

Mohamed Arsath
CSE(CYBER SECURITY)

BASIC NETWORKING COMMAND IN WINDOWS.

- **IPCONFIG**

The IPCONFIG network command provides a comprehensive view of information regarding the IP address configuration of the device we are currently working on.

Command to enter in Prompt – ipconfig

```
C:\Users\Lenovo>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::6730:5879:147c:7b94%9
    IPv4 Address. . . . . : 172.16.52.177
    Subnet Mask . . . . . : 255.255.252.0
    Default Gateway . . . . . : 172.16.52.1
```

- **NSLOOKUP**

The NSLOOKUP command is used to troubleshoot network connectivity issues in the system. Using the nslookup command, we can access the information related to our system's DNS server, i.e., domain name and IP address.

Command to enter in Prompt – nslookup

```
C:\Users\Lenovo>nslookup
Default Server: UnKnown
Address: 172.16.52.1

> www.google.com
Server: UnKnown
Address: 172.16.52.1

Non-authoritative answer:
Name: www.google.com
Addresses: 2404:6800:4007:819::2004
          142.250.182.4
```

- **HOSTNAME**

The HOSTNAME command displays the hostname of the system. The hostname command is much easier to use than going into the system settings to search for it.

Command to enter in Prompt - hostname

```
C:\Users\Lenovo>HOSTNAME
HDC0422230
C:\Users\Lenovo>
```

- **PING**

The Ping command is one of the most widely used commands in the prompt tool, as it allows the user to check the connectivity of our system to another host.

Command to enter in Prompt - ping www.destination_host_name.com

```
>
C:\Users\Lenovo>ping www.google.com

Pinging www.google.com [142.250.182.4] with 32 bytes of data:
Reply from 142.250.182.4: bytes=32 time=3ms TTL=120
Reply from 142.250.182.4: bytes=32 time=3ms TTL=120
Reply from 142.250.182.4: bytes=32 time=3ms TTL=120
Reply from 142.250.182.4: bytes=32 time=3ms TTL=120

Ping statistics for 142.250.182.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 3ms, Average = 3ms
```

- **TRACERT**

The TRACERT command is used to trace the route during the transmission of the data packet over to the destination host and also provides us with the “hop” count during transmission.

Using the number of hops and the hop IP address, we can troubleshoot network issues and

identify the point of the problem during the transmission of the data packet. Command to enter in Prompt- tracert IP-address OR tracert www.destination_host_name.com

```
C:\Users\Lenovo>tracert www.google.com

Tracing route to www.google.com [142.250.182.4]
over a maximum of 30 hops:

  1  <1 ms    <1 ms    <1 ms    172.16.52.1
  2   3 ms     6 ms     3 ms     static-41.229.249.49-tataidc.co.in [49.249.229.41]
  3   3 ms     3 ms     2 ms     142.250.171.162
  4   5 ms     5 ms     5 ms     142.251.227.217
  5   3 ms     3 ms     3 ms     142.251.55.219
  6   3 ms     3 ms     3 ms     maa05s18-in-f4.1e100.net [142.250.182.4]

Trace complete.
```

- **NETSTAT**

The Netstat command as the name suggests displays an overview of all the network connections in the device. The table shows detail about the connection protocol, address, and the current state of the network.

Command to enter in Prompt - netstat

```
C:\Users\Lenovo>netstat
```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:49684	HDC0422230:49685	ESTABLISHED
TCP	127.0.0.1:49685	HDC0422230:49684	ESTABLISHED
TCP	127.0.0.1:49686	HDC0422230:49687	ESTABLISHED
TCP	127.0.0.1:49687	HDC0422230:49686	ESTABLISHED
TCP	172.16.52.177:23635	20.24.249.45:https	CLOSE_WAIT
TCP	172.16.52.177:23636	152.195.38.76:http	CLOSE_WAIT
TCP	172.16.52.177:24089	20.198.119.143:https	ESTABLISHED
TCP	172.16.52.177:24424	server-108-158-46-66:https	ESTABLISHED
TCP	172.16.52.177:24427	172.64.155.61:https	ESTABLISHED
TCP	172.16.52.177:24428	a23-201-220-154:https	ESTABLISHED
TCP	172.16.52.177:24429	a23-201-220-154:https	ESTABLISHED
TCP	172.16.52.177:24430	172.64.155.61:https	ESTABLISHED
TCP	172.16.52.177:24432	server-18-66-41-102:https	ESTABLISHED
TCP	172.16.52.177:24433	server-52-84-12-2:https	ESTABLISHED
TCP	172.16.52.177:24434	server-108-158-251-26:https	ESTABLISHED
TCP	172.16.52.177:24440	172.66.0.163:https	ESTABLISHED
TCP	172.16.52.177:24445	104.18.32.77:https	ESTABLISHED
TCP	172.16.52.177:24448	151.101.193.138:https	ESTABLISHED
TCP	172.16.52.177:24450	a23-223-244-177:https	CLOSE_WAIT
TCP	172.16.52.177:24451	a23-223-244-177:https	CLOSE_WAIT
TCP	172.16.52.177:24452	a23-223-244-177:https	CLOSE_WAIT
TCP	172.16.52.177:24453	a23-223-244-177:https	CLOSE_WAIT
TCP	172.16.52.177:24454	13.107.226.58:https	CLOSE_WAIT
TCP	172.16.52.177:24455	52.108.8.254:https	CLOSE_WAIT
TCP	172.16.52.177:24456	52.123.128.254:https	CLOSE_WAIT
TCP	172.16.52.177:24457	204.79.197.222:https	CLOSE_WAIT
TCP	172.16.52.177:24458	52.182.143.208:https	CLOSE_WAIT
TCP	172.16.52.177:24459	a23-223-244-88:https	CLOSE_WAIT
TCP	172.16.52.177:24460	a23-223-244-88:https	CLOSE_WAIT
TCP	172.16.52.177:24461	a23-223-244-88:https	CLOSE_WAIT
TCP	172.16.52.177:24462	a23-223-244-88:https	CLOSE_WAIT
TCP	172.16.52.177:24463	a23-223-244-88:https	CLOSE_WAIT
TCP	172.16.52.177:24465	a104-114-94-26:https	ESTABLISHED
TCP	172.16.52.177:24466	204.79.197.239:https	ESTABLISHED
TCP	172.16.52.177:24469	20.198.118.190:https	ESTABLISHED
TCP	[fe80::6730:5879:147c:7b94%9]:1521	HDC0422230:49688	ESTABLISHED
TCP	[fe80::6730:5879:147c:7b94%9]:49688	HDC0422230:1521	ESTABLISHED

- **ARP(Address Resolution Protocol)**

The ARP command is used to access the mapping structure of IP addresses to the MAC address. This provides us with a better understanding of the transmission of packets in the network channel.

Command to enter in Prompt – arp

```

C:\Users\Lenovo>arp

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

-a          Displays current ARP entries by interrogating the current
            protocol data. If inet_addr is specified, the IP and Physical
            addresses for only the specified computer are displayed. If
            more than one network interface uses ARP, entries for each ARP
            table are displayed.
-g          Same as -a.
-v          Displays current ARP entries in verbose mode. All invalid
            entries and entries on the loop-back interface will be shown.
inet_addr   Specifies an internet address.
-N if_addr  Displays the ARP entries for the network interface specified
            by if_addr.
-d          Deletes the host specified by inet_addr. inet_addr may be
            wildcarded with * to delete all hosts.
-s          Adds the host and associates the Internet address inet_addr
            with the Physical address eth_addr. The Physical address is
            given as 6 hexadecimal bytes separated by hyphens. The entry
            is permanent.
eth_addr    Specifies a physical address.
if_addr     If present, this specifies the Internet address of the
            interface whose address translation table should be modified.
            If not present, the first applicable interface will be used.

Example:
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Adds a static entry.
> arp -a .... Displays the arp table.

```

- **SYSTEMINFO**

Using the SYSTEMINFO command, we can access the system's hardware and software details, such as processor data, booting data, Windows version, etc.

Command to enter in Prompt – systeminfo


```

Host Name:                HDC0422230
OS Name:                  Microsoft Windows 11 Pro
OS Version:               10.0.22000 N/A Build 22000
OS Manufacturer:         Microsoft Corporation
OS Configuration:        Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:         Lenovo
Registered Organization:
Product ID:                00331-20000-73468-AA240
Original Install Date:     6/10/2022, 1:45:14 AM
System Boot Time:          8/5/2024, 3:49:29 PM
System Manufacturer:       LENOVO
System Model:              11QCS01V00
System Type:               x64-based PC
Processor(s):               1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 167 Stepping 1 GenuineIntel ~2592 Mhz
BIOS Version:              LENOVO M3GKT34A, 3/2/2022
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:              en-us;English (United States)
Input Locale:              00004009
Time Zone:                 (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory:     16,122 MB
Available Physical Memory: 11,017 MB
Virtual Memory: Max Size:  18,554 MB
Virtual Memory: Available: 11,061 MB
Virtual Memory: In Use:    7,493 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\HDC0422230
Hotfix(s):                  7 Hotfix(s) Installed.
                           [01]: KB5029717
                           [02]: KB5028014
                           [03]: KB5007575
                           [04]: KB5011048
                           [05]: KB5012170
                           [06]: KB5030217
                           [07]: KB5029782
Network Card(s):           1 NIC(s) Installed.
                           [01]: Realtek PCIe GbE Family Controller
                               Connection Name: Ethernet
                               DHCP Enabled:    No
                               IP address(es)
                                   [01]: 172.16.52.177
                                   [02]: fe80::6730:5879:147c:7b94
Hyper-V Requirements:      VM Monitor Mode Extensions: Yes
                           Virtualization Enabled In Firmware: Yes
                           Second Level Address Translation: Yes
                           Data Execution Prevention Available: Yes

```

- **ROUTE**

Provides the data of routing data packets in the system over the communication channel. Command to enter in Prompt – route print

```
C:\Users\Lenovo>route print
```

```
=====
```

```
Interface List
```

```
  9...88 ae dd 12 c7 fc .....Realtek PCIe GbE Family Controller
  1.....Software Loopback Interface 1
```

```
=====
```

```
IPv4 Route Table
```

```
=====
```

```
Active Routes:
```

Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	172.16.52.1	172.16.52.177	281
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
172.16.52.0	255.255.252.0	On-link	172.16.52.177	281
172.16.52.177	255.255.255.255	On-link	172.16.52.177	281
172.16.55.255	255.255.255.255	On-link	172.16.52.177	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	172.16.52.177	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	172.16.52.177	281

```
=====
```

```
Persistent Routes:
```

Network Address	Netmask	Gateway Address	Metric
0.0.0.0	0.0.0.0	172.16.52.1	Default

```
=====
```

```
IPv6 Route Table
```

```
=====
```

```
Active Routes:
```

If	Metric	Network Destination	Gateway
1	331	::1/128	On-link
9	281	fe80::/64	On-link
9	281	fe80::6730:5879:147c:7b94/128	On-link
1	331	ff00::/8	On-link
9	281	ff00::/8	On-link

```
=====
```

```
Persistent Routes:
```

```
None
```