FILZA SAFDAR

TASK 4 REPORT:
Networks Commands Documentation (WINDOWS/LINUX)

TASK:04

FILZA SAFDAR

1. Introduction

Network commands are used to configure, test, and troubleshoot computer networks.
This document explains commonly used Windows and Linux network commands, their syntax, usage, and sample outputs.

Linux Commands:

ping

In Linux, the ping command works the same way as in Windows. It checks whether a system or website is reachable over the network. It is commonly used to test internet connectivity and network stability.

```
┌──(filza㉿Filza)-[~]
└─$ ping google.com
PING google.com (142.250.187.78) 56(84) bytes of data.
64 bytes from pnfjra-ao-in-f14.1e100.net (142.250.187.78): icmp_seq=1 ttl=115 time=22.7 ms
64 bytes from pnfjra-ao-in-f14.1e100.net (142.250.187.78): icmp_seq=2 ttl=115 time=24.3 ms
64 bytes from pnfjra-ao-in-f14.1e100.net (142.250.187.78): icmp_seq=3 ttl=115 time=22.5 ms
64 bytes from pnfjra-ao-in-f14.1e100.net (142.250.187.78): icmp_seq=4 ttl=115 time=23.9 ms
64 bytes from pnfjra-ao-in-f14.1e100.net (142.250.187.78): icmp_seq=5 ttl=115 time=23.1 ms
64 bytes from pnfjra-ao-in-f14.1e100.net (142.250.187.78): icmp_seq=6 ttl=115 time=22.4 ms
64 bytes from pnfjra-ao-in-f14.1e100.net (142.250.187.78): icmp_seq=7 ttl=115 time=22.9 ms
64 bytes from pnfjra-ao-in-f14.1e100.net (142.250.187.78): icmp_seq=8 ttl=115 time=23.9 ms
64 bytes from pnfjra-ao-in-f14.1e100.net (142.250.187.78): icmp_seq=9 ttl=115 time=22.9 ms
64 bytes from pnfjra-ao-in-f14.1e100.net (142.250.187.78): icmp_seq=10 ttl=115 time=26.0 ms
64 bytes from pnfjra-ao-in-f14.1e100.net (142.250.187.78): icmp_seq=11 ttl=115 time=22.2 ms
64 bytes from pnfjra-ao-in-f14.1e100.net (142.250.187.78): icmp_seq=12 ttl=115 time=23.2 ms
64 bytes from pnfjra-ao-in-f14.1e100.net (142.250.187.78): icmp_seq=13 ttl=115 time=22.6 ms
64 bytes from pnfjra-ao-in-f14.1e100.net (142.250.187.78): icmp_seq=14 ttl=115 time=22.5 ms
64 bytes from pnfjra-ao-in-f14.1e100.net (142.250.187.78): icmp_seq=15 ttl=115 time=23.6 ms
64 bytes from pnfjra-ao-in-f14.1e100.net (142.250.187.78): icmp_seq=16 ttl=115 time=24.5 ms
^C
── google.com ping statistics ──
16 packets transmitted, 16 received, 0% packet loss, time 15105ms
rtt min/avg/max/mdev = 22.154/23.332/26.004/0.974 ms
```

ss / netstat

The ss and netstat commands are used to display network socket information. They show active connections, listening ports, and services running on the system. The ss command is faster and more modern, so it is preferred in newer Linux systems.

```
┌──(filza㉿Filza)-[~]
└─$ netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:42799         0.0.0.0:*               LISTEN
```

TASK:04

FILZA SAFDAR

```
┌──(filza㉿Filza)-[~]
└─$ ss -tuln
Netid  State      Recv-Q     Send-Q          Local Address:Port
tcp    LISTEN     0          4096                127.0.0.1:42799
```

nslookup

The nslookup command is used to find the IP address of a domain name. It queries DNS servers and helps check whether DNS is working properly. This command is useful when troubleshooting website access problems.

```
┌──(filza㉿Filza)-[~]
└─$ nslookup google.com
Server:         192.168.100.1
Address:        192.168.100.1#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.187.78
Name:   google.com
Address: 2a00:1450:4019:804::200e
```

dig

```
┌──(filza㉿Filza)-[~]
└─$ dig google.com

; <<>> DiG 9.20.15-2-Debian <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58350
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             120     IN      A       142.250.187.78

;; Query time: 0 msec
;; SERVER: 192.168.100.1#53(192.168.100.1) (UDP)
;; WHEN: Fri Dec 26 13:37:41 CST 2025
;; MSG SIZE  rcvd: 44
```

TASK:04

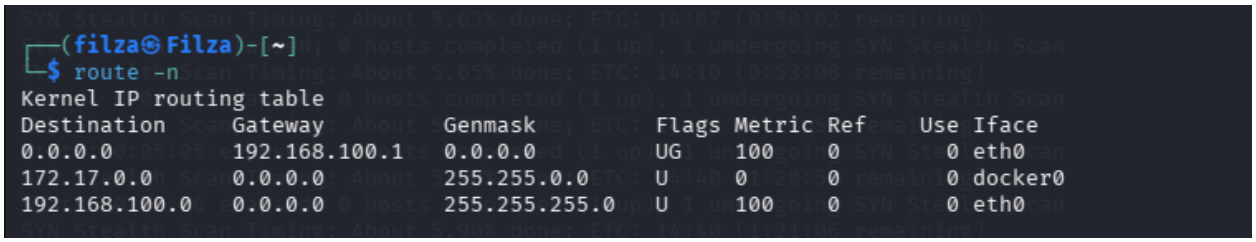
FILZA SAFDAR

The dig command is an advanced DNS lookup tool. It provides detailed information about DNS records and server responses. Network administrators use this command for deep analysis of DNS-related issues.

Windows Commands

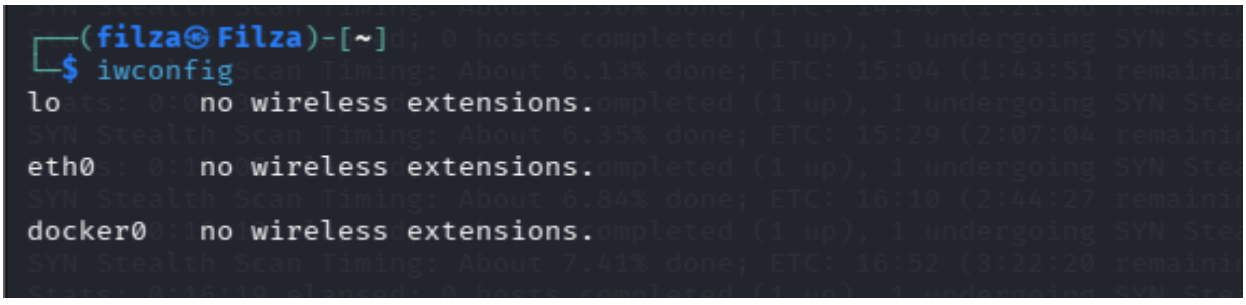
route

The route command displays the routing table of the system. It shows how network traffic is directed from one network to another. This command helps in understanding and troubleshooting routing problems.



iwconfig

The iwconfig command is used to display and configure wireless network interfaces in Linux. It shows information such as the wireless network name (SSID) and signal strength. This command is helpful for managing Wi-Fi connections.

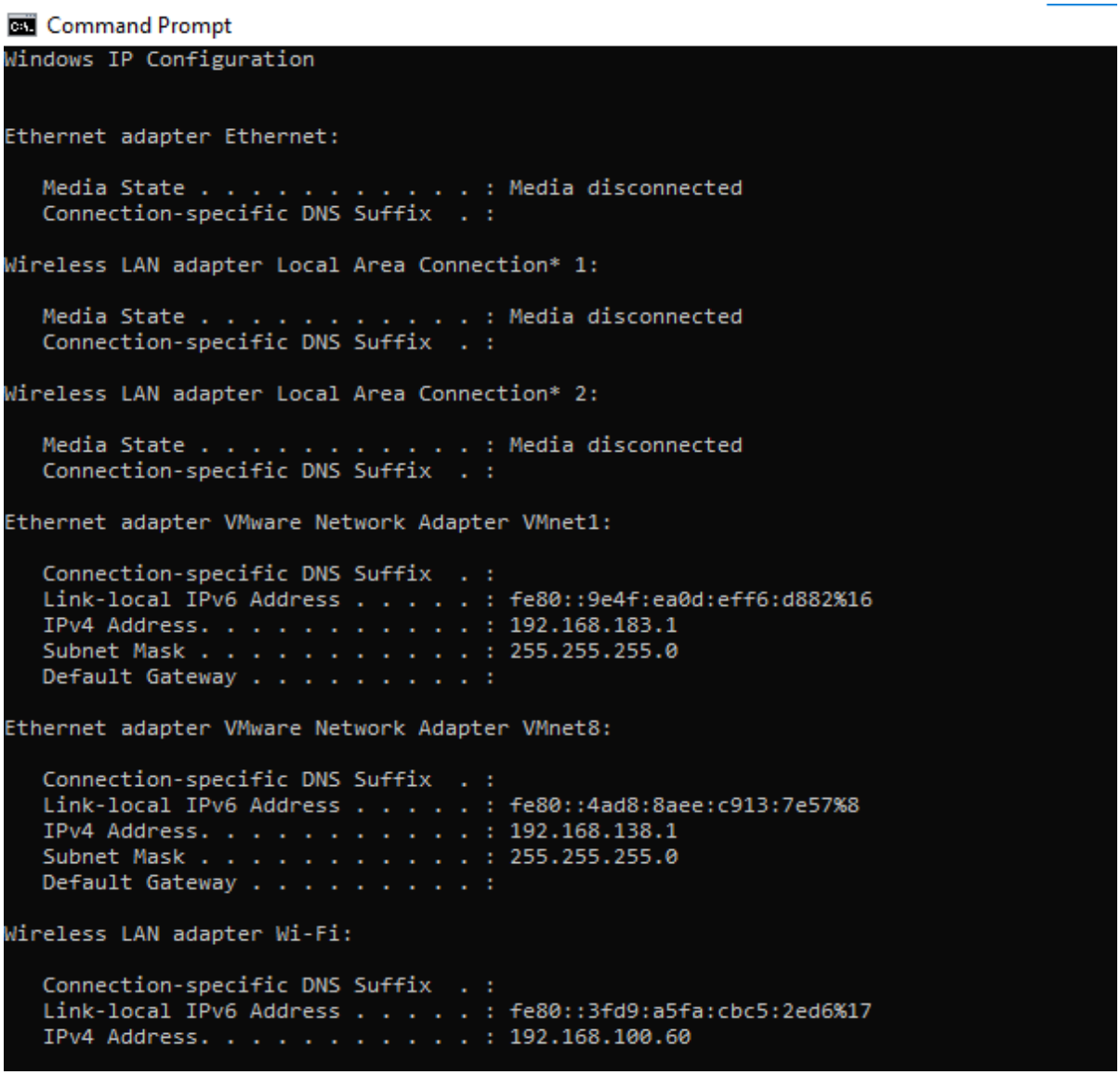


TASK:04

FILZA SAFDAR

ipconfig

The ipconfig command is used to see the network details of a computer. It shows important information such as the IP address, subnet mask, and default gateway assigned to the system. This command is very helpful when checking whether the computer is properly connected to a network or not. Using ipconfig /all gives more detailed information like MAC address and DNS servers.



TASK:04

FILZA SAFDAR

ping

The ping command is used to check whether another computer or website is reachable over the network. It sends small data packets to the target and waits for a reply. If replies are received, it means the connection is working. Ping also shows how long it takes for data to travel, which helps measure network speed and delay.

```
C:\Users\HP>ping google.com

Pinging google.com [142.250.187.78] with 32 bytes of data:
Reply from 142.250.187.78: bytes=32 time=24ms TTL=115
Reply from 142.250.187.78: bytes=32 time=23ms TTL=115
Reply from 142.250.187.78: bytes=32 time=23ms TTL=115
Reply from 142.250.187.78: bytes=32 time=22ms TTL=115

Ping statistics for 142.250.187.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 22ms, Maximum = 24ms, Average = 23ms
```

tracert

The tracert command is used to find the path that data packets follow to reach a destination. It shows all the routers (hops) between the source computer and the target system. This command is useful for identifying where network delays or connection problems occur.

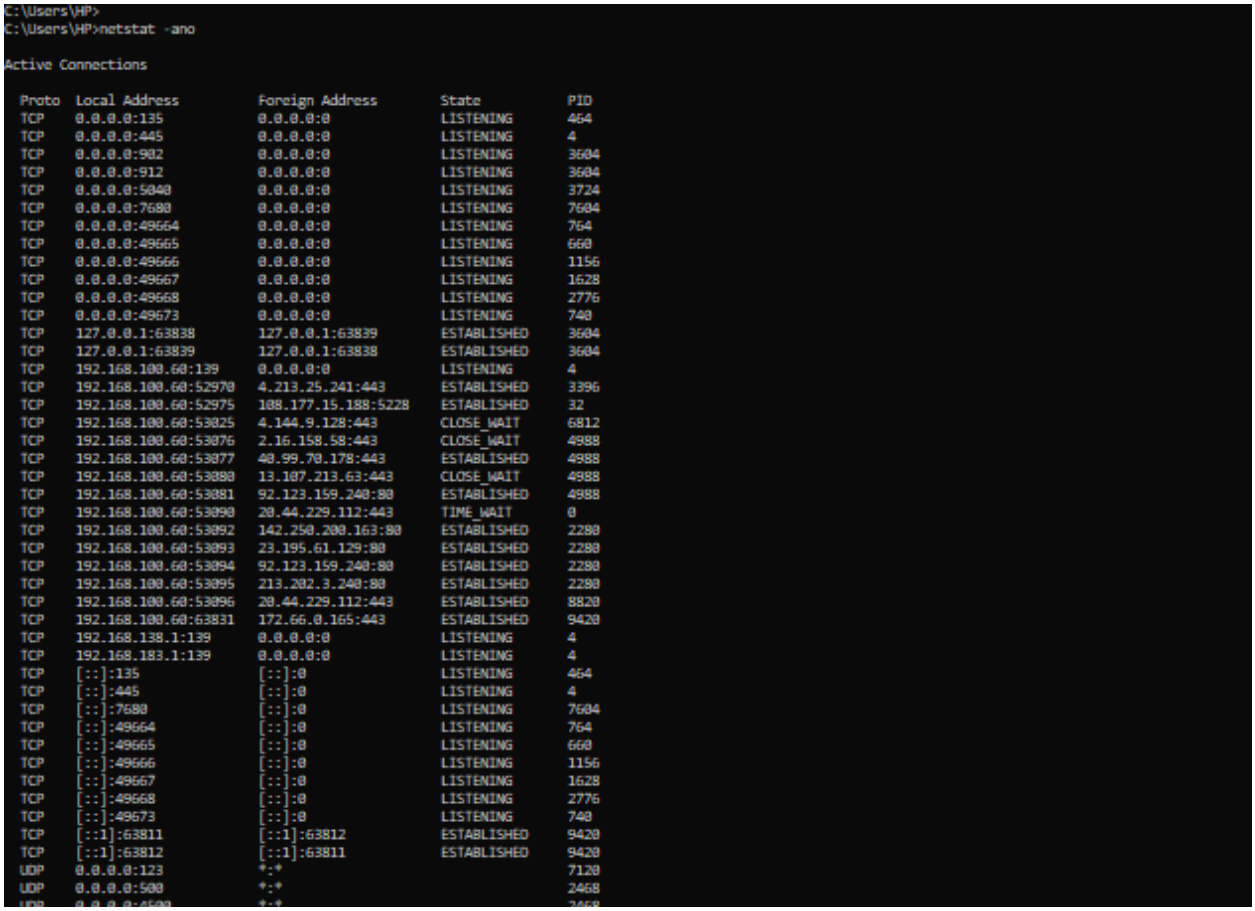
```
C:\Users\HP>tracert google.com

Tracing route to google.com [142.250.187.78]
over a maximum of 30 hops:

  1     4 ms     2 ms     1 ms  192.168.100.1
  2     4 ms     3 ms     1 ms  172.30.0.5
  3     2 ms     2 ms     3 ms  192.168.40.252
  4     4 ms     3 ms     2 ms  192.168.45.1
  5     6 ms     3 ms     2 ms  static.connect.net.pk.249.120.221.in-addr.arpa [221.120.249.233]
  6     5 ms     7 ms     4 ms  119.159.240.165
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9    23 ms    23 ms    21 ms  72.14.216.38
 10    24 ms    23 ms    23 ms  209.85.241.201
 11    22 ms    21 ms    22 ms  192.178.96.205
 12    24 ms    22 ms    24 ms  pnfjra-ao-in-f14.1e100.net [142.250.187.78]

Trace complete.
```

TASK:04

FILZA SAFDAR

netstat

The netstat command displays active network connections and open ports on a system. It helps users understand which applications are using the network. This command is often used to troubleshoot network problems and to check for suspicious or unwanted connections.



```
C:\Users\HP>
C:\Users\HP>netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       464
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:902            0.0.0.0:0              LISTENING       3604
  TCP    0.0.0.0:912            0.0.0.0:0              LISTENING       3604
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       3724
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING       7604
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       764
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       660
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       1156
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       1628
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       2776
  TCP    0.0.0.0:49673          0.0.0.0:0              LISTENING       740
  TCP    127.0.0.1:63838        127.0.0.1:63839        ESTABLISHED     3604
  TCP    127.0.0.1:63839        127.0.0.1:63838        ESTABLISHED     3604
  TCP    192.168.100.60:139     0.0.0.0:0              LISTENING       4
  TCP    192.168.100.60:52970   4.213.25.241:443       ESTABLISHED     3396
  TCP    192.168.100.60:52975   188.177.15.188:5228    ESTABLISHED     32
  TCP    192.168.100.60:53025   4.144.9.128:443        CLOSE_WAIT      6812
  TCP    192.168.100.60:53076   2.16.158.58:443        CLOSE_WAIT      4988
  TCP    192.168.100.60:53077   40.99.70.178:443       ESTABLISHED     4988
  TCP    192.168.100.60:53080   13.107.213.63:443      CLOSE_WAIT      4988
  TCP    192.168.100.60:53081   92.123.159.240:80      ESTABLISHED     4988
  TCP    192.168.100.60:53090   20.44.229.112:443      TIME_WAIT       0
  TCP    192.168.100.60:53092   142.250.200.163:80     ESTABLISHED     2280
  TCP    192.168.100.60:53093   23.195.61.129:80       ESTABLISHED     2280
  TCP    192.168.100.60:53094   92.123.159.240:80      ESTABLISHED     2280
  TCP    192.168.100.60:53095   213.202.3.240:80       ESTABLISHED     2280
  TCP    192.168.100.60:53096   20.44.229.112:443      ESTABLISHED     8820
  TCP    192.168.100.60:63831   172.66.0.165:443       ESTABLISHED     9420
  TCP    192.168.138.1:139      0.0.0.0:0              LISTENING       4
  TCP    192.168.183.1:139      0.0.0.0:0              LISTENING       4
  TCP    [::]:135               [::]:0                 LISTENING       464
  TCP    [::]:445               [::]:0                 LISTENING       4
  TCP    [::]:7680              [::]:0                 LISTENING       7604
  TCP    [::]:49664             [::]:0                 LISTENING       764
  TCP    [::]:49665             [::]:0                 LISTENING       660
  TCP    [::]:49666             [::]:0                 LISTENING       1156
  TCP    [::]:49667             [::]:0                 LISTENING       1628
  TCP    [::]:49668             [::]:0                 LISTENING       2776
  TCP    [::]:49673             [::]:0                 LISTENING       740
  TCP    [::1]:63811            [::1]:63812            ESTABLISHED     9420
  TCP    [::1]:63812            [::1]:63811            ESTABLISHED     9420
  UDP    0.0.0.0:123            *:*                                    7120
  UDP    0.0.0.0:500            *:*                                    2468
```

TASK:04

FILZA SAFDAR

arp

The arp command shows the ARP table, which maps IP addresses to physical MAC addresses on the local network. It helps the system communicate with other devices in the same network. This command is useful for diagnosing local network and IP conflicts.

```
C:\Users\HP>arp -a

Interface: 192.168.138.1 --- 0x8
  Internet Address      Physical Address      Type
  192.168.138.254       00-50-56-f8-c2-9a     dynamic
  192.168.138.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     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
  239.0.0.251           01-00-5e-00-00-fb     static
  239.255.255.251       01-00-5e-7f-ff-fb     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.183.1 --- 0x10
  Internet Address      Physical Address      Type
  192.168.183.254       00-50-56-fd-2c-e0     dynamic
  192.168.183.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     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
  239.0.0.251           01-00-5e-00-00-fb     static
  239.255.255.251       01-00-5e-7f-ff-fb     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.100.60 --- 0x11
  Internet Address      Physical Address      Type
  192.168.100.1         34-00-a3-af-3c-42     dynamic
  192.168.100.4         1c-5f-2b-10-51-8c     dynamic
  192.168.100.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     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
  239.0.0.251           01-00-5e-00-00-fb     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  239.255.255.251       01-00-5e-7f-ff-fb     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

GITHUB:https://github.com/filzasafdar8-netizen/CODEINTERN_TASKS

TASK:04