Exp 1: Demonstrate the working of network tools such as Ping, TCPDump, Traceroute, Netstat.

Aim:

To study and demonstrate the usage of basic network diagnostic tools: Ping, TCPDump, Traceroute and Netstat.

Objective

- To understand the purpose and functioning of each tool
- To learn how to use these tools for network diagnostics and monitoring
- To interpret and analyze the outputs

Software Required

1. Operating System (windows or Linux)
2. Terminal/Command prompt access
3. Network Connectivity
4. Installed utilities
   - i. Ping
   - ii. Tcpdump
   - iii. Traceroute / tracert (windows)
   - iv. Netstat or ss

Background Theory

Computer networks can encounter connectivity, performance or routing issues. To troubleshoot these problems, network diagnostic tools are used. Understanding these tools is essential for network administrators.

- Ping uses the ICMP protocol to test connectivity between two devices and measures latency
- TCPDump captures and inspects network packets on interfaces for detailed analysis of communication.
- Traceroute traces the path packets take from source to destination, showing all intermediate hops and delays.
- Netstat displays network connection status ports and interface statistics, helping detect open or suspicious connections

These tools are fundamental for diagnosing issues like packet loss, unreachable hosts or misconfigured.

Algorithm

1. Ping

- Send ICMP echo requests to a host
- Measure response time and packet loss

2. TCPdump

- Capture and analyze network places
- Apply filters to narrow down captured data

3. Traceroute

- Trace the path packets take to reach the destination
- Display intermediate routers/hops

4. Netstat

- Display network connections, routing tables, interface statistics etc.

Step –by-Step Procedure

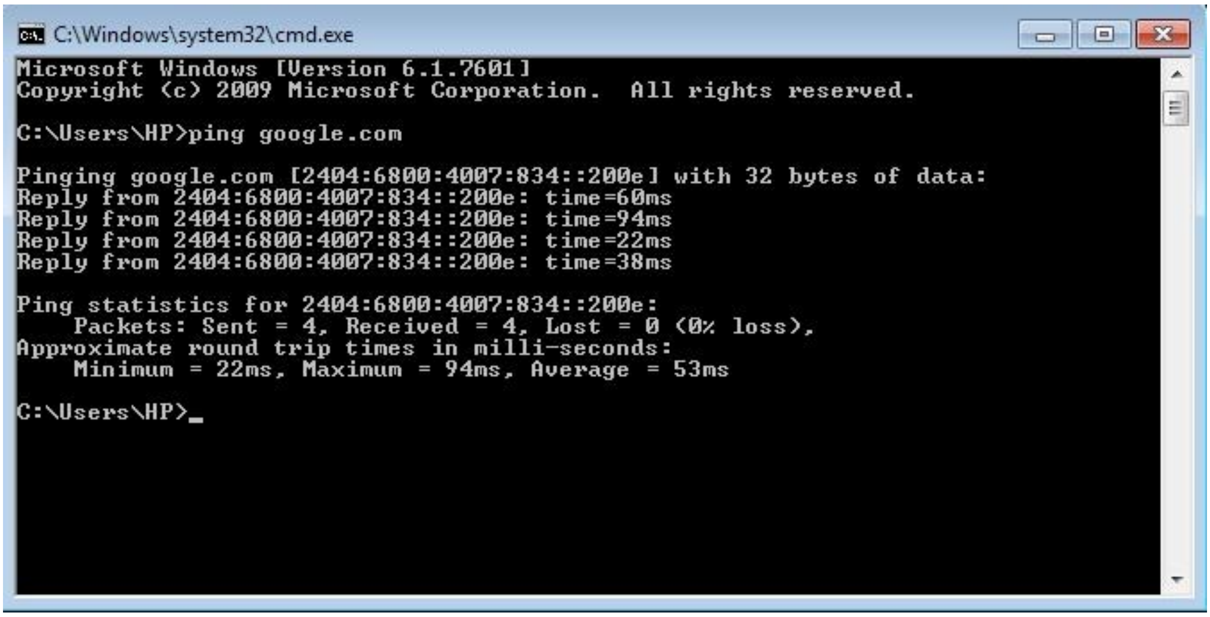
1. Ping

Ping google.com

Expected Output

- Packets sent/receive
- RTT (Round Trip Time)
- Packet loss(ifany)

Output



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\HP>ping google.com

Pinging google.com [2404:6800:4007:834::200e] with 32 bytes of data:
Reply from 2404:6800:4007:834::200e: time=60ms
Reply from 2404:6800:4007:834::200e: time=94ms
Reply from 2404:6800:4007:834::200e: time=22ms
Reply from 2404:6800:4007:834::200e: time=38ms

Ping statistics for 2404:6800:4007:834::200e:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 22ms, Maximum = 94ms, Average = 53ms

C:\Users\HP>_
```

2. tcpdump

Sudo tcpdump –i any

To capture specific port (e.g.HTTP)

Sudo tcpdump port 80

Expected Output

- Real time packet headers and source/destination IPs
- Protocol info

Stop with Ctrl + C

3. using traceroute

Linux command

traceroute google.com

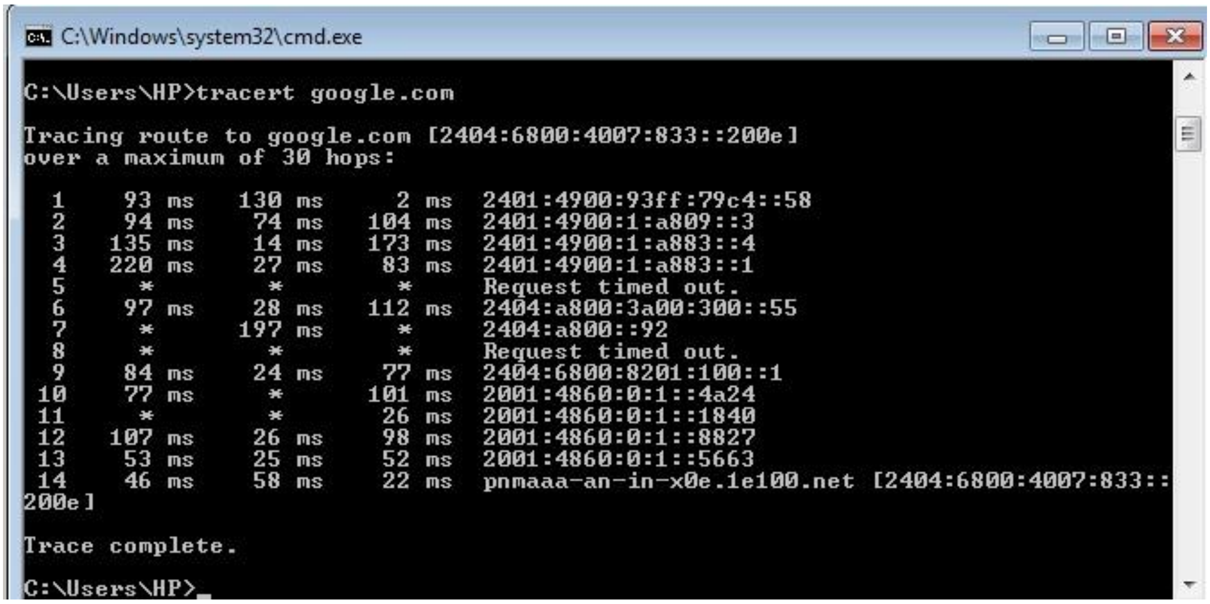
Windows Command

tracert google.com

Expected Output

- List of routers(hop)
- IPs and latency at each hop

Output



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

Tracing route to google.com [2404:6800:4007:833::200e]
over a maximum of 30 hops:

  1    93 ms   130 ms     2 ms  2401:4900:93ff:79c4::58
  2    94 ms    74 ms   104 ms  2401:4900:1:a809::3
  3   135 ms    14 ms   173 ms  2401:4900:1:a883::4
  4   220 ms    27 ms    83 ms  2401:4900:1:a883::1
  5     *        *        *     Request timed out.
  6    97 ms    28 ms   112 ms  2404:a800:3a00:300::55
  7     *      197 ms     *     2404:a800::92
  8     *        *        *     Request timed out.
  9    84 ms    24 ms    77 ms  2404:6800:8201:100::1
 10    77 ms     *      101 ms  2001:4860:0:1::4a24
 11     *        *       26 ms  2001:4860:0:1::1840
 12   107 ms    26 ms    98 ms  2001:4860:0:1::8827
 13    53 ms    25 ms    52 ms  2001:4860:0:1::5663
 14    46 ms    58 ms    22 ms  pnmaaa-an-in-x0e.1e100.net [2404:6800:4007:833::
200e]

Trace complete.

C:\Users\HP>_
```

4. Using netstat

Basic usage

netstat –an

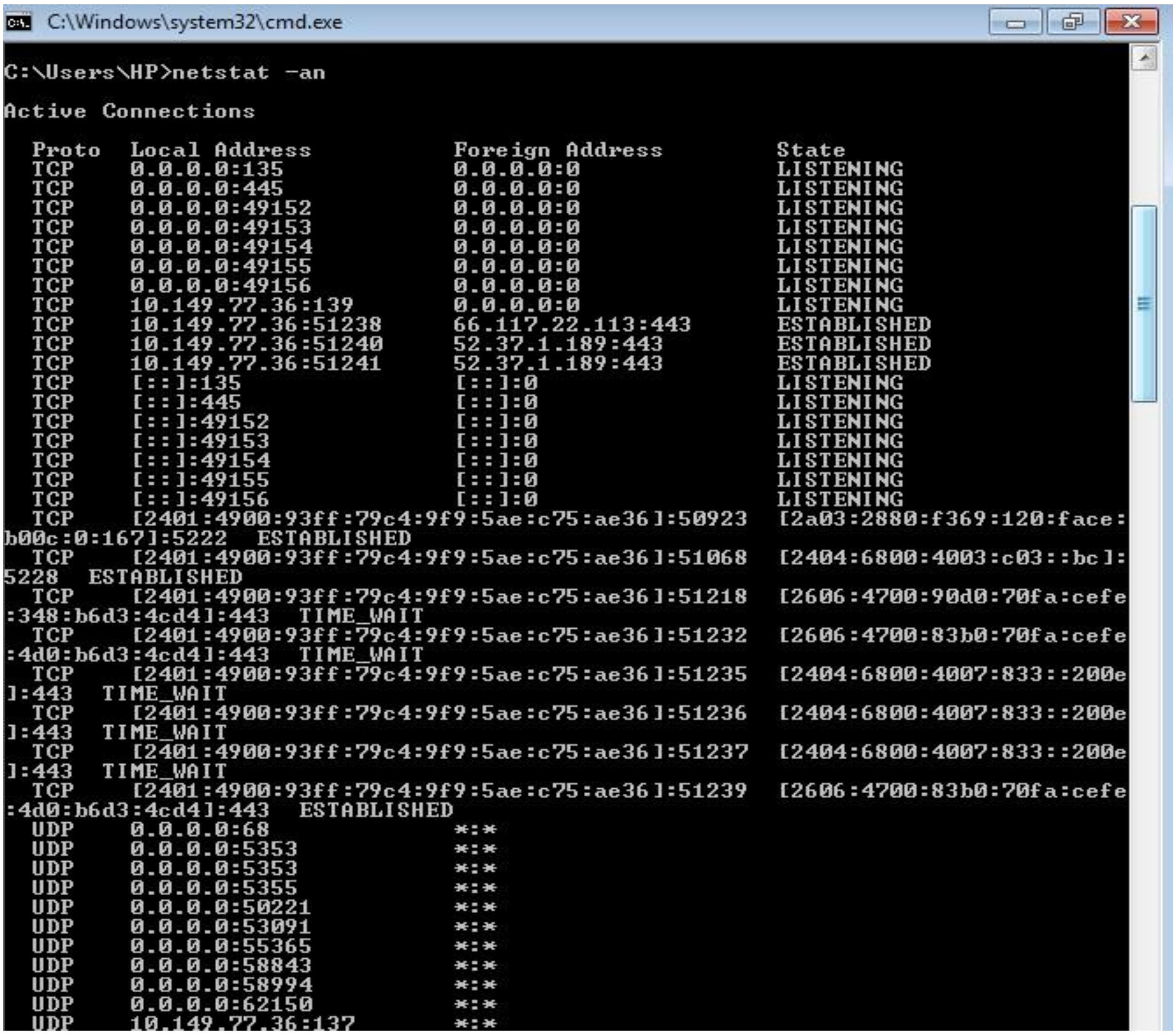
To Show listing ports and processes

netstat –tulnp

Expected Output

- List of TCP/UDP connection
- Listening ports and related services

Output



```
C:\Users\HP>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    0.0.0.0:49152          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49156          0.0.0.0:0              LISTENING
  TCP    10.149.77.36:139       0.0.0.0:0              LISTENING
  TCP    10.149.77.36:51238     66.117.22.113:443      ESTABLISHED
  TCP    10.149.77.36:51240     52.37.1.189:443        ESTABLISHED
  TCP    10.149.77.36:51241     52.37.1.189:443        ESTABLISHED
  TCP    [::]:135               [::]:0                 LISTENING
  TCP    [::]:445               [::]:0                 LISTENING
  TCP    [::]:49152             [::]:0                 LISTENING
  TCP    [::]:49153             [::]:0                 LISTENING
  TCP    [::]:49154             [::]:0                 LISTENING
  TCP    [::]:49155             [::]:0                 LISTENING
  TCP    [::]:49156             [::]:0                 LISTENING
  TCP    [2401:4900:93ff:79c4:9f9:5ae:c75:ae36]:50923  [2a03:2880:f369:120:face:
b00c:0:167]:5222  ESTABLISHED
  TCP    [2401:4900:93ff:79c4:9f9:5ae:c75:ae36]:51068  [2404:6800:4003:c03::bc]:
5228  ESTABLISHED
  TCP    [2401:4900:93ff:79c4:9f9:5ae:c75:ae36]:51218  [2606:4700:90d0:70fa:cefe
:348:b6d3:4cd4]:443  TIME_WAIT
  TCP    [2401:4900:93ff:79c4:9f9:5ae:c75:ae36]:51232  [2606:4700:83b0:70fa:cefe
:4d0:b6d3:4cd4]:443  TIME_WAIT
  TCP    [2401:4900:93ff:79c4:9f9:5ae:c75:ae36]:51235  [2404:6800:4007:833::200e
]:443  TIME_WAIT
  TCP    [2401:4900:93ff:79c4:9f9:5ae:c75:ae36]:51236  [2404:6800:4007:833::200e
]:443  TIME_WAIT
  TCP    [2401:4900:93ff:79c4:9f9:5ae:c75:ae36]:51237  [2404:6800:4007:833::200e
]:443  TIME_WAIT
  TCP    [2401:4900:93ff:79c4:9f9:5ae:c75:ae36]:51239  [2606:4700:83b0:70fa:cefe
:4d0:b6d3:4cd4]:443  ESTABLISHED
  UDP    0.0.0.0:68             *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5355           *:*
  UDP    0.0.0.0:50221          *:*
  UDP    0.0.0.0:53091          *:*
  UDP    0.0.0.0:55365          *:*
  UDP    0.0.0.0:58843          *:*
  UDP    0.0.0.0:58994          *:*
  UDP    0.0.0.0:62150          *:*
  UDP    10.149.77.36:137       *:*
```

Result

The working of basic network tools was demonstrated and their outputs were interpreted successfully.

Pre-viva questions

1. What is the purpose of the ping command?

2. Which protocol does ping use?

3. How does tcpdump help in network troubleshooting?

4. What is the difference between traceroute and ping?

5. What information does netstat provide?

Post-viva questions

1. How would you capture packets only from a specific IP using tcpdump

2. How does traceroute handle unreachable destinations?

3. What does the TTL value indicate in ping and traceroute?

4. Explain the difference between netstat and ss

5. How do you interpret high latency in traceroute output?