Name: Aarya Pandey
Registration No: 231071003
Batch C

CN Assignment 2
Study of Networking Commands

Aim: To study networking commands.

Theory:
Networking commands are the instructions used in command-line interfaces like Command Prompt, Terminal, or PowerShell. They are essential tools for managing, configuring, and troubleshooting network connections in computer systems.

Some of the networking commands are:

1. **hostname**

    - A hostname is used to identify or set the system's hostname. It is a name given to a computer attached to a network, and its main purpose is to uniquely identify it over a network.

    - `hostname -d` : Displays the domain name the machine belongs to. Returns nothing if no local domain is set.

    - `hostname -f` : Displays the fully qualified domain name (FQDN), which contains the short hostname and the DNS domain.

      `hostname -i` : Displays the IP address of the current machine. This is the address the machine uses to communicate over the network.

`2.ping`

The `ping` command checks connectivity between two systems over a network (by IP address or domain name). It works by sending ICMP (Internet Control Message Protocol) Echo Request packets to a destination and waiting for ICMP Echo Reply packets in return.

- `ping -c <number>` : Sends a specific number of ping requests.
- `ping <hostname>` : Example — `ping google.com`

This is used to check the connectivity between the computer and Google's server. It sends ICMP Echo Request packets to *google.com* and waits for replies.

The output returns:

- IP address of the server that responded successfully
- Size of each ICMP packet
- Round-trip time taken for the packet to reach the server and return
- TTL (Time To Live) — number of hops left before the packet would be discarded

---

3.ifconfig

`ifconfig` stands for *Interface Configuration*. It is used to view, configure, and manage network interfaces.

ifconfig

It provides information such as:

- IP address
- Subnet mask
- Broadcast address
- MAC address of each interface

It also shows network statistics like transmitted and received packets, errors, and dropped packets basically, it provides a comprehensive list of all network interfaces along with their respective addresses, MAC addresses, and other relevant details.

- `ifconfig -a` : Displays all interfaces, including those that are down.
- `ifconfig -s` : Displays a short list instead of detailed information.

4.netstat

`netstat` stands for *network statistics*. It allows users to display network-related information and diagnose various networking issues. It is used to display:

- Active network connections
- Routing tables
- Interface statistics
- Network protocol information

Common options:

2. `netstat -a` : Displays all connections.
3. `netstat -n` : Displays numerical addresses.
4. `netstat -r` : Shows the routing table.
5. `netstat -t` : Displays only TCP connections.
6. `netstat -u` : Displays only UDP connections.

5.nslookup

`nslookup` stands for *Name Server Lookup*. It is useful for getting information from the DNS server.
To find all the IP addresses for a given domain name, `nslookup` is used.
One must have a connection to the internet for this to be useful.

6.traceroute

This command is used to trace the route taken by packets from a source to a destination over an IP network.
It helps visualize the path taken by packets across the internet and can be useful for diagnosing network latency and routing issues.

Common options:

- `traceroute -m <max_hops>` : Sets the maximum number of hops.
- `traceroute -w <timeout>` : Sets the time (in seconds) to wait for a response from each hop.
- `traceroute -n` : Does not resolve IP addresses to domain names.
- `traceroute -p <port>` : Sets the destination port.

7.finger

This command is used by system administrators to retrieve detailed user information, including:

- Login name
- Full name
- Idle time
- Login time

Usage:

- `finger <username>` : Gets detailed information about a specific user.
- `finger -s <username>` : Provides a summary of the user's details, including idle status.
- `finger -p <username>` : Displays the login name, directory, login time, and email, but not the plan or project of the user.

8.telnet

This command allows logging in and communicating with a system through a TCP/IP network.

It is commonly used for testing network connectivity, diagnosing port issues, and interacting with services directly.

Note: Telnet transmits data in plaintext, making it insecure for sensitive operations. It has largely been replaced by more secure protocols like SSH.

9.nmap

This is frequently used for security audits to see what services are exposed on a host.

It is an excellent tool to identify potential vulnerabilities or unintended services running on a machine.

Screenshots :

Hostname

```
sysadmin@sysadmin:~$ hostname
sysadmin
sysadmin@sysadmin:~$ hostname -d
sysadmin@sysadmin:~$ hostname -f
sysadmin
sysadmin@sysadmin:~$ hostname -i
127.0.1.1
```

ping

```
sysadmin@sysadmin:~$ ping www.yahoo.com
PING me-ycpi-cf-www.g06.yahoodns.net (27.123.42.204) 56(84) bytes of data.
64 bytes from e1-ha.ycpi.ina.yahoo.com (27.123.42.204): icmp_seq=1 ttl=55 time=33.5 ms
64 bytes from e1-ha.ycpi.ina.yahoo.com (27.123.42.204): icmp_seq=2 ttl=55 time=30.6 ms
64 bytes from e1-ha.ycpi.ina.yahoo.com (27.123.42.204): icmp_seq=3 ttl=55 time=21.4 ms
64 bytes from e1-ha.ycpi.ina.yahoo.com (27.123.42.204): icmp_seq=4 ttl=55 time=31.1 ms
64 bytes from e1-ha.ycpi.ina.yahoo.com (27.123.42.204): icmp_seq=5 ttl=55 time=61.1 ms
64 bytes from e1-ha.ycpi.ina.yahoo.com (27.123.42.204): icmp_seq=6 ttl=55 time=121 ms
64 bytes from e1-ha.ycpi.ina.yahoo.com (27.123.42.204): icmp_seq=7 ttl=55 time=45.2 ms
^C
--- me-ycpi-cf-www.g06.yahoodns.net ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 8158ms
rtt min/avg/max/mdev = 21.375/49.151/121.126/31.679 ms
```

ifconfig

```
sysadmin@sysadmin:~$ ifconfig
eno1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 30:13:8b:f1:48:71  txqueuelen 1000  (Ethernet)
        RX packets 761095  bytes 69681728 (69.6 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 19680  bytes 1737777 (1.7 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19  memory 0x80a00000-80a20000

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 77511  bytes 6413883 (6.4 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 77511  bytes 6413883 (6.4 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.128  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::3d16:84f4:3629:f9af  prefixlen 64  scopeid 0x20<link>
        ether 28:d0:43:1e:82:e8  txqueuelen 1000  (Ethernet)
        RX packets 1018590  bytes 932406665 (932.4 MB)
        RX errors 0  dropped 21  overruns 0  frame 0
        TX packets 156101  bytes 71688062 (71.6 MB)
        TX errors 0  dropped 5 overruns 0  carrier 0  collisions 0
```

netstat

```
sysadmin@sysadmin:~$ netstat -nap | grep port
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
unix  3      [ ]         STREAM     CONNECTED     24441    3456/ibus-portal
unix  3      [ ]         STREAM     CONNECTED     20443    3456/ibus-portal
unix  3      [ ]         STREAM     CONNECTED     26098    3456/ibus-portal
unix  3      [ ]         STREAM     CONNECTED     29780    3456/ibus-portal
```

```
sysadmin@sysadmin:~$ netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:37965           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:58101           0.0.0.0:*               LISTEN
tcp        0      0 localhost:smtp          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:sunrpc          0.0.0.0:*               LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:44299           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:35831           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:nfs             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:59665           0.0.0.0:*               LISTEN
tcp        0      0 192.168.0.128:55638     bom12s16-in-f14.1:https ESTABLISHED
tcp        0      0 192.168.0.128:57620     93.243.107.34.bc.:https ESTABLISHED
```

```
sysadmin@sysadmin:~$ netstat --tcp
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.0.128:55638     bom12s16-in-f14.1:https ESTABLISHED
tcp        0      0 192.168.0.128:57620     93.243.107.34.bc.:https ESTABLISHED
```

```
sysadmin@sysadmin:~$ netstat --udp
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 192.168.0.128:bootpc    192.168.0.1:bootps      ESTABLISHED
```

```
sysadmin@sysadmin:~$ netstat -g
IPv6/IPv4 Group Memberships
Interface       RefCnt Group
--------------- ------ ---------------------
lo              1      mdns.mcast.net
lo              1      all-systems.mcast.net
eno1            1      all-systems.mcast.net
wlp2s0          1      mdns.mcast.net
wlp2s0          1      all-systems.mcast.net
lo              1      ff02::fb
lo              1      ip6-allnodes
lo              1      ff01::1
eno1            1      ip6-allnodes
eno1            1      ff01::1
wlp2s0          1      ff02::fb
wlp2s0          1      ff02::1:ff29:f9af
wlp2s0          1      ip6-allnodes
wlp2s0          1      ff01::1
```

nslookup

```
sysadmin@sysadmin:~$ nslookup google.com
;; communications error to 192.168.0.46#53: timed out
;; communications error to 192.168.0.46#53: timed out
;; communications error to 192.168.0.46#53: timed out
Server:         192.168.0.1
Address:        192.168.0.1#53

Non-authoritative answer:
Name:   google.com
Address: 142.251.42.238
;; communications error to 192.168.0.46#53: timed out
;; communications error to 192.168.0.46#53: timed out
;; communications error to 192.168.0.46#53: timed out
Name:   google.com
Address: 2404:6800:4009:802::200e
```

traceroute

```
sysadmin@sysadmin:~$ traceroute google.com
traceroute to google.com (142.251.220.46), 30 hops max, 60 byte packets
 1  192.168.0.1 (192.168.0.1)  97.848 ms  98.436 ms  98.674 ms
 2  172.18.38.1 (172.18.38.1)  99.089 ms  99.083 ms  99.078 ms
 3  172.18.35.2 (172.18.35.2)  98.877 ms  99.069 ms  99.065 ms
 4  14.139.108.49 (14.139.108.49)  99.196 ms  99.192 ms  101.616 ms
 5  10.152.23.5 (10.152.23.5)  105.941 ms  128.757 ms  106.158 ms
 6  10.152.7.38 (10.152.7.38)  128.748 ms  210.463 ms  4.484 ms
 7  10.152.8.66 (10.152.8.66)  4.682 ms  5.008 ms  5.003 ms
 8  * 72.14.204.62 (72.14.204.62)  5.750 ms *
 9  * * *
10  142.250.214.100 (142.250.214.100)  7.210 ms 216.239.46.136 (216.239.46.136)  6.991 ms 142.250.235.10 (142.250.235.10)  7.441 ms
11  192.178.110.206 (192.178.110.206)  9.924 ms  34.707 ms 192.178.110.108 (192.178.110.108)  7.185 ms
12  142.250.209.71 (142.250.209.71)  8.736 ms^C
```

finger

```
sysadmin@sysadmin:~$ finger
finger: /dev//seat0: No such file or directory
Login     Name       Tty      Idle  Login Time   Office     Office Phone
sysadmin  sysadmin   seat0          Aug  4 13:32 (login screen)
sysadmin  sysadmin   tty2    22:39  Aug  4 13:32 (tty2)
```