Learn to use commands like tcp dump, netstat, ifconfig, nslookup and traceroute.

Capture ping and trace route PDUs using a network protocol analyzer and examine

PROGRAM:

#show ip configuration

Ipconfig

#view active TCP/UDP connection and port

Netstat -an

#perform dns lookup

Nslookup www.google.com

#trace a route to website

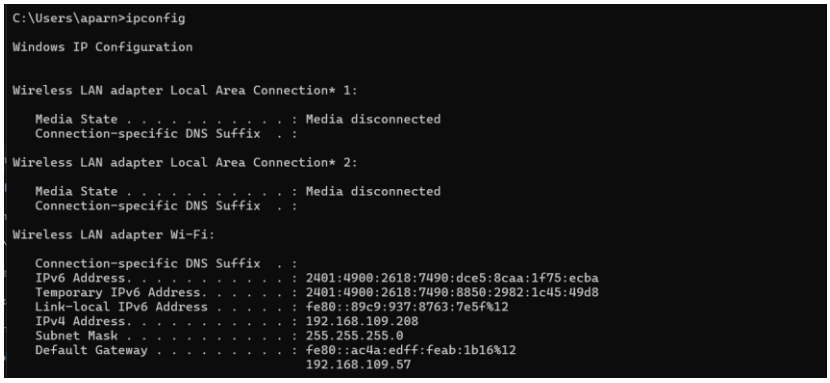
Tracert www.google.com

#ping server to test connectivity

Ping www.google.com

OUTPUT:

1.ipconfig



2. Netstat -an

```
C:\Users\aparn>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    0.0.0.0:3306           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:20080          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    0.0.0.0:49668          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49672          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49676          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49677          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49678          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49679          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49680          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49692          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:7080         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:27017        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:49686        127.0.0.1:49687        ESTABLISHED
  TCP    127.0.0.1:49687        127.0.0.1:49686        ESTABLISHED
  TCP    127.0.0.1:49688        127.0.0.1:49689        ESTABLISHED
  TCP    127.0.0.1:49689        127.0.0.1:49688        ESTABLISHED
  TCP    127.0.0.1:49713        127.0.0.1:49714        ESTABLISHED
  TCP    127.0.0.1:49714        127.0.0.1:49713        ESTABLISHED
  TCP    127.0.0.1:49715        127.0.0.1:49718        ESTABLISHED
  TCP    127.0.0.1:49716        127.0.0.1:49717        ESTABLISHED
  TCP    127.0.0.1:49717        127.0.0.1:49716        ESTABLISHED
  TCP    127.0.0.1:49718        127.0.0.1:49715        ESTABLISHED
  TCP    192.168.109.208:139    0.0.0.0:0              LISTENING
  TCP    192.168.109.208:20080  192.168.109.208:49197  ESTABLISHED
  TCP    192.168.109.208:20080  192.168.109.208:49199  ESTABLISHED
  TCP    192.168.109.208:20080  192.168.109.208:49203  ESTABLISHED
  TCP    192.168.109.208:20080  192.168.109.208:49249  ESTABLISHED
  TCP    192.168.109.208:20080  192.168.109.208:49271  ESTABLISHED
```

```
  TCP    192.168.109.208:20080  192.168.109.208:65479  ESTABLISHED
  TCP    192.168.109.208:20080  192.168.109.208:65481  ESTABLISHED
  TCP    192.168.109.208:20080  192.168.109.208:65496  ESTABLISHED
  TCP    192.168.109.208:49152  57.144.159.32:443      CLOSE_WAIT
  TCP    192.168.109.208:49154  57.144.159.32:443      CLOSE_WAIT
  TCP    192.168.109.208:49156  57.144.159.32:443      CLOSE_WAIT
  TCP    192.168.109.208:49157  57.144.159.32:443      CLOSE_WAIT
  TCP    192.168.109.208:49158  57.144.159.32:443      CLOSE_WAIT
  TCP    192.168.109.208:49170  142.250.206.46:443     CLOSE_WAIT
  TCP    192.168.109.208:49177  57.144.157.32:443      CLOSE_WAIT
  TCP    192.168.109.208:49179  57.144.157.32:443      CLOSE_WAIT
  TCP    192.168.109.208:49197  35.190.10.96:443       ESTABLISHED
  TCP    192.168.109.208:49199  35.190.10.96:443       ESTABLISHED
  TCP    192.168.109.208:49200  35.190.10.96:443       ESTABLISHED
  TCP    192.168.109.208:49201  35.190.10.96:443       ESTABLISHED
  TCP    192.168.109.208:49203  34.227.4.145:443       ESTABLISHED
  TCP    192.168.109.208:49204  34.227.4.145:443       ESTABLISHED
  TCP    192.168.109.208:49223  172.64.146.98:443      CLOSE_WAIT
  TCP    192.168.109.208:49249  142.250.183.131:443    ESTABLISHED
  TCP    192.168.109.208:49251  142.250.176.3:443      CLOSE_WAIT
  TCP    192.168.109.208:49252  142.250.183.131:443    ESTABLISHED
  TCP    192.168.109.208:49256  142.250.176.3:443      CLOSE_WAIT
  TCP    192.168.109.208:49257  142.250.179.227:443    CLOSE_WAIT
  TCP    192.168.109.208:49258  142.250.183.131:443    CLOSE_WAIT
  TCP    192.168.109.208:49268  104.18.32.47:443       CLOSE_WAIT
  TCP    192.168.109.208:49271  104.18.32.47:443       ESTABLISHED
  TCP    192.168.109.208:49272  104.18.32.47:443       ESTABLISHED
  TCP    192.168.109.208:49273  104.18.32.47:443       ESTABLISHED
  TCP    192.168.109.208:49274  104.18.32.47:443       ESTABLISHED
  TCP    192.168.109.208:49276  104.18.32.47:443       CLOSE_WAIT
  TCP    192.168.109.208:49282  104.18.32.47:443       CLOSE_WAIT
  TCP    192.168.109.208:49286  104.18.32.47:443       CLOSE_WAIT
  TCP    192.168.109.208:49288  104.18.32.47:443       CLOSE_WAIT
  TCP    192.168.109.208:49289  104.18.32.47:443       ESTABLISHED
  TCP    192.168.109.208:49290  104.18.32.47:443       ESTABLISHED
  TCP    192.168.109.208:49294  104.18.32.47:443       CLOSE_WAIT
  TCP    192.168.109.208:49312  142.250.205.138:443    CLOSE_WAIT
  TCP    192.168.109.208:49313  35.190.80.1:443        CLOSE_WAIT
  TCP    192.168.109.208:49314  35.190.80.1:443        CLOSE_WAIT
  TCP    192.168.109.208:49332  3.233.158.24:443       ESTABLISHED
  TCP    192.168.109.208:49334  3.233.158.24:443       ESTABLISHED
```

```
UDP    0.0.0.0:500            *:*
UDP    0.0.0.0:4500           *:*
UDP    0.0.0.0:5050           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5355           *:*
UDP    0.0.0.0:50509          *:*
UDP    0.0.0.0:56504          23.211.60.142:443
UDP    0.0.0.0:59024          *:*
UDP    0.0.0.0:59058          *:*
UDP    0.0.0.0:59567          *:*
UDP    0.0.0.0:63101          *:*
UDP    0.0.0.0:63839          *:*
UDP    0.0.0.0:64929          23.33.114.33:443
UDP    127.0.0.1:1900         *:*
UDP    127.0.0.1:49664        127.0.0.1:49664
UDP    127.0.0.1:51285        *:*
UDP    192.168.109.208:137    *:*
UDP    192.168.109.208:138    *:*
UDP    192.168.109.208:1900   *:*
UDP    192.168.109.208:51284  *:*
UDP    [::]:500               *:*
UDP    [::]:4500              *:*
UDP    [::]:5353              *:*
UDP    [::]:5353              *:*
UDP    [::]:5353              *:*
UDP    [::]:5353              *:*
UDP    [::]:5355              *:*
UDP    [::]:50509             *:*
UDP    [::]:59024             *:*
UDP    [::]:59058             *:*
UDP    [::]:59567             *:*
UDP    [::]:63839             *:*
UDP    [::1]:1900             *:*
UDP    [::1]:51283            *:*
UDP    [fe80::89c9:937:8763:7e5f%12]:1900  *:*
```

3.Nslookup www.google.com

```
C:\Users\aparn>nslookup www.google.com
Server:  UnKnown
Address:  192.168.109.57

Non-authoritative answer:
Name:    www.google.com
Addresses:  2404:6800:4007:835::2004
          142.251.222.196
```

4. Tracert www.google.com

```
C:\Users\aparn>tracert www.google.com

Tracing route to www.google.com [2404:6800:4007:835::2004]
over a maximum of 30 hops:

  1    50 ms   206 ms     7 ms  2401:4900:2618:7490::b9
  2   166 ms    98 ms   107 ms  2401:4900:2618:7490:0:5b:4d27:ef40
  3     *        *        *     Request timed out.
  4   169 ms   102 ms   321 ms  2401:4900:0:c000::26
  5   248 ms   188 ms   197 ms  2401:4900:a:802f::3
  6     *      159 ms    97 ms  2404:a800:3a00:1::2c9
  7   106 ms   218 ms    92 ms  2404:a800::92
  8   224 ms   191 ms   102 ms  2001:4860:1:1::674
  9   221 ms    97 ms   303 ms  2404:6800:8202:2c0::1
 10   139 ms   208 ms    84 ms  2001:4860:0:1::5664
 11   391 ms   102 ms    99 ms  2001:4860:0:1::565d
 12   317 ms   187 ms   201 ms  pnmaaa-as-in-x04.1e100.net [2404:6800:4007:835::2004]

Trace complete.
```

5. Ping www.google.com

```
C:\Users\aparn>ping www.google.com

Pinging www.google.com [2404:6800:4007:835::2004] with 32 bytes of
Reply from 2404:6800:4007:835::2004: time=381ms
Reply from 2404:6800:4007:835::2004: time=127ms
Reply from 2404:6800:4007:835::2004: time=131ms
Reply from 2404:6800:4007:835::2004: time=144ms

Ping statistics for 2404:6800:4007:835::2004:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 127ms, Maximum = 381ms, Average = 195ms
```