21CY681– Internet Protocol lab

Name: Rahul Raj

Register Number: CYS22011

Title: Network Administration and Troubleshooting Using Windows Command Line Utilities.

Date of Assignment provided: 26/09/2022

Aim: To study more various Windows command-line utilities to perform troubleshooting in the network.

Tools Required: Command Prompt with administrative privileges,

---

PROCEDURE:

1. **ipconfig** – This command displays all the ip configuration details of the system

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19044.2130]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b1ee:a3cd:bd11:2216%18
   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:

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

Ethernet adapter Bluetooth Network Connection:

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

C:\Windows\system32>
```

2. Ipconfig /all – Displays full TCP/IP configuration for all the adapters

```
Administrator: Command Prompt
C:\Windows\system32>ipconfig/all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-PC2M5D2
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter
   Physical Address. . . . . . . . . : 0A-00-27-00-00-12
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::b1ee:a3cd:bd11:2216%18(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.56.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 822738983
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2A-D8-CC-84-EC-8E-B5-FB-12-0F
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   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. . . . . . . . . : 56-8C-A0-98-79-99
   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. . . . . . . . . : 54-8C-A0-98-79-99
   DHCP Enabled. . . . . . . . . . . : Yes
```

3. Ipconfig /renew [adapter_name] – This parameter renews an IPv4 address. For IPv6 we need to specify /renew6.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19044.2130]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig/renew

Windows IP Configuration

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

Ethernet adapter Ethernet:

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

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b1ee:a3cd:bd11:2216%18
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet 3:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2401:4900:629a:6cb3:88ae:cdc:7687:c8a3
   Temporary IPv6 Address. . . . . . : 2401:4900:629a:6cb3:99e0:51c9:af5:5f11
   Link-local IPv6 Address . . . . . : fe80::88ae:cdc:7687:c8a3%59
   IPv4 Address. . . . . . . . . . . : 192.168.10.135
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::7cb5:42ff:fe57:c190%59
                                       192.168.10.199

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:

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

Ethernet adapter Bluetooth Network Connection:

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

4. Ipconfig /flushdns - The /flushdns parameter will flush the DNS resolver cache. This can be useful when you are troubleshooting or when you want to get rid of defective or obsolete DNS records. The cache will be repopulated as you browse the Internet or during normal system activity.

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

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

5.Ipconfig /displaydns – This command displays the DNS resolver cache of your system.

Ipconfig /registerdns – It refreshes all DHCP leases and re-registers DNS names for all your system's network adapters. It might take some time for this to happen. It helps to resolve problems between your system and the DNS server.

ipconfig /showclassid <ADAPTER> - The /showclassid parameter will display the DHCP class ID for a specified adapter.

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

Windows IP Configuration


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.

C:\Windows\system32>ipconfig/showclassid

Error: unrecognized or incomplete command line.

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
                                        compartments
```

6. Ping <IP> is used to test and verify a IP of the computer network.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19044.2130]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>ping 192.168.56.1

Pinging 192.168.56.1 with 32 bytes of data:
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.56.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

7. Tracert IP is used to trace the route to

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19044.2130]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>tracert 192.168.56.1

Tracing route to DESKTOP-PC2M5D2 [192.168.56.1]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  DESKTOP-PC2M5D2 [192.168.56.1]

Trace complete.
```

8. Nslookup command can be used to get the configuration information of a DNS network. **Nslookup type –a** is used to specify a networks ip address.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19044.2130]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>nslookup google.com
Server:  UnKnown
Address:  192.168.10.199

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4007:828::200e
          142.250.196.174
```

9. Nslookup type soa command gives the information of primary mail server, mail address, the expiry of the number etc.

```
C:\Windows\system32>nslookup -type=soa google.com
Server:  UnKnown
Address:  192.168.10.199

Non-authoritative answer:
google.com
        primary name server = ns1.google.com
        responsible mail addr = dns-admin.google.com
        serial  = 483625360
        refresh = 900 (15 mins)
        retry   = 900 (15 mins)
        expire  = 1800 (30 mins)
        default TTL = 60 (1 min)
```

```
C:\Windows\system32>nslookup -type=a google.com
Server:  UnKnown
Address:  192.168.10.199

Non-authoritative answer:
Name:    google.com
Address:  142.250.196.174
```

10. Netstat command is used to know the current update of the network

```
C:\Windows\system32>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.10.135:50842   20.198.118.190:https   ESTABLISHED
  TCP    192.168.10.135:50847   20.189.173.10:https    ESTABLISHED
  TCP    [2409:4072:987:a87d:7c1e:fa3c:fa0d:a0e6]:50848  g2600-140f-0400-01ac-0000-0000-0000-3114:http  ESTABLISHED
  TCP    [2409:4072:987:a87d:7c1e:fa3c:fa0d:a0e6]:50849  g2600-140f-0400-01ac-0000-0000-0000-3114:http  ESTABLISHED
```

11. Arp –a command is used to map IP addresss with their repective MAC address.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19044.2130]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>arp -a

Interface: 192.168.56.1 --- 0x12
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 192.168.10.135 --- 0x3b
  Internet Address      Physical Address      Type
  192.168.10.199        1a-1c-bb-69-0b-2a     dynamic
  192.168.10.255        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
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

12. Gpresult displays the resulting set of policy settings on the computer.

```
Administrator: Command Prompt

C:\Windows\system32>gpresult

GPRESULT [/S system [/U username [/P [password]]]] [/SCOPE scope]
           [/USER targetusername] [/R | /V | /Z]

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

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

    /U        [domain\]user    Specifies the user context under which the
                               command should run.
    /P        [password]       Specifies the password for the given user
                               context. Prompts for input if omitted.
    /SCOPE    scope            Specifies whether the user or the
                               computer settings need to be displayed.
                               Valid values: "USER", "COMPUTER".

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

    /R                         Displays RSoP summary data.

    /V                         Specifies that verbose information should
                               be displayed. Verbose information provides
                               additional detailed settings that have
                               been applied with a precedence of 1.

    /Z                         Specifies that the super-verbose
                               information should be displayed. Super-
                               verbose information provides additional
                               detailed settings that have been applied
                               with a precedence of 1 and higher. This
                               allows you to see if a setting was set in
                               multiple places. See the Group Policy
                               online help topic for more information.

    /?                         Displays this help message.
```

13. Nbstat –a is used to display protocol settings and shows different commands and their uses.

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

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

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

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

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

14. Nbstat ip is used to

```
C:\Windows\system32>nbtstat -a 192.168.56.1

Ethernet 2:
Node IpAddress: [192.168.56.1] Scope Id: []

    Host not found.

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

    Host not found.

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

    Host not found.

Wi-Fi:
Node IpAddress: [0.0.0.0] Scope Id: []

    Host not found.

Local Area Connection* 1:
Node IpAddress: [0.0.0.0] Scope Id: []

    Host not found.

Local Area Connection* 2:
Node IpAddress: [0.0.0.0] Scope Id: []

    Host not found.

Ethernet 3:
Node IpAddress: [192.168.10.135] Scope Id: []

    Host not found.
```

15. Nbstat- R is used to purge and preload the Remote Cache Name table. **Nbstat –r** is used for detecting errors in WINS.

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

C:\Windows\system32>nbtstat -r

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

    Resolved By Broadcast     = 0
    Resolved By Name Server   = 0

    Registered By Broadcast   = 39
    Registered By Name Server = 0
```

16. Nbstat –n is used to list the BIOS names

```
Select Administrator: Command Prompt
C:\Windows\system32>nbtstat -n

Ethernet 2:
Node IpAddress: [192.168.56.1] Scope Id: []

                NetBIOS Local Name Table

       Name               Type         Status
    ---------------------------------------------
    DESKTOP-PC2M5D2<20>  UNIQUE      Registered
    DESKTOP-PC2M5D2<00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered

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

    No names in cache

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

    No names in cache

Wi-Fi:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache

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

Ethernet 3:
Node IpAddress: [192.168.10.135] Scope Id: []

                NetBIOS Local Name Table

       Name               Type         Status
    ---------------------------------------------
    DESKTOP-PC2M5D2<20>  UNIQUE      Registered
    DESKTOP-PC2M5D2<00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered
```

.

17. Netstat –ab is used to show network status.

```
Select Administrator: Command Prompt
Microsoft Windows [Version 10.0.19044.2130]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>netstat -ab

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            DESKTOP-PC2M5D2:0      LISTENING
  RpcSs
 [svchost.exe]
  TCP    0.0.0.0:445            DESKTOP-PC2M5D2:0      LISTENING
 Can not obtain ownership information
  TCP    0.0.0.0:5040           DESKTOP-PC2M5D2:0      LISTENING
  CDPSvc
 [svchost.exe]
  TCP    0.0.0.0:5357           DESKTOP-PC2M5D2:0      LISTENING
 Can not obtain ownership information
  TCP    0.0.0.0:49664          DESKTOP-PC2M5D2:0      LISTENING
 [lsass.exe]
  TCP    0.0.0.0:49665          DESKTOP-PC2M5D2:0      LISTENING
 Can not obtain ownership information
  TCP    0.0.0.0:49666          DESKTOP-PC2M5D2:0      LISTENING
  EventLog
 [svchost.exe]
  TCP    0.0.0.0:49667          DESKTOP-PC2M5D2:0      LISTENING
  Schedule
 [svchost.exe]
  TCP    0.0.0.0:49668          DESKTOP-PC2M5D2:0      LISTENING
 [spoolsv.exe]
  TCP    0.0.0.0:49670          DESKTOP-PC2M5D2:0      LISTENING
 Can not obtain ownership information
  TCP    192.168.10.135:139     DESKTOP-PC2M5D2:0      LISTENING
 Can not obtain ownership information
  TCP    192.168.10.135:50937   20.198.119.84:https    ESTABLISHED
  WpnService
 [svchost.exe]
  TCP    192.168.10.135:50940   204.79.197.222:https   TIME_WAIT
  TCP    192.168.10.135:50947   13.107.42.254:https    ESTABLISHED
 [SearchApp.exe]
  TCP    192.168.10.135:50949   204.79.197.222:https   ESTABLISHED
 [SearchApp.exe]
  TCP    192.168.56.1:139       DESKTOP-PC2M5D2:0      LISTENING
 Can not obtain ownership information
```

18. Netstat an is used to display protocol statistics and current TCP/IP network connections.

```
Administrator: Command Prompt
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>netstat an

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.
```

19. Pathping is used to measure the quality of network connections.

Set U is used to shows the name of the user logged in.

Set L is used to show the log on server

Ping –a <IP> is used to resolve IP to hostname.

```
C:\Windows\system32>pathping

Usage: pathping [-g host-list] [-h maximum_hops] [-i address] [-n]
                [-p period] [-q num_queries] [-w timeout]
                [-4] [-6] target_name

Options:
    -g host-list     Loose source route along host-list.
    -h maximum_hops  Maximum number of hops to search for target.
    -i address       Use the specified source address.
    -n               Do not resolve addresses to hostnames.
    -p period        Wait period milliseconds between pings.
    -q num_queries   Number of queries per hop.
    -w timeout       Wait timeout milliseconds for each reply.
    -4               Force using IPv4.
    -6               Force using IPv6.

C:\Windows\system32>set u
USERDOMAIN=DESKTOP-PC2M5D2
USERDOMAIN_ROAMINGPROFILE=DESKTOP-PC2M5D2
USERNAME=HP
USERPROFILE=C:\Users\HP

C:\Windows\system32>set l
LOCALAPPDATA=C:\Users\HP\AppData\Local
LOGONSERVER=\\DESKTOP-PC2M5D2

C:\Windows\system32>ping -a 192.168.56.1

Pinging DESKTOP-PC2M5D2 [192.168.56.1] with 32 bytes of data:
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.56.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

20. Netstat –an|find"LISTENING" is used to show the open ports with opening status.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19044.2130]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>netstat -an|find "LISTENING"
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING
  TCP    192.168.10.135:139     0.0.0.0:0              LISTENING
  TCP    192.168.56.1:139       0.0.0.0:0              LISTENING
  TCP    [::]:135               [::]:0                 LISTENING
  TCP    [::]:445               [::]:0                 LISTENING
  TCP    [::]:5357              [::]:0                 LISTENING
  TCP    [::]:49664             [::]:0                 LISTENING
  TCP    [::]:49665             [::]:0                 LISTENING
  TCP    [::]:49666             [::]:0                 LISTENING
  TCP    [::]:49667             [::]:0                 LISTENING
  TCP    [::]:49668             [::]:0                 LISTENING
  TCP    [::]:49670             [::]:0                 LISTENING
```

21. Netstat –s displays the IPv4, IPv6, IOPv4, IOPv6 and TCP statistics.

```
Select Administrator: Command Prompt

TCP Statistics for IPv4

  Active Opens                        = 2372
  Passive Opens                       = 66
  Failed Connection Attempts          = 861
  Reset Connections                   = 558
  Current Connections                 = 0
  Segments Received                   = 142204
  Segments Sent                       = 94136
  Segments Retransmitted              = 2687

TCP Statistics for IPv6

  Active Opens                        = 681
  Passive Opens                       = 22
  Failed Connection Attempts          = 302
  Reset Connections                   = 115
  Current Connections                 = 0
  Segments Received                   = 51367
  Segments Sent                       = 37993
  Segments Retransmitted              = 993

UDP Statistics for IPv4

  Datagrams Received    = 86176
  No Ports              = 130
  Receive Errors        = 1605
  Datagrams Sent        = 26708

UDP Statistics for IPv6

  Datagrams Received    = 96302
  No Ports              = 470
  Receive Errors        = 4
  Datagrams Sent        = 29511

C:\Windows\system32>
```

```
Select Administrator: Command Prompt
C:\Windows\system32>netstat -s

IPv4 Statistics

  Packets Received                   = 225964
  Received Header Errors             = 0
  Received Address Errors            = 8
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 0
  Received Packets Discarded         = 1722
  Received Packets Delivered         = 230268
  Output Requests                    = 125074
  Routing Discards                   = 0
  Discarded Output Packets           = 205
  Output Packet No Route             = 42
  Reassembly Required                = 0
  Reassembly Successful              = 0
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 0
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 0

IPv6 Statistics

  Packets Received                   = 144575
  Received Header Errors             = 0
  Received Address Errors            = 138
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 0
  Received Packets Discarded         = 474
  Received Packets Delivered         = 145090
  Output Requests                    = 68105
  Routing Discards                   = 0
  Discarded Output Packets           = 13
  Output Packet No Route             = 0
  Reassembly Required                = 0
  Reassembly Successful              = 0
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 0
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 0
```

```
Select Administrator: Command Prompt
ICMPv4 Statistics

                            Received    Sent
  Messages                  111         162
  Errors                    0           0
  Destination Unreachable   89          140
  Time Exceeded             0           0
  Parameter Problems        0           0
  Source Quenches           0           0
  Redirects                 0           0
  Echo Replies              11          11
  Echos                     11          11
  Timestamps                0           0
  Timestamp Replies         0           0
  Address Masks             0           0
  Address Mask Replies      0           0
  Router Solicitations      0           0
  Router Advertisements     0           0

ICMPv6 Statistics

                            Received    Sent
  Messages                  288         491
  Errors                    0           0
  Destination Unreachable   3           157
  Packet Too Big            0           0
  Time Exceeded             0           0
  Parameter Problems        0           0
  Echos                     0           0
  Echo Replies              0           0
  MLD Queries               0           0
  MLD Reports               0           0
  MLD Dones                 0           0
  Router Solicitations      0           33
  Router Advertisements     45          0
  Neighbor Solicitations    140         136
  Neighbor Advertisements   100         165
  Redirects                 0           0
  Router Renumberings       0           0
```

22. Ping <IP> -f is used for fragmentation with 32 bytes of data.

```
C:\Windows\system32>ping 192.168.56.1 -f

Pinging 192.168.56.1 with 32 bytes of data:
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.56.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

23. Netstat –o is used to display TCP connections and Process ID(PID)

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

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    127.0.0.1:54132        DESKTOP-PC2M5D2:wsd    TIME_WAIT       0
  TCP    192.168.10.135:54134   13.107.4.52:http       TIME_WAIT       0
  TCP    192.168.10.135:54135   20.198.119.84:https    SYN_SENT        6352
  TCP    192.168.10.135:54136   20.189.173.9:https     ESTABLISHED     4456
  TCP    192.168.10.135:54138   40.74.108.123:https    FIN_WAIT_1      4456
  TCP    192.168.10.135:54139   1drv:https             ESTABLISHED     6352
  TCP    192.168.10.135:54140   20.198.119.84:https    SYN_SENT        4800
  TCP    192.168.10.135:54141   1drv:https             ESTABLISHED     6352
  TCP    192.168.10.135:54142   1drv:https             ESTABLISHED     6352
  TCP    [::1]:54133            DESKTOP-PC2M5D2:wsd    TIME_WAIT       0
  TCP    [::1]:54137            DESKTOP-PC2M5D2:wsd    TIME_WAIT       0
  TCP    [2401:4900:629a:6cb3:99e0:51c9:af5:5f11]:54144  [2600:1901:1:c36::]:https  ESTABLISHED     11664
  TCP    [2401:4900:629a:6cb3:99e0:51c9:af5:5f11]:54158  g2600-140f-f400-0000-0000-0000-1730-e21a:https  ESTABLISHED     9372
  TCP    [2401:4900:629a:6cb3:99e0:51c9:af5:5f11]:54159  [2620:1ec:c11::200]:https  ESTABLISHED     9372
  TCP    [2401:4900:629a:6cb3:99e0:51c9:af5:5f11]:54165  g2600-140f-2400-0182-0000-0000-0000-1011:https  ESTABLISHED     9372
  TCP    [2401:4900:629a:6cb3:99e0:51c9:af5:5f11]:54166  [2603:1030:805:3::46]:https  ESTABLISHED     11536
  TCP    [2401:4900:629a:6cb3:99e0:51c9:af5:5f11]:54170  https-2402-6800-760-a000--8000:http  TIME_WAIT       0
```

24. Netstat –r displays the contents of IP routing table.

```
Administrator: Command Prompt

C:\Windows\system32>netstat -r
===========================================================================
Interface List
  7...ec 8e b5 fb 12 0f ......Realtek PCIe FE Family Controller
 18...0a 00 27 00 00 12 ......VirtualBox Host-Only Ethernet Adapter
 59...46 e1 32 b8 ec cd ......Remote NDIS based Internet Sharing Device
 17...56 8c a0 98 79 99 ......Microsoft Wi-Fi Direct Virtual Adapter
  8...54 8c a0 98 79 99 ......Microsoft Wi-Fi Direct Virtual Adapter #2
  9...54 8c a0 98 79 99 ......Realtek RTL8723BE 802.11 bgn Wi-Fi Adapter
  5...54 8c a0 98 79 9a ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0   192.168.10.199   192.168.10.135     25
        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
      192.168.10.0    255.255.255.0         On-link    192.168.10.135    281
    192.168.10.135  255.255.255.255         On-link    192.168.10.135    281
    192.168.10.255  255.255.255.255         On-link    192.168.10.135    281
      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    192.168.10.135    281
  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    192.168.10.135    281
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
 59     41 ::/0                     fe80::7cb5:42ff:fe57:c190
  1    331 ::1/128                  On-link
 59     41 2401:4900:629a:6cb3::/64 On-link
 59    281 2401:4900:629a:6cb3:88ae:cdc:7687:c8a3/128
                                    On-link
 59    281 2401:4900:629a:6cb3:99e0:51c9:af5:5f11/128
                                    On-link
 18    281 fe80::/64                On-link
 59    281 fe80::/64                On-link
 59    281 fe80::88ae:cdc:7687:c8a3/128
                                    On-link
 18    281 fe80::b1ee:a3cd:bd11:2216/128
                                    On-link
  1    331 ff00::/8                 On-link
 18    281 ff00::/8                 On-link
 59    281 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

25. Net user is used to show user for the computer.

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

User accounts for \\DESKTOP-PC2M5D2

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

26. Net user/domain specifies computer available in specific domain.

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

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