Name: Palsutkar Vivek Ramesh

Section: B

BITS ID: 202117b3734

Subject: Computer Networks

Topic: Experiment 1

Experiment 1: Explore Your Network

Objective

The objective of this experiment is to understand and use various networking commands to explore and diagnose a system's network configuration.

1. ipconfig / ifconfig

Command used:

On Windows: ipconfig

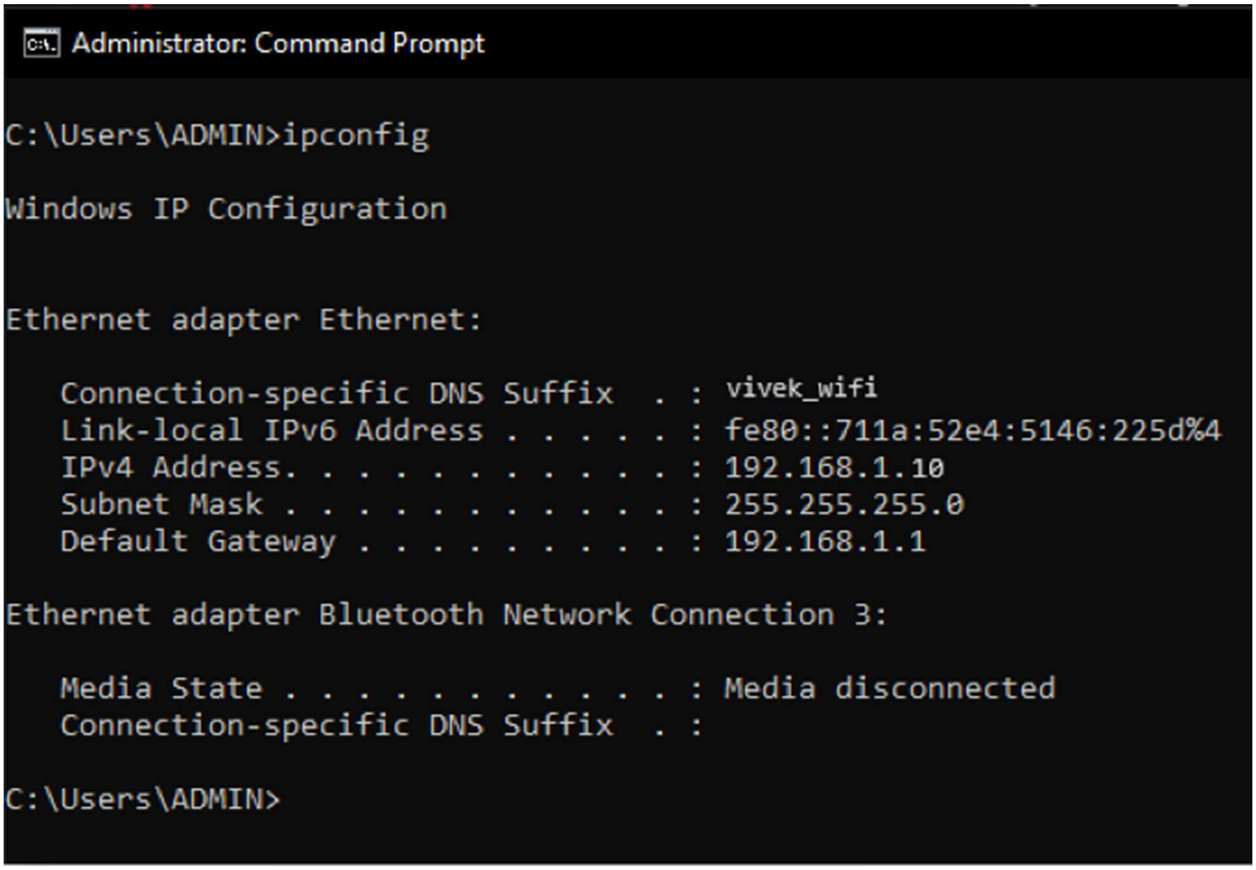
On Linux/Mac: ifconfig

Description:

ipconfig (Windows) and ifconfig (Linux/Mac) are used to display the current network configuration of the system.

They show details like IP address, subnet mask, default gateway, and active network adapters.

Output (Screenshot here):



```
C:\Users\ADMIN>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : vivek_wifi
   Link-local IPv6 Address . . . . . : fe80::711a:52e4:5146:225d%4
   IPv4 Address. . . . . . . . . . . : 192.168.1.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter Bluetooth Network Connection 3:

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

C:\Users\ADMIN>
```

Explanation of Output:

IPv4 Address: Identifies your system on the network.

Subnet Mask: Defines the range of IPs in your local network.

Default Gateway: The router’s IP, used to access external networks.

Adapter Info: Shows wired/wireless network details.

Example Usage:

Checking if your device received a proper IP from the router (e.g., DHCP assignment).

2. ping

Command used:

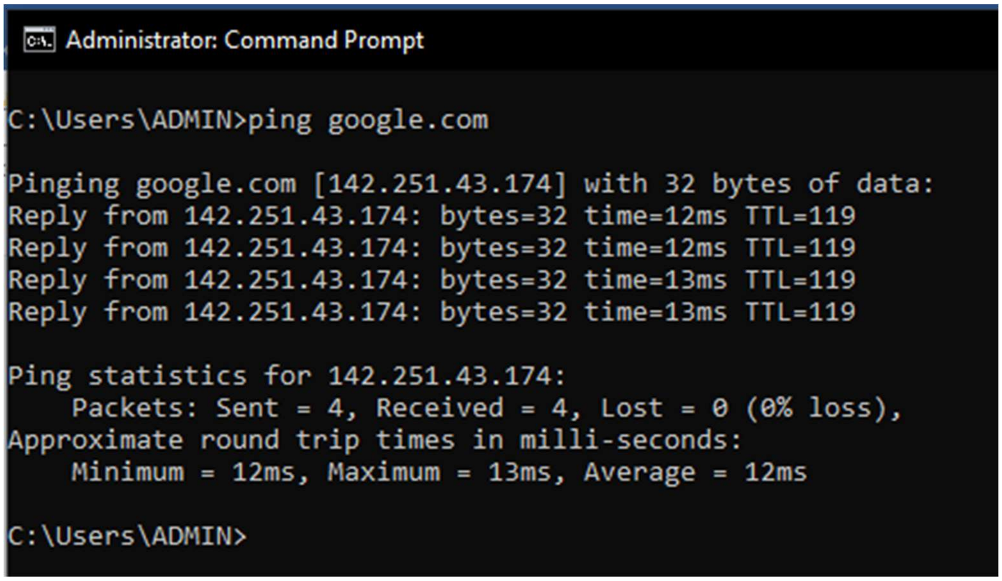
ping <domain or IP>

Description:

The ping command tests connectivity between your system and another host.

It measures round-trip time (RTT) and packet loss.

Output (Screenshot here):



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

Pinging google.com [142.251.43.174] with 32 bytes of data:
Reply from 142.251.43.174: bytes=32 time=12ms TTL=119
Reply from 142.251.43.174: bytes=32 time=12ms TTL=119
Reply from 142.251.43.174: bytes=32 time=13ms TTL=119
Reply from 142.251.43.174: bytes=32 time=13ms TTL=119

Ping statistics for 142.251.43.174:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 13ms, Average = 12ms

C:\Users\ADMIN>
```

Explanation of Output:

Reply from... → Indicates successful communication.

Time=<ms> → Shows latency.

Packets Sent/Received/Lost: Helps detect connectivity issues.

Example Usage:

ping google.com → To check if your internet connection is working.

3. tracert / traceroute

Command used:

On Windows: tracert <domain>

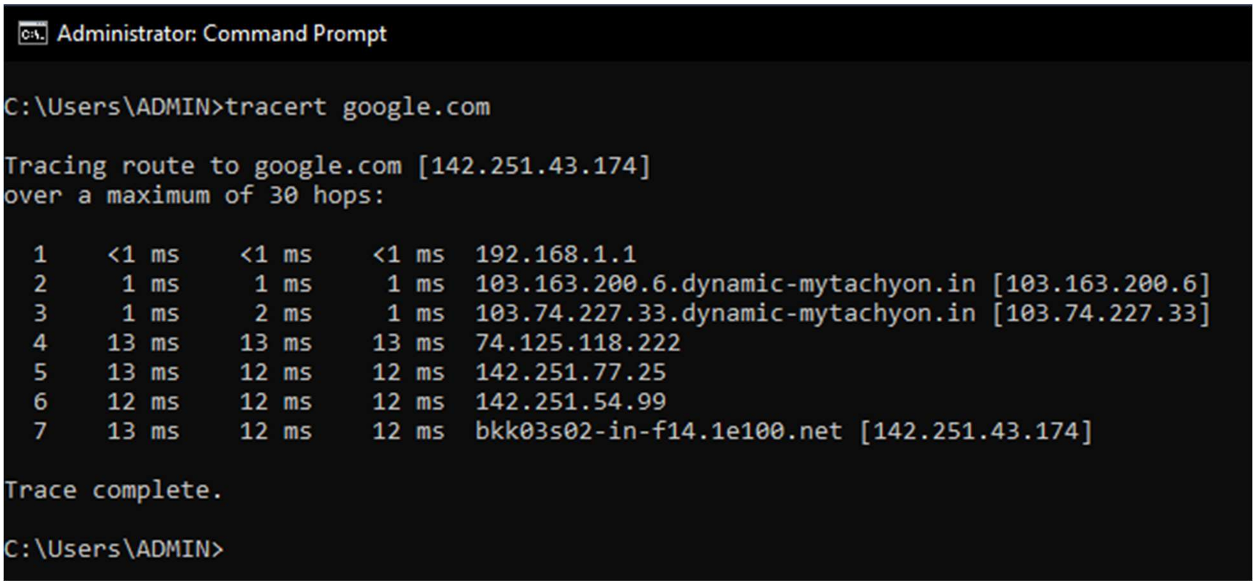
On Linux/Mac: traceroute <domain>

Description:

This command shows the path your packets take to reach a destination.

Displays each hop (router) between your system and the destination server.

Output (Screenshot here):



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

Tracing route to google.com [142.251.43.174]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.1.1
  2     1 ms     1 ms     1 ms  103.163.200.6.dynamic-mytachyon.in [103.163.200.6]
  3     1 ms     2 ms     1 ms  103.74.227.33.dynamic-mytachyon.in [103.74.227.33]
  4    13 ms    13 ms    13 ms  74.125.118.222
  5    13 ms    12 ms    12 ms  142.251.77.25
  6    12 ms    12 ms    12 ms  142.251.54.99
  7    13 ms    12 ms    12 ms  bkk03s02-in-f14.1e100.net [142.251.43.174]

Trace complete.

C:\Users\ADMIN>
```

Explanation of Output:

Each line = one hop (router/switch).

Shows IP address and response time of each hop.

Helps identify delays or where a connection breaks.

Example Usage:

tracert google.com → To identify the network path and diagnose where latency occurs.

4. netstat

Command used:

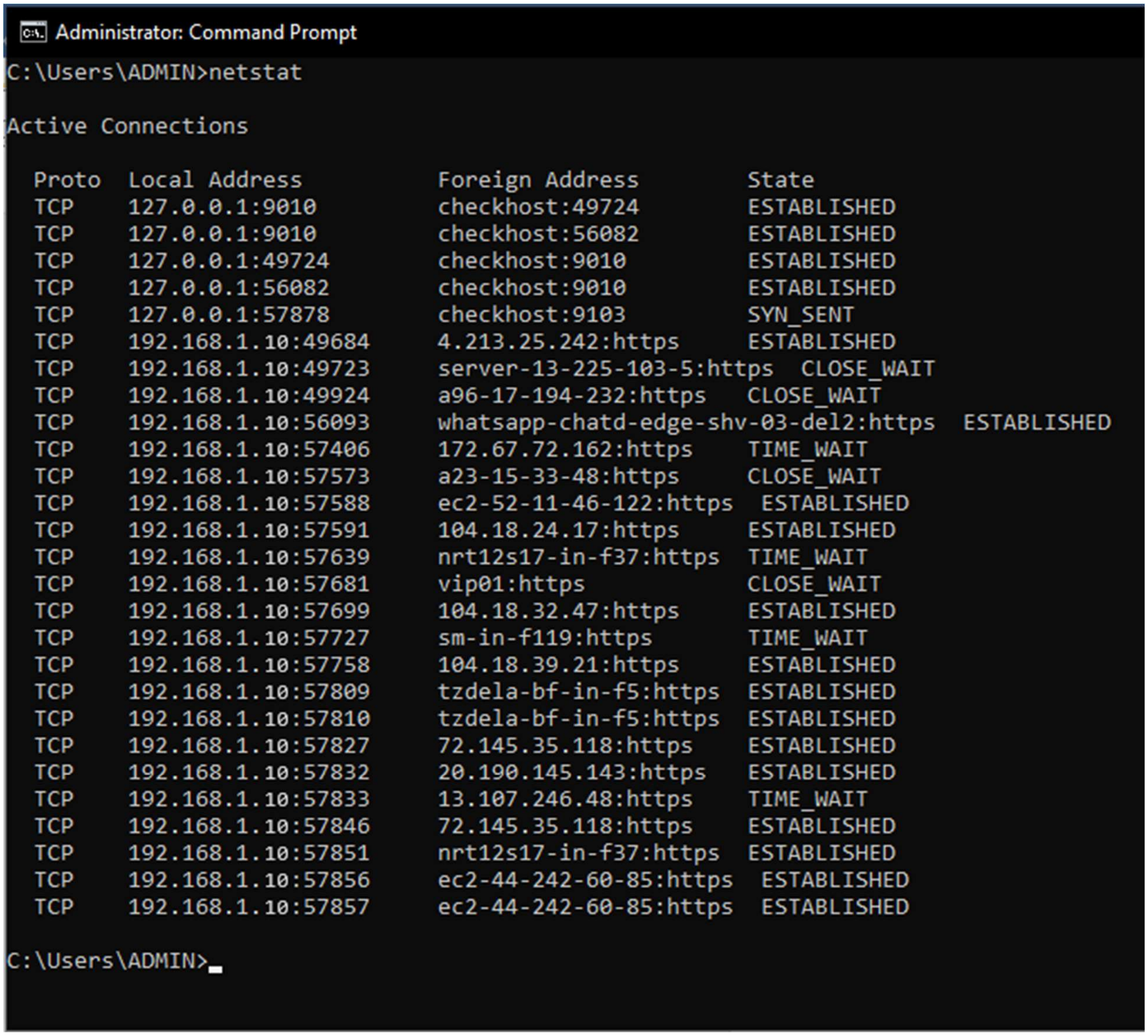
netstat

Description:

Displays active network connections, listening ports, and routing tables.

Useful to check which applications are using the network.

Output (Screenshot here):



```
C:\Users\ADMIN>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:9010         checkhost:49724        ESTABLISHED
  TCP    127.0.0.1:9010         checkhost:56082        ESTABLISHED
  TCP    127.0.0.1:49724        checkhost:9010         ESTABLISHED
  TCP    127.0.0.1:56082        checkhost:9010         ESTABLISHED
  TCP    127.0.0.1:57878        checkhost:9103         SYN_SENT
  TCP    192.168.1.10:49684     4.213.25.242:https     ESTABLISHED
  TCP    192.168.1.10:49723     server-13-225-103-5:https  CLOSE_WAIT
  TCP    192.168.1.10:49924     a96-17-194-232:https   CLOSE_WAIT
  TCP    192.168.1.10:56093     whatsapp-chatd-edge-shv-03-del2:https  ESTABLISHED
  TCP    192.168.1.10:57406     172.67.72.162:https    TIME_WAIT
  TCP    192.168.1.10:57573     a23-15-33-48:https     CLOSE_WAIT
  TCP    192.168.1.10:57588     ec2-52-11-46-122:https  ESTABLISHED
  TCP    192.168.1.10:57591     104.18.24.17:https     ESTABLISHED
  TCP    192.168.1.10:57639     nrt12s17-in-f37:https  TIME_WAIT
  TCP    192.168.1.10:57681     vip01:https            CLOSE_WAIT
  TCP    192.168.1.10:57699     104.18.32.47:https     ESTABLISHED
  TCP    192.168.1.10:57727     sm-in-f119:https       TIME_WAIT
  TCP    192.168.1.10:57758     104.18.39.21:https     ESTABLISHED
  TCP    192.168.1.10:57809     tzdela-bf-in-f5:https  ESTABLISHED
  TCP    192.168.1.10:57810     tzdela-bf-in-f5:https  ESTABLISHED
  TCP    192.168.1.10:57827     72.145.35.118:https    ESTABLISHED
  TCP    192.168.1.10:57832     20.190.145.143:https   ESTABLISHED
  TCP    192.168.1.10:57833     13.107.246.48:https    TIME_WAIT
  TCP    192.168.1.10:57846     72.145.35.118:https    ESTABLISHED
  TCP    192.168.1.10:57851     nrt12s17-in-f37:https  ESTABLISHED
  TCP    192.168.1.10:57856     ec2-44-242-60-85:https  ESTABLISHED
  TCP    192.168.1.10:57857     ec2-44-242-60-85:https  ESTABLISHED

C:\Users\ADMIN>_
```

Explanation of Output:

Proto (TCP/UDP): Shows type of connection.

Local Address: Your system’s IP/port.

Foreign Address: Remote system’s IP/port.

State: Connection status (e.g., ESTABLISHED, LISTENING).

Example Usage:

Checking if a suspicious process is using an unknown port.

5. nslookup

Command used:

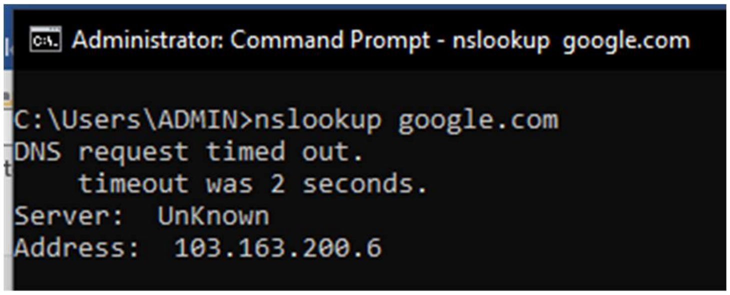
nslookup <domain>

Description:

Used to query DNS servers and find the IP address of a domain.

Can also display mail servers and other DNS records.

Output (Screenshot here):



Administrator: Command Prompt - nslookup google.com

```
C:\Users\ADMIN>nslookup google.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  103.163.200.6
```

Explanation of Output:

Server: DNS server used.

Address: IP address of the domain queried.

Example Usage:

nslookup openai.com → To get the IP address of OpenAI's server.

6. arp

Command used:

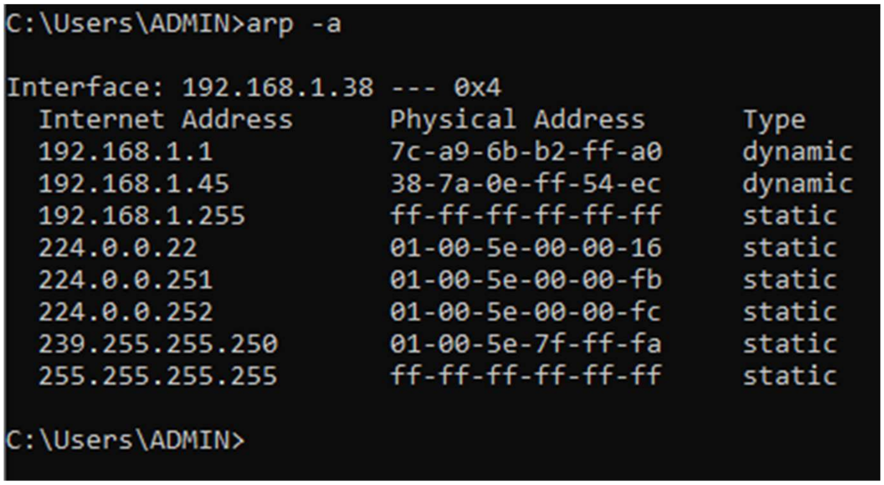
arp -a

Description:

Displays the ARP (Address Resolution Protocol) table.

Maps IP addresses to physical MAC addresses in the local network.

Output (Screenshot here):



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

Interface: 192.168.1.38 --- 0x4
  Internet Address      Physical Address      Type
  192.168.1.1           7c-a9-6b-b2-ff-a0     dynamic
  192.168.1.45          38-7a-0e-ff-54-ec     dynamic
  192.168.1.255         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

C:\Users\ADMIN>
```

Explanation of Output:

Internet Address: IP of local devices.

Physical Address: MAC address of the devices.

Type: Dynamic (assigned by ARP) or Static (manually set).

Example Usage:

Checking connected devices in your LAN (e.g., detecting unauthorized devices).