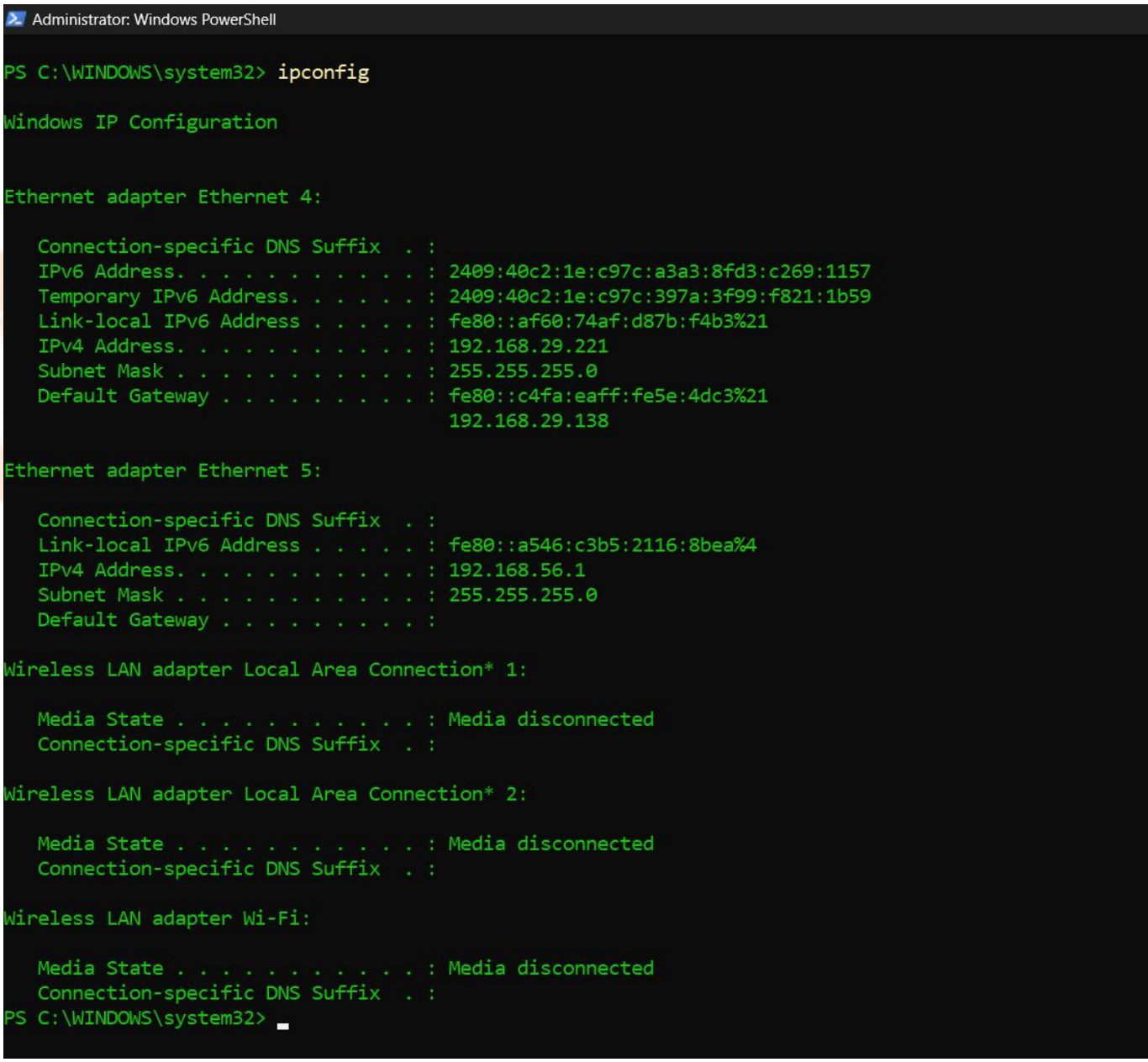
Student Name	Pratik Manoj Dharam
SRN No	31232438
Roll No	20
Program	Computer Engg
Year	Third Year
Division	H
Subject	Computer Network Laboratory (BTECCE22506)
Assignment No	Two

Assignment Number - 02

Title : Study of Linux and Windows Network commands

Problem Statement Studying Linux and Windows network commands. [ping, pathping, ipconfig/ifconfig, arp, netstat, nbtstat, nslookup, route, traceroute/tracert, nmap, etc]

Try to execute following commands on linux terminal or Windows command prompt.



- **Ipconfig / ifconfig**

- **ping**

```
PS C:\WINDOWS\system32> ping 192.168.29.221

Pinging 192.168.29.221 with 32 bytes of data:
Reply from 192.168.29.221: bytes=32 time<1ms TTL=128
Reply from 192.168.29.221: bytes=32 time<1ms TTL=128
Reply from 192.168.29.221: bytes=32 time<1ms TTL=128
Reply from 192.168.29.221: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.29.221:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\WINDOWS\system32>
```

- **Tracert/Traceroute/Tracepath**

```
PS C:\WINDOWS\system32> tracert 192.168.29.221

Tracing route to PratikDP-Lap [192.168.29.221]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  PratikDP-Lap [192.168.29.221]

Trace complete.
```

- **Finger**

```
PS C:\WINDOWS\system32> finger PratikDP-Lap

[PratikDP-Lap]
> Finger: connect::Connection refused
PS C:\WINDOWS\system32> S
```

- **NSlookup**

```
PS C:\WINDOWS\system32> nslookup instagram.com
Server:  UnKnown
Address:  192.168.29.138

Non-authoritative answer:
Name:    instagram.com
Addresses:  2a03:2880:f285:e7:face:b00c:0:4420
          163.70.140.174
```

- **Netstat**

```
PS C:\WINDOWS\system32> netstat -an
>>

Active Connections

  Proto  Local Address          Foreign Address        State
  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    0.0.0.0:1521           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:33060          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    0.0.0.0:49672          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49673          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:8080         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:49670        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:49677        127.0.0.1:49678        ESTABLISHED
  TCP    127.0.0.1:49678        127.0.0.1:49677        ESTABLISHED
  TCP    127.0.0.1:49679        127.0.0.1:49680        ESTABLISHED
  TCP    127.0.0.1:49680        127.0.0.1:49679        ESTABLISHED
  TCP    127.0.0.1:50555        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:55939        0.0.0.0:0              LISTENING
  TCP    192.168.29.221:139     0.0.0.0:0              LISTENING
  TCP    192.168.29.221:60247   104.18.157.37:443      CLOSE_WAIT
  TCP    192.168.56.1:139       0.0.0.0:0              LISTENING
  TCP    192.168.56.1:1521      192.168.56.1:49674     ESTABLISHED
  TCP    192.168.56.1:49674     192.168.56.1:1521      ESTABLISHED
```

- **Hostname**

```
PS C:\WINDOWS\system32> hostname
PratikDP-Lap
```

- **Port Scan / nmap**

- **Arp**

```
PS C:\WINDOWS\system32> arp -a
>>

Interface: 192.168.56.1 --- 0x4
  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: 192.168.29.221 --- 0x15
  Internet Address      Physical Address      Type
  192.168.29.138        c6-fa-ea-5e-4d-c3     dynamic
  192.168.29.255        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
```

```
PS C:\WINDOWS\system32> route print
>>
===========================================================================
Interface List
 21...56 d5 a9 d4 0a e5 ......Remote NDIS based Internet Sharing Device
  4...0a 00 27 00 00 04 ......VirtualBox Host-Only Ethernet Adapter
  5...c8 b2 9b c0 a1 58 ......Microsoft Wi-Fi Direct Virtual Adapter
 19...ca b2 9b c0 a1 57 ......Microsoft Wi-Fi Direct Virtual Adapter #2
 16...c8 b2 9b c0 a1 57 ......Intel(R) Wireless-AC 9560 160MHz
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0   192.168.29.138   192.168.29.221     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
     192.168.29.0    255.255.255.0         On-link    192.168.29.221    281
   192.168.29.221  255.255.255.255         On-link    192.168.29.221    281
   192.168.29.255  255.255.255.255         On-link    192.168.29.221    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    192.168.29.221    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    192.168.29.221    281
===========================================================================
Persistent Routes:
  None
```

- **Route**
- **Whois**

Theory :

1. ipconfig / ifconfig

- **Purpose**: `ipconfig` (Windows) and `ifconfig` (Linux) are used to display and manage network interface configurations.

- **Details**:

  - Windows (`ipconfig`): Shows the IP address, subnet mask, and default gateway for each network adapter. Useful for identifying network configurations and troubleshooting network issues.

  - Linux (`ifconfig`): Displays similar information, including IP addresses, network masks, and hardware addresses for network interfaces. It's often replaced by the `ip` command in modern Linux distributions.

2. ping

- Purpose: `ping` checks the reachability of a network host by sending ICMP Echo Request messages and measuring the time it takes to receive a reply.

- Details:

  - Used to test connectivity between your system and another device on the network or the internet.

  - Helps diagnose network issues, such as whether a device is reachable or if there is high latency or packet loss.

3. tracert / traceroute / tracepath

- Purpose: These commands trace the route packets take from your system to a target host, showing each hop along the way.

- Details:

  - Windows (`tracert`): Displays the path packets take to reach a destination and the time taken for each hop.

  - Linux (`traceroute` or `tracepath`): Provides similar functionality. `tracepath` is a simpler, often pre-installed tool that shows path and latency information.

4. finger

- **Purpose**: `finger` retrieves user information from a remote host on a network.

- **Details**:

  - Provides details about users logged into a system, including login name, real name, and login time.

- This command is less commonly used today and may not be available on all systems by default.

5. **nslookup**

- **Purpose**: `nslookup` queries DNS to obtain domain name or IP address mappings.
- **Details**:
  - Used to resolve domain names to IP addresses and vice versa.
  - Helps in diagnosing DNS issues and understanding how DNS records are configured.

6. netstat

- **Purpose**: `netstat` displays network connections, routing tables, and interface statistics.
- **Details**:
  - Shows active network connections, listening ports, and current network statistics.
  - Useful for monitoring network activity and diagnosing connection issues.

7. **hostname**

- **Purpose**: `hostname` displays or sets the system's hostname.
- **Details**:
  - Shows the current hostname of the system, which identifies it on the network.
  - Useful for verifying or changing the network name of a computer.

8. port scan / nmap

- **Purpose**: `nmap` scans for open ports and services on a network host.
- **Details**:
  - Provides information about which ports are open and which services are running on a target system.
  - Useful for security assessments and identifying vulnerabilities in networked systems.

9. arp

- **Purpose**: `arp` displays or modifies the ARP (Address Resolution Protocol) cache.
- **Details**:
  - Shows mappings between IP addresses and MAC addresses in the local ARP cache.
  - Useful for diagnosing issues related to IP-to-MAC address resolution on a local network.

10. route

- **Purpose**: `route` displays or modifies the IP routing table.

- **Details**:

  - Shows how packets are routed through the network, including routes and gateways.

  - Helps in diagnosing routing issues and configuring network paths.

11. whois

- **Purpose**: `whois` retrieves domain registration information from a WHOIS database.

- **Details**:

  - Provides information about the domain owner, registration dates, and contact details.

  - Useful for domain management, ownership verification, and finding contact information for domain-related inquiries.

Conclusion :

Through this assignment, I gained hands-on experience with various network commands used in both Linux and Windows environments. I learned how to check network configurations, test connectivity, trace routes, and gather important information about domains and network interfaces. This practical exposure has deepened my understanding of how these tools work together to manage and troubleshoot network issues. By using these commands, I now feel more confident in diagnosing network problems and ensuring that everything is running smoothly. This knowledge is crucial for anyone looking to manage networks effectively.