms
Reply from 2001:4998:124:1507::f000: time=258ms
Reply from 2001:4998:124:1507::f000: time=258ms

Ping statistics for 2001:4998:124:1507::f000:
    Packets: Sent = 5, Received = 4, Lost = 1 (20% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 257ms, Maximum = 258ms, Average = 257ms
PS C:\Windows\system32>
```

- ping -w

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

```
Administrator: Windows PowerShell
PS C:\Windows\system32> ping -w 5 gmail.com

Pinging gmail.com [2404:6800:4009:813::2005] with 32 bytes of data:
Request timed out.
Reply from 2404:6800:4009:813::2005: time=49ms
Reply from 2404:6800:4009:813::2005: time=50ms
Reply from 2404:6800:4009:813::2005: time=31ms

Ping statistics for 2404:6800:4009:813::2005:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 31ms, Maximum = 50ms, Average = 43ms
PS C:\Windows\system32>
```

- ping -l

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

```
C:\Windows\system32\cmd.exe
C:\Users\sirip> ping -l 56 google.com

Pinging google.com [2404:6800:4009:827::200e] with 56 bytes of data:
Request timed out.
Reply from 2404:6800:4009:827::200e: time=28ms
Reply from 2404:6800:4009:827::200e: time=44ms
Reply from 2404:6800:4009:827::200e: time=45ms

Ping statistics for 2404:6800:4009:827::200e:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 28ms, Maximum = 45ms, Average = 39ms
C:\Users\sirip>
```

- 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.

```
Administrator: Windows PowerShell
PS C:\Windows\system32> ping -f www.youtube.com

Pinging youtube-ui.l.google.com [142.250.199.174] with 32 bytes of data:
Reply from 142.250.199.174: bytes=32 time=105ms TTL=53
Reply from 142.250.199.174: bytes=32 time=61ms TTL=53
Reply from 142.250.199.174: bytes=32 time=61ms TTL=53
Reply from 142.250.199.174: bytes=32 time=43ms TTL=53

Ping statistics for 142.250.199.174:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 43ms, Maximum = 105ms, Average = 67ms
PS C:\Windows\system32>
```


>> Tracert

- Tool that determines the route to destination by sending ICMP packets to the destination.
- Entry or a hop 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:
  0  272 ms  2 ms  1 ms  2405:201:c019:c0dc:aada:cff:fe51:e43
  1  *      *      *      Request timed out.
  2  22 ms  12 ms  12 ms  2405:203:400:100:172:31:2:118
  3  70 ms  34 ms  38 ms  ae9:pr02.maa2.tfbw.net [2620:0:1c:dead:beef:992]
  4  26 ms  24 ms  25 ms  po102.psw04.maa2.tfbw.net [2620:0:1c:dead:beef:771]
  5  38 ms  27 ms  28 ms  po8.mslak.02.maa2.tfbw.net [2a03:2880:f037:ffff:381]
  6  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-VI80W0K4-62586 ESTABLISHED
TCP    127.0.0.1:62586          LAPTOP-VI80W0K4-62585 ESTABLISHED
TCP    127.0.0.1:62590          LAPTOP-VI80W0K4-62592 ESTABLISHED
TCP    127.0.0.1:62591          LAPTOP-VI80W0K4-62590 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    192.168.29.195:63116     151.101.138.137:https ESTABLISHED
TCP    192.168.29.195:63607     19.185.184.8:https     ESTABLISHED
TCP    192.168.29.195:63424     20.199.173.2:https     TIME_WAIT
TCP    192.168.29.195:63429     20.199.173.15:https     TIME_WAIT
TCP    192.168.29.195:63435     20.42.65.85:https      TIME_WAIT
TCP    192.168.29.195:63436     49.44.145.28:https     ESTABLISHED
TCP    192.168.29.195:63437     20.199.173.2: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:2f45:3aa2]:55282 [2606:4700:9ae1:f52:6add:6f:6811:bbbd]:https CLOSE_WAIT
TCP    [2405:201:c019:c0dc:18f2:9e3e:2f45:3aa2]:55290 [2606:4700:9ae1:f52:6add:6f:6811:bbbd]:https CLOSE_WAIT
TCP    [2405:201:c019:c0dc:18f2:9e3e:2f45:3aa2]:55291 [2606:4700:9ae1:f52:6add:6f:6811:bbbd]:https CLOSE_WAIT
TCP    [2405:201:c019:c0dc:18f2:9e3e:2f45:3aa2]:62682 [2606:4700:9ae1:f52:6add:6f:6811:bbbd]:https CLOSE_WAIT
TCP    [2405:201:c019:c0dc:18f2:9e3e:2f45:3aa2]:62816 [2603:104d:1400:1::2]:https ESTABLISHED
TCP    [2405:201:c019:c0dc:18f2:9e3e:2f45:3aa2]:63265 4f-4e-f180-5228        ESTABLISHED
TCP    [2405:201:c019:c0dc:18f2:9e3e:2f45:3aa2]:63271 [2620:1cc:a921:171]:https ESTABLISHED
TCP    [2405:201:c019:c0dc:18f2:9e3e:2f45:3aa2]:63308 msn01a11.br-c13:https TIME_WAIT
TCP    [2405:201:c019:c0dc:18f2:9e3e:2f45:3aa2]:63439 [2600:9000:1300:8000:11:ebc9:84dc:21]:https ESTABLISHED
TCP    [2405:201:c019:c0dc:18f2:9e3e:2f45:3aa2]:63450 [2405:200:1630:a011:312c:c540]:https ESTABLISHED

C:\Users\sirip>
```

- **netstat -a**

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

[illegible]

- **netstat -e**

Shows statistics about network connection data

```
C:\Windows\system32\cmd.exe
C:\Users\sirip>netstat -e
Interface Statistics

            Received            Sent
Bytes      2715441847      1880958086
Unicast packets      9848055      4683105
Non-unicast packets      99428      124467
Discards              0              0
Errors                0              0
Unknown protocols      0

C:\Users\sirip>
```

■ netstat-n

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

```
C:\Windows\system32\cmd.exe
Received Sent
Bytes 2715441847 1880950806
Unicast packets 8848055 4681105
Non-unicast packets 99428 124467
Discards 0 0
Errors 0 0
Unknown protocols 0 0

C:\Users\virip>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 192.168.29.195:50811 20.198.135.143:443 ESTABLISHED
TCP 192.168.29.195:50814 20.198.135.143:443 ESTABLISHED
TCP 192.168.29.195:63841 184.2.13.29:443 CLOSE_WAIT
TCP 192.168.29.195:63367 185.184.8.90:443 ESTABLISHED
TCP 192.168.29.195:63466 25.247.144.219:443 ESTABLISHED
TCP 192.168.29.195:63447 25.247.185.126:443 TIME_WAIT
TCP 192.168.29.195:63465 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 13.187.42.12:443 ESTABLISHED
TCP 192.168.29.195:63465 20.198.135.143:443 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 192.168.29.195:63481 25.247.185.126:443 ESTABLISHED
TCP [2405:201:c819:c8a2:18f2:9a3e:2f05:3aa2]:55282 [2606:4700:9a01:f52:6add:6f:8b11:bbbf]:443 CLOSE_WAIT
TCP [2405:201:c819:c8a2:18f2:9a3e:2f05:3aa2]:55280 [2606:4700:9a01:f52:6add:6f:8b11:bbbf]:443 CLOSE_WAIT
TCP [2405:201:c819:c8a2:18f2:9a3e:2f05:3aa2]:55291 [2606:4700:9a01:f52:6add:6f:8b11:bbbf]:443 CLOSE_WAIT
TCP [2405:201:c819:c8a2:18f2:9a3e:2f05:3aa2]:62682 [2606:4700:9a01:f52:6add:6f:8b11:bbbf]:443 CLOSE_WAIT
TCP [2405:201:c819:c8a2:18f2:9a3e:2f05:3aa2]:62616 [2603:1846:1a00:1:2]:443 ESTABLISHED
TCP [2405:201:c819:c8a2:18f2:9a3e:2f05:3aa2]:63205 [2404:1000:4005:c051:bc]:5228 ESTABLISHED
TCP [2405:201:c819:c8a2:18f2:9a3e:2f05:3aa2]:63271 [2400:1a4c:a02:1371:4a3]: ESTABLISHED
TCP [2405:201:c819:c8a2:18f2:9a3e:2f05:3aa2]:63481 [2405:200:1630:a01:1312c:c540]:443 ESTABLISHED

C:\Users\virip>
```

■ 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:bootpc         ESTABLISHED off (0.00/0/0)

Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags     Type       State          I-Node   Path
unix  2      [ ]       DGRAM      CONNECTED     37273    /run/user/1000/systemd/notify
unix  2      [ ]       DGRAM      CONNECTED     13355    /run/systemd/journal/syslog
unix  16     [ ]       DGRAM      CONNECTED     13365    /run/systemd/journal/dev-log
unix  11     [ ]       DGRAM      CONNECTED     13369    /run/systemd/journal/socket
unix  3      [ ]       DGRAM      CONNECTED     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\slurp\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 = 4712
Received Packets Delivered = 800018
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 Quench 0 0
Redirects 0 0
Echo Replies 461 555
Timestamps 0 0
```

■ netstat-r

Ip routing table similar to route print command

```
C:\Windows\system32\cmd.exe
C:\Users\slurp\netstat -r

Interface List
14...da 00 27 00 80 .....Realtek PCIe GbE Family Controller
17...76 4c a1 76 ff ff .....VirtualBox Host-Only Ethernet Adapter
11...76 4c a1 76 ff ff .....Microsoft Wi-Fi Direct Virtual Adapter #2
9...74 4c a1 76 ff ff .....MediaTek MT-7612 802.11n Wireless LAN Card
12...74 4c a1 76 ff ff .....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 30
127.0.0.0 255.0.0.0 On-link 127.0.0.1 331
192.168.29.0 255.255.255.255 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
192.168.56.0 255.255.255.0 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
240.0.0.0 240.0.0.0 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

Parallel Routes:
None

IPv6 Route Table
Active Routes:
If Metric Network Destination Gateway
1 331 ::::/32 On-link
9 51 ::1 On-link
9 51 2001::c019:c0d0::/64 On-link
9 201 2001::c019:c0d0::10f2::/64 On-link
9 201 2001::c019:c0d0::10f2::/64 On-link
14 281 fe80::/64 On-link
9 291 fe80::/64 On-link
9 291 fe80::/64 On-link
14 281 fe80::/64 On-link
1 331 ::::/32 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 10.0.19044.2005]
(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-VIIRONKA:49671  ESTABLISHED 7552
TCP    127.0.0.1:49671          LAPTOP-VIIRONKA:49670  ESTABLISHED 7552
TCP    127.0.0.1:49674          LAPTOP-VIIRONKA:49675  ESTABLISHED 7552
TCP    127.0.0.1:49675          LAPTOP-VIIRONKA:49674  ESTABLISHED 7552
TCP    127.0.0.1:58304          LAPTOP-VIIRONKA:58305  ESTABLISHED 16936
TCP    127.0.0.1:58305          LAPTOP-VIIRONKA:58304  ESTABLISHED 16936
TCP    127.0.0.1:58306          LAPTOP-VIIRONKA:58307  ESTABLISHED 16936
TCP    127.0.0.1:58307          LAPTOP-VIIRONKA:58306  ESTABLISHED 16936
TCP    127.0.0.1:58308          LAPTOP-VIIRONKA:58309  ESTABLISHED 16936
TCP    127.0.0.1:58309          LAPTOP-VIIRONKA:58308  ESTABLISHED 16936
TCP    127.0.0.1:58310          LAPTOP-VIIRONKA:58311  ESTABLISHED 16936
TCP    127.0.0.1:58311          LAPTOP-VIIRONKA:58310  ESTABLISHED 16936
TCP    127.0.0.1:58312          LAPTOP-VIIRONKA:58313  ESTABLISHED 16936
TCP    127.0.0.1:58313          LAPTOP-VIIRONKA:58312  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] [-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 10.0.19044.2001]
(c) Microsoft Corporation. All rights reserved.

C:\Users\virip>arp -a

Interface: 192.168.29.195 --- 0x9
Internet Address      Physical Address      Type
192.168.29.1         08-da-0c-51-e6-43     dynamic
192.168.29.11        00-c0-3c-3c-c0-da     dynamic
192.168.29.255       ff-ff-ff-ff-ff-ff     static
224.0.0.252          01-00-5e-00-00-00-00 static
224.0.0.251          01-00-5e-00-00-00-00 static
224.0.0.252          01-00-5e-00-00-00-00 static
239.255.255.250      01-00-5e-7f-ff-fa     static

Interface: 192.168.56.1 --- 0x0
Internet Address      Physical Address      Type
224.0.0.252          01-00-5e-00-00-00-00 static
224.0.0.251          01-00-5e-00-00-00-00 static
224.0.0.252          01-00-5e-00-00-00-00 static
239.255.255.250      01-00-5e-7f-ff-fa     static

C:\Users\virip>
```

- 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\virip>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 17:18:53

RSOP data for LAPTOP-VIIR0NKA\virip on LAPTOP-VIIR0NKA : Logging Mode
-----
OS Configuration:      Standalone Workstation
OS Version:             10.0.19044
Site Name:              N/A
Roaming Profile:        N/A
Local Profile:          C:\Users\virip
Connected over a slow link?: No

USER SETTINGS
-----

Last time Group Policy was applied: 02-10-2022 at 18:18:14
Group Policy was applied from: N/A
Group Policy slow link threshold: 500 kbps
Domain Name:            LAPTOP-VIIR0NKA
Domain Type:            <Local Computer>

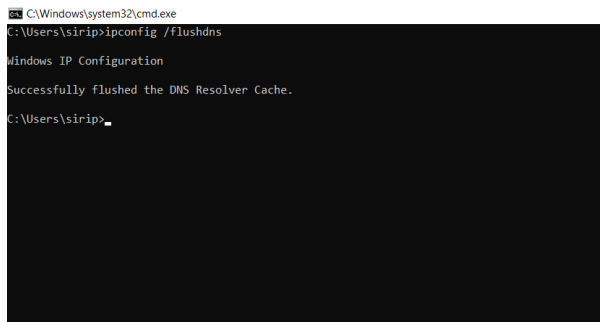
Applied Group Policy Objects
-----
N/A

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
viriparapsparshika@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



```
C:\Windows\system32\cmd.exe
C:\Users\sirip>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

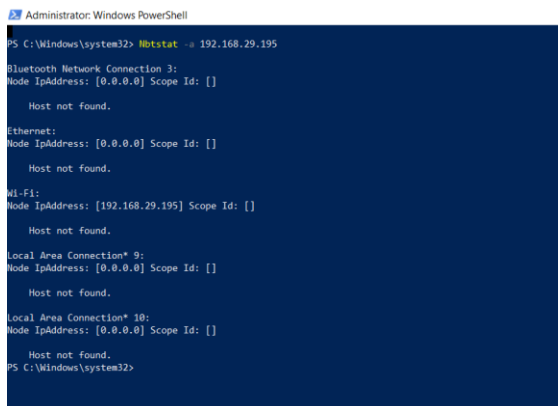
C:\Users\sirip>
```

- **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.



```
Administrator: Windows PowerShell

PS C:\Windows\system32> nbtstat -a 192.168.29.195

Bluetooth Network Connection 3:
Node IpAddress: [0.0.0.0] Scope Id: []

Host not found.

Ethernet:
Node IpAddress: [0.0.0.0] Scope Id: []

Host not found.

Wi-Fi:
Node IpAddress: [192.168.29.195] Scope Id: []

Host not found.

Local Area Connection* 0:
Node IpAddress: [0.0.0.0] Scope Id: []

Host not found.

Local Area Connection* 10:
Node IpAddress: [0.0.0.0] Scope Id: []

Host not found.

PS C:\Windows\system32>
```

- **nbtstat -R**

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

```
C:\Windows\system32\cmd.exe
C:\Users\sirip>nbtstat -R
Failed to Purge the NBT Remote Cache Table.
Failed to Purge the NBT Remote Cache Table.
Failed to Purge the NBT Remote Cache Table.
Failed to Purge the NBT Remote Cache Table.
Failed to Purge the NBT Remote Cache Table.
Failed to Purge the NBT Remote Cache Table.
C:\Users\sirip>
```

- **nbtstat -n**

List locally registered NetBios names

```
C:\Windows\system32\cmd.exe
C:\Users\sirip>nbtstat -n
VirtualBox Host-Only Network:
Node IpAddress: [192.168.56.1] Scope Id: []

    NetBIOS Local Name Table

    Name                Type             Status
    -----
    LAPTOP-VI1R00K4<00>  UNIQUE           Registered
    WORKGROUP            <00>             GROUP           Registered
    LAPTOP-VI1R00K4<20>  UNIQUE           Registered

Ethernet:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache

Bluetooth Network Connection 3:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache

Wi-Fi:
Node IpAddress: [192.168.29.195] Scope Id: []

    NetBIOS Local Name Table

    Name                Type             Status
    -----
    LAPTOP-VI1R00K4<00>  UNIQUE           Registered
    WORKGROUP            <00>             GROUP           Registered
    LAPTOP-VI1R00K4<20>  UNIQUE           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

C:\Users\sirip>
```

- **nbtstat-r**

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

```
C:\Windows\system32\cmd.exe
C:\Users\sirip>nbtstat -r

NetBIOS Names Resolution and Registration Statistics
-----

Resolved By Broadcast      = 0
Resolved By Name Server    = 0

Registered By Broadcast    = 78
Registered By Name Server  = 0

C:\Users\sirip>
```

- **netstat -ab**

Executable involved in creating each connection or listening port

```
Administrator: Windows PowerShell
C:\Windows\system32\cmd.exe
C:\Windows\system32>netstat -ab

Active Connections
[...]
```

- **netstat-an**

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

C:\Windows\system32\netstat -s		Administrator: Windows PowerShell	
Active Connections			
Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:*	LISTENING
TCP	0.0.0.0:445	0.0.0.0:*	LISTENING
TCP	0.0.0.0:1040	0.0.0.0:*	LISTENING
TCP	0.0.0.0:1157	0.0.0.0:*	LISTENING
TCP	0.0.0.0:4646	0.0.0.0:*	LISTENING
TCP	0.0.0.0:49664	0.0.0.0:*	LISTENING
TCP	0.0.0.0:49665	0.0.0.0:*	LISTENING
TCP	0.0.0.0:49666	0.0.0.0:*	LISTENING
TCP	0.0.0.0:49667	0.0.0.0:*	LISTENING
TCP	0.0.0.0:49668	0.0.0.0:*	LISTENING
TCP	0.0.0.0:49669	0.0.0.0:*	LISTENING
TCP	127.0.0.1:5199	0.0.0.0:*	LISTENING
TCP	127.0.0.1:49670	0.0.0.0:*	ESTABLISHED
TCP	127.0.0.1:49671	127.0.0.1:49670	ESTABLISHED
TCP	127.0.0.1:49674	127.0.0.1:49675	ESTABLISHED
TCP	127.0.0.1:49675	127.0.0.1:49674	ESTABLISHED
TCP	127.0.0.1:50384	127.0.0.1:50385	ESTABLISHED
TCP	127.0.0.1:50386	127.0.0.1:50387	ESTABLISHED
TCP	127.0.0.1:50388	127.0.0.1:50389	ESTABLISHED
TCP	127.0.0.1:50389	127.0.0.1:50388	ESTABLISHED
TCP	127.0.0.1:50390	127.0.0.1:50391	ESTABLISHED
TCP	127.0.0.1:50391	127.0.0.1:50390	ESTABLISHED
TCP	127.0.0.1:50392	127.0.0.1:50393	ESTABLISHED
TCP	127.0.0.1:50393	127.0.0.1:50392	ESTABLISHED
TCP	127.0.0.1:50394	127.0.0.1:50395	ESTABLISHED
TCP	127.0.0.1:50395	127.0.0.1:50394	ESTABLISHED
TCP	127.0.0.1:50396	127.0.0.1:50397	ESTABLISHED
TCP	127.0.0.1:50397	127.0.0.1:50396	ESTABLISHED
TCP	127.0.0.1:50398	127.0.0.1:50399	ESTABLISHED
TCP	127.0.0.1:50399	127.0.0.1:50398	ESTABLISHED
TCP	127.0.0.1:50400	127.0.0.1:50401	ESTABLISHED
TCP	127.0.0.1:50401	127.0.0.1:50400	ESTABLISHED
TCP	127.0.0.1:50402	127.0.0.1:50403	ESTABLISHED
TCP	127.0.0.1:50403	127.0.0.1:50402	ESTABLISHED
TCP	127.0.0.1:50404	127.0.0.1:50405	ESTABLISHED
TCP	127.0.0.1:50405	127.0.0.1:50404	ESTABLISHED
TCP	127.0.0.1:50406	127.0.0.1:50407	ESTABLISHED
TCP	127.0.0.1:50407	127.0.0.1:50406	ESTABLISHED
TCP	127.0.0.1:50408	127.0.0.1:50409	ESTABLISHED
TCP	127.0.0.1:50409	127.0.0.1:50408	ESTABLISHED
TCP	127.0.0.1:50410	127.0.0.1:50411	ESTABLISHED
TCP	127.0.0.1:50411	127.0.0.1:50410	ESTABLISHED
TCP	127.0.0.1:50412	127.0.0.1:50413	ESTABLISHED
TCP	127.0.0.1:50413	127.0.0.1:50412	ESTABLISHED
TCP	127.0.0.1:50414	127.0.0.1:50415	ESTABLISHED
TCP	127.0.0.1:50415	127.0.0.1:50414	ESTABLISHED
TCP	127.0.0.1:50416	127.0.0.1:50417	ESTABLISHED
TCP	127.0.0.1:50417	127.0.0.1:50416	ESTABLISHED
TCP	127.0.0.1:50418	127.0.0.1:50419	ESTABLISHED
TCP	127.0.0.1:50419	127.0.0.1:50418	ESTABLISHED
TCP	127.0.0.1:50420	127.0.0.1:50421	ESTABLISHED
TCP	127.0.0.1:50421	127.0.0.1:50420	ESTABLISHED
TCP	127.0.0.1:50422	127.0.0.1:50423	ESTABLISHED
TCP	127.0.0.1:50423	127.0.0.1:50422	ESTABLISHED
TCP	127.0.0.1:50424	127.0.0.1:50425	ESTABLISHED
TCP	127.0.0.1:50425	127.0.0.1:50424	ESTABLISHED
TCP	127.0.0.1:50426	127.0.0.1:50427	ESTABLISHED
TCP	127.0.0.1:50427	127.0.0.1:50426	ESTABLISHED
TCP	127.0.0.1:50428	127.0.0.1:50429	ESTABLISHED
TCP	127.0.0.1:50429	127.0.0.1:50428	ESTABLISHED
TCP	127.0.0.1:50430	127.0.0.1:50431	ESTABLISHED
TCP	127.0.0.1:50431	127.0.0.1:50430	ESTABLISHED
TCP	127.0.0.1:50432	127.0.0.1:50433	ESTABLISHED
TCP	127.0.0.1:50433	127.0.0.1:50432	ESTABLISHED
TCP	127.0.0.1:50434	127.0.0.1:50435	ESTABLISHED
TCP	127.0.0.1:50435	127.0.0.1:50434	ESTABLISHED
TCP	127.0.0.1:50436	127.0.0.1:50437	ESTABLISHED
TCP	127.		

- **netstat-an1 | find "15868"**

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

- **netstat-an1 | find “listening”**

Displays all the strings that contain “listening”

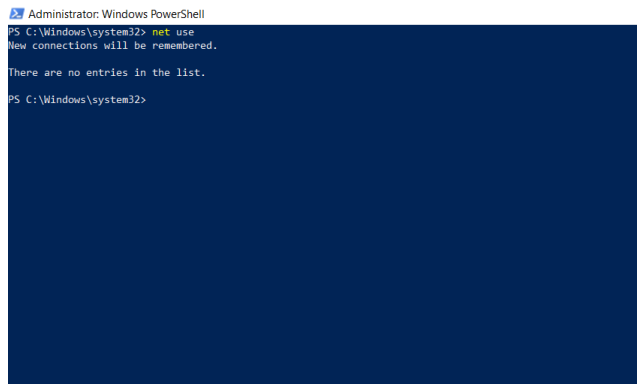
```
PS C:\Windows\system32> netstat -n | Select-String LISTENING
```

Protocol	Local Address	Foreign Address	State
TCP	0.0.0.0:8135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:8445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:8500	0.0.0.0:0	LISTENING
TCP	0.0.0.0:8537	0.0.0.0:0	LISTENING
TCP	0.0.0.0:8666	0.0.0.0:0	LISTENING
TCP	0.0.0.0:8968	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	127.0.0.1:5939	0.0.0.0:0	LISTENING
TCP	127.0.0.1:5980	0.0.0.0:0	LISTENING
TCP	127.0.0.1:5989	0.0.0.0:0	LISTENING
TCP	192.168.29.195:139	0.0.0.0:0	LISTENING
TCP	:::1335	:::1	LISTENING
TCP	:::1445	:::1	LISTENING
TCP	:::1567	:::1	LISTENING
TCP	:::49666	:::1	LISTENING
TCP	:::49665	:::1	LISTENING
TCP	:::49666	:::1	LISTENING
TCP	:::49667	:::1	LISTENING
TCP	:::49668	:::1	LISTENING
TCP	:::49669	:::1	LISTENING

```
PS C:\Windows\system32>
```

- **netuse:**

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



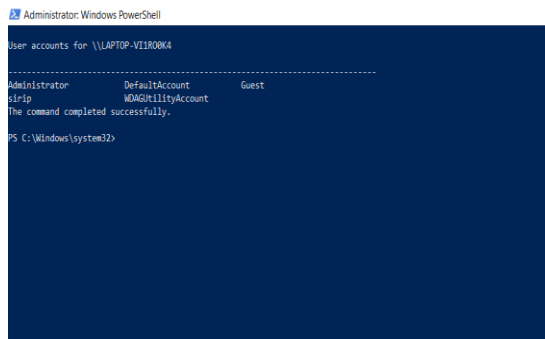
```
Administrator: Windows PowerShell
PS C:\Windows\system32> net use
New connections will be remembered.

There are no entries in the list.

PS C:\Windows\system32>
```

- **net user**

Displays list of the user's accounts on the computer



```
Administrator: Windows PowerShell

User accounts for \\LAPTOP-VI1R08K4

-----
Administrator          DefaultAccount          Guest
sirip                   WDAGUtilityAccount
The command completed successfully.

PS C:\Windows\system32>
```

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

```
Administrator: Windows PowerShell
PS C:\Windows\system32> net user Administrator
User name                Administrator
Full Name                Administrator
Comment                  Built-in account for administering the computer/domain
User's comment            Administrator
Country/region code      000 (System Default)
Account active            No
Account expires           Never
Password last set        02-10-2022 23:46:10
Password expires         Never
Password changeable      02-10-2022 23:46:10
Password required        Yes
User may change password Yes
Workstations allowed     All
Logon script             
User profile             
Home directory            C:\Users\Administrator
Last logon               08-09-2021 19:30:05
Logon hours allowed      All
Local Group Memberships  *Administrators
Global Group memberships *None
The command completed successfully.

PS C:\Windows\system32> net user /domain Administrator
The request will be processed at a domain controller for domain WORKGROUP.
System error 1355 has occurred.

The specified domain either does not exist or could not be contacted.
PS C:\Windows\system32>
```

- **net view/cache**

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

```
Administrator: Windows PowerShell
PS C:\Windows\system32> net view /ALL
System error 6118 has occurred.

The list of servers for this workgroup is not currently available
PS C:\Windows\system32> net view
System error 6118 has occurred.

The list of servers for this workgroup is not currently available
PS C:\Windows\system32>
```

- **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:\Windows\system32\cmd.exe
C:\Users\virgip>ping -a 192.168.29.195

Pinging LAPTOP-VI18MOKA [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\virgip>ping 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=3ms TTL=112
Reply from 8.8.8.8: bytes=32 time=4ms TTL=112
Reply from 8.8.8.8: bytes=32 time=4ms TTL=112
Reply from 8.8.8.8: bytes=32 time=4ms 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 = 3ms, Maximum = 4ms, Average = 3ms

C:\Users\virgip>
```

- **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:\Windows\system32\cmd.exe
C:\Users\slirip>tel 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
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 = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\Users\slirip>
```


- **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

```
C:\Windows\system32\cmd.exe
C:\Users\sirip>pathping 192.168.29.195

Tracing route to LAPTOP-VI1R00K4 [192.168.29.195]
over a maximum of 30 hops:
  0  LAPTOP-VI1R00K4 [192.168.29.195]
  1  LAPTOP-VI1R00K4 [192.168.29.195]

Computing statistics for 25 seconds...
Hop  RTT      Source to Here   This Node/Link   Address
 0      Lost/Sent = Pct  Lost/Sent = Pct  |
 0      0/ 100 = 0%      0/ 100 = 0%      | LAPTOP-VI1R00K4 [192.168.29.195]
 1  0ms      0/ 100 = 0%      0/ 100 = 0%      | LAPTOP-VI1R00K4 [192.168.29.195]

Trace complete.
C:\Users\sirip>
```

- **set-U**

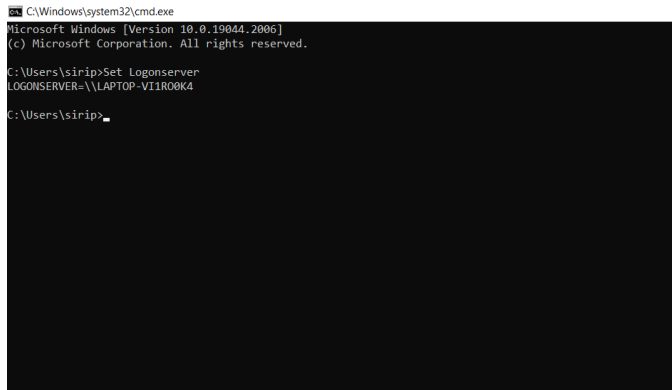
shows which user is logged in

```
C:\Windows\system32\cmd.exe
C:\Users\sirip>Set U
USERDOMAIN=LAPTOP-VI1R00K4
USERDOMAIN_ROAMINGPROFILE=LAPTOP-VI1R00K4
USERNAME=sirip
USERPROFILE=C:\Users\sirip

C:\Users\sirip>
```

- **set-logonserver:**

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



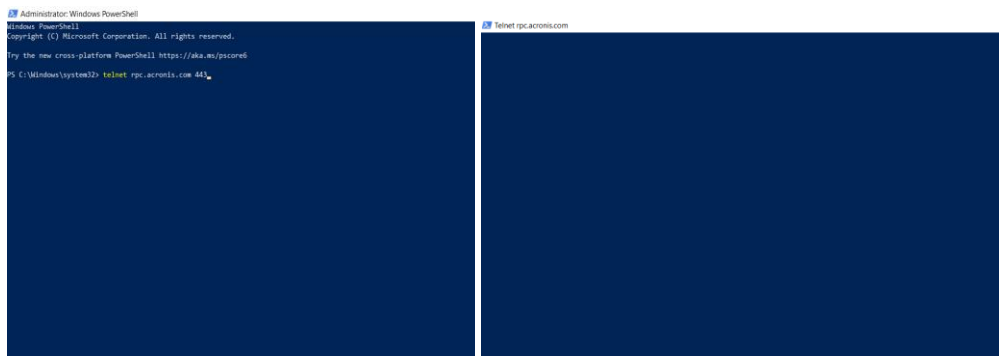
```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19044.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\sirip>Set Logonserver
LOGONSERVER=\\LAPTOP-VI1R08K4

C:\Users\sirip>
```

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

- Computer protocols that were built for interacting with remote computers
- Test connectivity to remote machine and issues commands through the keyboard.



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/powershell

PS C:\Windows\system32> telnet rpc.acronis.com 443_

Telnet: rpc.acronis.com
```

RESULT:

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

