Department of Computer Science & Engineering

COMPUTER NETWORKS

LAB-1

UE22CS251B

4th Semester, Academic Year 2023-2024

Date:25-01-2024

Name: V V Mohith	SRN:PES2UG22CS641	Section:-K

Task 1: Linux Interface Configuration (ifconfig / IP command)

STEP:-1

```
(base) vvmohith@Mohiths-MacBook-Pro ~ % ip addr show
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
        inet 127.0.0.1/8 lo0
        inet6 ::1/128
        inet6 fe80::1/64 scopeid 0x1
ap1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether ea:89:f3:ec:42:e4
        inet6 fe80::e889:f3ff:feec:42e4/64 scopeid 0xe
en0: flags=88e3<UP,BROADCAST,SMART,RUNNING,NOARP,SIMPLEX,MULTICAST> mtu 1500
        ether c8:89:f3:ec:42:e4
        inet 10.0.4.26/24 brd 10.0.4.255 en0
        inet6 fe80::82f:1fbd:7f9f:92f8/64 secured scopeid 0xf
        inet6 2409:40f2:100e:c650:1c7d:e41f:f61f:9cbe/64 autoconf secured
        inet6 2409:40f2:100e:c650:fd64:e76d:4a34:c776/64 autoconf temporary
        inet 192.0.0.2/32 brd 192.0.0.2 en0
        inet6 2409:40f2:100e:c650:1827:42cb:77b8:7565/64 clat46
awdl0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether d6:dc:60:38:18:47
        inet6 fe80::d4dc:60ff:fe38:1847/64 scopeid 0x10
llw0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether d6:dc:60:38:18:47
        inet6 fe80::d4dc:60ff:fe38:1847/64 scopeid 0x11
utun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1500
        inet6 fe80::797:95d3:273f:e7/64 scopeid 0x12
utun1: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1380
        inet6 fe80::c18c:2a9d:b8a6:60a0/64 scopeid 0x13
utun2: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 2000
        inet6 fe80::b662:ba23:1602:63ba/64 scopeid 0x14
utun3: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1000
        inet6 fe80::ce81:b1c:bd2c:69e/64 scopeid 0x15
utun4: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1380
        inet6 fe80::df58:f1a4:d0e5:d165/64 scopeid 0x16
utun5: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1380
        inet6 fe80::a613:870f:836b:460f/64 scopeid 0x17
```

Interface name	IP address (IPv4 / IPv6)	MAC address
Lo	127.0.0.1/8	00:00:00:00:00:00
enp0s5	10.211.55.3/24	10.211.55.255

Step :-2(To assign an IP address)

command used:-sudo ip addr add 10.0.11.641 dev enp0s5

```
(base) vvmohith@Mohiths-MacBook-Pro ~ % sudo ip addr add 10.0.11.641 dev en0
Password:
Executing: /usr/bin/sudo /sbin/ifconfig en0 add 10.0.11.641
ifconfig: 10.0.11.641: bad value
Usage: ip addr show [ dev STRING ]
       ip addr { add | del } PREFIX dev STRING
```

Step :-3(To activate and deactivate a network)

(I)Deactivating

command used:-sudo ifconfig enp0s5 down

```
(base) vvmohith@Mohiths-MacBook-Pro ~ % ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
        options=1203<RXCSUM,TXCSUM,TXSTATUS,SW_TIMESTAMP>
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
anpi0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether be:23:97:e5:c1:de
        media: none
        status: inactive
anpi2: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether be:23:97:e5:c1:e0
        media: none
        status: inactive
anpi1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether be:23:97:e5:c1:df
        media: none
        status: inactive
en4: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether be:23:97:e5:c1:be
        nd6 options=201<PERFORMNUD,DAD>
        media: none
        status: inactive
en5: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether be:23:97:e5:c1:bf
        nd6 options=201<PERFORMNUD,DAD>
        media: none
        status: inactive
en6: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether be:23:97:e5:c1:c0
        nd6 options=201<PERFORMNUD,DAD>
        media: none
        status: inactive
```

(II)Activating

command used:-sudo ifconfig enp0s5 up

```
en0: flags=88e3<UP,BROADCAST,SMART,RUNNING,NOARP,SIMPLEX,MULTICAST> mtu 1500
        options=6460<TSO4,TSO6,CHANNEL_IO,PARTIAL_CSUM,ZEROINVERT_CSUM>
        ether c8:89:f3:ec:42:e4
        inet 10.0.4.26 netmask 0xffffff00 broadcast 10.0.4.255
        inet6 fe80::82f:1fbd:7f9f:92f8%en0 prefixlen 64 secured scopeid 0xf
        inet6 2409:40f2:104b:9713:14f5:8b5:2eb9:61f5 prefixlen 64 autoconf secured
        inet6 2409:40f2:104b:9713:702d:b4d6:64b9:b172 prefixlen 64 autoconf temporary
        inet 192.0.0.2 netmask 0xffffffff broadcast 192.0.0.2
        inet6 2409:40f2:104b:9713:14d7:a7d1:963b:52d5 prefixlen 64 clat46
        nat64 prefix 64:ff9b:: prefixlen 96
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
awdl0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=6460<TSO4,TSO6,CHANNEL_IO,PARTIAL_CSUM,ZEROINVERT_CSUM>
        ether 2e:45:97:9c:d3:d1
        inet6 fe80::2c45:97ff:fe9c:d3d1%awdl0 prefixlen 64 scopeid 0x10
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
llw0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether 2e:45:97:9c:d3:d1
        inet6 fe80::2c45:97ff:fe9c:d3d1%llw0 prefixlen 64 scopeid 0x11
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: inactive
utun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1500
        inet6 fe80::797:95d3:273f:e7%utun0 prefixlen 64 scopeid 0x12
        nd6 options=201<PERFORMNUD,DAD>
utun1: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1380
        inet6 fe80::c18c:2a9d:b8a6:60a0%utun1 prefixlen 64 scopeid 0x13
        nd6 options=201<PERFORMNUD,DAD>
utun2: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 2000
        inet6 fe80::b662:ba23:1602:63ba%utun2 prefixlen 64 scopeid 0x14
        nd6 options=201<PERFORMNUD,DAD>
utun3: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1000
        inet6 fe80::ce81:b1c:bd2c:69e%utun3 prefixlen 64 scopeid 0x15
        nd6 options=201<PERFORMNUD,DAD>
utun4: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1380
        inet6 fe80::df58:f1a4:d0e5:d165%utun4 prefixlen 64 scopeid 0x16
        nd6 options=201<PERFORMNUD,DAD>
utun5: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1380
        inet6 fe80::a613:870f:836b:460f%utun5 prefixlen 64 scopeid 0x17
        nd6 options=201<PERFORMNUD,DAD>
(base) vvmohith@Mohiths-MacBook-Pro ~ %
```

Step :-4(To show the current neighbor table)

Command used:-ip neigh

```
(base) vvmohith@Mohiths-MacBook-Pro ~ % ip neigh
2409:40f2:104b:9713:14d7:a7d1:963b:52d5 dev en0 lladdr c8:89:f3:ec:42:e4 REACHABLE
2409:40f2:104b:9713:14f5:8b5:2eb9:61f5 dev en0 lladdr c8:89:f3:ec:42:e4 REACHABLE
2409:40f2:104b:9713:1c85:2366:9475:41b1 dev en0 INCOMPLETE
2409:40f2:104b:9713:6cb9:b22e:355a:26b8 dev en0 lladdr 92:ec:ea:dc:29:64 router STALE
2409:40f2:104b:9713:702d:b4d6:64b9:b172 dev en0 lladdr c8:89:f3:ec:42:e4 REACHABLE
fe80::1 dev lo0 REACHABLE
fe80::e889:f3ff:feec:42e4 dev ap1 lladdr ea:89:f3:ec:42:e4 REACHABLE
fe80::82f:1fbd:7f9f:92f8 dev en0 lladdr c8:89:f3:ec:42:e4 REACHABLE
fe80::90ec:eaff:fedc:2964 dev en0 lladdr 92:ec:ea:dc:29:64 router REACHABLE
fe80::2c45:97ff:fe9c:d3d1 dev awdl0 lladdr 2e:45:97:9c:d3:d1 REACHABLE
fe80::2c45:97ff:fe9c:d3d1 dev llw0 lladdr 2e:45:97:9c:d3:d1 REACHABLE
fe80::797:95d3:273f:e7 dev utun0 REACHABLE
fe80::c18c:2a9d:b8a6:60a0 dev utun1 REACHABLE
fe80::b662:ba23:1602:63ba dev utun2 REACHABLE
fe80::ce81:b1c:bd2c:69e dev utun3 REACHABLE
fe80::df58:f1a4:d0e5:d165 dev utun4 REACHABLE
fe80::a613:870f:836b:460f dev utun5 REACHABLE
10.0.4.255 dev en0 lladdr ff:ff:ff:ff:ff:ff REACHABLE
192.0.0.1 dev en0 INCOMPLETE
192.0.0.2 dev en0 lladdr c8:89:f3:ec:42:e4 REACHABLE
224.0.0.251 dev en0 lladdr 1:0:5e:0:0:fb REACHABLE
```

Task 2: Ping PDU (Packet Data Units or Packets) Capture

Step 1: Assign an IP address to the system (Host).
Note: IP address of your system should be 10.0.your_section.your_sno.
Step 2: Launch Wireshark and select 'any' interface
Step 3: In terminal, type ping 10.0.your_section.your_sno
Observations to be made
Step 4: Analyze the following in Terminal

- **TTL**
- **Protocol used by ping**
- **Time**

Step 5: Analyze the following in Wireshark

Details	First Echo Request	First Echo Reply
Frame Number	10836	10838
Source IP address	10.1.1.22	192.168.254.1
Destination IP address	192.168.254.1	10.1.1.22
ICMP Type Value	3	3
ICMP Code Value	3	3
Source Ethernet Address	1c:57:dc:48:ef:0d	1c:57:dc:48:ef:0d
Destination Ethernet Address	3c:a8:2a:4a:d7:80	3c:a8:2a:4a:d7:80
Internet Protocol	4	4
Time to Live (TTL) value	64	62

Task 3: HTTP PDU Capture

Step 1: Launch Wireshark and select 'any' interface. On the Filter toolbar, type-in 'http' and

press enter

Step 2: Open Firefox browser, and browse www.flipkart.com

Observations to be made

Step 3: Analyze the first (interaction of host to the web server) and second frame (response

of server to the client). By analyzing the filtered frames, complete the table below:

Details	First Echo Request	First Echo Reply
Frame Number	260	269
Source Port	53652	443
Destination Port	443	53652
Source IP Address	192.168.1.6	163.53.76.86
Destination IP Address	163.53.76.86	192.168.1.6
Source Ethernet Address	1c:57:dc:48:ef:0d	64:fb:92:5f:a1:c9
Destination Ethernet Address	64:fb:92:5f:a1:c9	1c:57:dc:48:ef:0d

Step 4: Analyze the HTTP request and response and complete the table below.

HTTP Request		HTTP Response	
Get	HTTP/1.1	Server	Microsoft-IIS/10.0\r\n
St	Host	Content-Type	application/json

User-Agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36\r\n	Date	Wed, 17 Jan 2024 10:49:11 GMT
Accept-Language	en-IN,en-GB;q=0.9,en;q=0.8\r\n	Location	None
Accept-Encoding	gzip, deflate\r\n	Content-Length	724
Connection	keep-alive\r\n	Connection	keep-alive\r\n

Task 4: Capturing packets with tcpdump

Step 1: Use the command tcpdump -D to see which interfaces are available for capture.

sudo tcpdump -D

```
(base) vvmohith@Mohiths-MacBook-Pro ~ % tcpdump -D
1.en0 [Up, Running, Wireless, Associated]
2.awdl0 [Up, Running, Wireless, Associated]
3.llw0 [Up, Running, Wireless, Not associated]
4.utun0 [Up, Running]
5.utun1 [Up, Running]
6.utun2 [Up, Running]
7.utun3 [Up, Running]
8.utun4 [Up, Running]
9.utun5 [Up, Running]
10.lo0 [Up, Running, Loopback]
11.anpi0 [Up, Running, Disconnected]
12.anpi2 [Up, Running, Disconnected]
13.anpi1 [Up, Running, Disconnected]
14.en4 [Up, Running, Disconnected]
15.en5 [Up, Running, Disconnected]
16.en6 [Up, Running, Disconnected]
17.en1 [Up, Running, Disconnected]
18.en2 [Up, Running, Disconnected]
19.en3 [Up, Running, Disconnected]
20.bridge0 [Up, Running, Disconnected]
21.ap1 [Up, Running, Disconnected]
22.gif0 [none]
23.stf0 [none]
```

Step 2: Capture all packets in any interface by running this command: sudo tcpdump -i any

```
(base) vvmohith@Mohiths-MacBook-Pro ~ % sudo tcpdump -i any
Password:
tcpdump: data link type PKTAP
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on any, link-type PKTAP (Apple DLT_PKTAP), snapshot length 524288 bytes
11:34:35.040077 IP6 ec2-35-81-90-104.us-west-2.compute.amazonaws.com.https > 2409:40f2:104a:5da8:3df6:d183:4b4:e797.54100: Flags [P.], seq 2792579226:2792579272, ack 2692217658, win 189, options [nop,nop,TS val 333
7861195 ecr 2101928169], length 46
11:34:35.040080 IP6 ec2-35-81-90-104.us-west-2.compute.amazonaws.com.https > 2409:40f2:104a:5da8:3df6:d183:4b4:e797.54100: Flags [P.], seq 46:77, ack 1, win 189, options [nop,nop,TS val 3337861195 ecr 2101928169],
length 31
11:34:35.040082 IP6 ec2-35-81-90-104.us-west-2.compute.amazonaws.com.https > 2409:40f2:104a:5da8:3df6:d183:4b4:e797.54100: Flags [F.], seq 77, ack 1, win 189, options [nop,nop,TS val 3337861195 ecr 2101928169], len
gth 0
11:34:35.040376 IP6 2409:40f2:104a:5da8:3df6:d183:4b4:e797.54100 > ec2-35-81-90-104.us-west-2.compute.amazonaws.com.https: Flags [.], ack 77, win 2046, options [nop,nop,TS val 2101988074 ecr 3337861195], length 0
11:34:35.040545 IP6 2409:40f2:104a:5da8:3df6:d183:4b4:e797.54100 > ec2-35-81-90-104.us-west-2.compute.amazonaws.com.https: Flags [.], ack 78, win 2046, options [nop,nop,TS val 2101988074 ecr 3337861195], length 0
11:34:35.040843 IP6 2409:40f2:104a:5da8:3df6:d183:4b4:e797.54100 > ec2-35-81-90-104.us-west-2.compute.amazonaws.com.https: Flags [P.], seq 1:32, ack 78, win 2048, options [nop,nop,TS val 2101988074 ecr 3337861195],
 length 31
11:34:35.040947 IP6 2409:40f2:104a:5da8:3df6:d183:4b4:e797.54100 > ec2-35-81-90-104.us-west-2.compute.amazonaws.com.https: Flags [F.], seq 32, ack 78, win 2048, options [nop,nop,TS val 2101988074 ecr 3337861195], l
ength 0
11:34:35.120627 IP6 mohiths-macbook-pro.local.58633 > fe80::90ec:eaff:fedc:2964.domain: 36104+ PTR? 7.9.7.e.4.b.4.0.3.8.1.d.6.f.d.3.8.a.d.5.a.4.0.1.2.f.0.4.9.0.4.2.ip6.arpa. (90)
11:34:35.157004 IP6 fe80::90ec:eaff:fedc:2964.domain > mohiths-macbook-pro.local.58633: 36104 NXDomain 0/1/0 (178)
11:34:35.299485 IP6 ec2-35-81-90-104.us-west-2.compute.amazonaws.com.https > 2409:40f2:104a:5da8:3df6:d183:4b4:e797.54100: Flags [R], seq 2792579304, win 0, length 0
11:34:35.304960 IP6 ec2-35-81-90-104.us-west-2.compute.amazonaws.com.https > 2409:40f2:104a:5da8:3df6:d183:4b4:e797.54100: Flags [R], seq 2792579304, win 0, length 0
11:34:35.375768 IP localhost.mdns > mdns.mcast.net.mdns: 0 PTR (QU)? 4.6.9.2.c.d.e.f.f.f.a.e.c.e.0.9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
11:34:35.375799 IP localhost.mdns > mdns.mcast.net.mdns: 0 PTR (QU)? 4.6.9.2.c.d.e.f.f.f.a.e.c.e.0.9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
11:34:35.375945 IP6 mohiths-macbook-pro.local.mdns > ff02::fb.mdns: 0 PTR (QU)? 4.6.9.2.c.d.e.f.f.f.a.e.c.e.0.9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
11:34:35.375963 IP6 mohiths-macbook-pro.local.mdns > ff02::fb.mdns: 0 PTR (QU)? 4.6.9.2.c.d.e.f.f.f.a.e.c.e.0.9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
11:34:35.376064 IP6 mohiths-macbook-pro.local.mdns > ff02::fb.mdns: 0 PTR (QU)? 4.6.9.2.c.d.e.f.f.f.a.e.c.e.0.9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
11:34:35.376082 IP6 mohiths-macbook-pro.local.mdns > ff02::fb.mdns: 0 PTR (QU)? 4.6.9.2.c.d.e.f.f.f.a.e.c.e.0.9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
11:34:35.376097 IP6 mohiths-macbook-pro.local.mdns > ff02::fb.mdns: 0 PTR (QU)? 4.6.9.2.c.d.e.f.f.f.a.e.c.e.0.9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
11:34:35.376182 IP 192.0.0.2.mdns > mdns.mcast.net.mdns: 0 PTR (QU)? 4.6.9.2.c.d.e.f.f.f.a.e.c.e.0.9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
11:34:35.376208 IP 192.0.0.2.mdns > mdns.mcast.net.mdns: 0 PTR (QU)? 4.6.9.2.c.d.e.f.f.f.a.e.c.e.0.9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
11:34:35.376210 IP 192.0.0.2.mdns > mdns.mcast.net.mdns: 0 PTR (QU)? 4.6.9.2.c.d.e.f.f.f.a.e.c.e.0.9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
11:34:35.376287 IP6 mohiths-macbook-pro.local.mdns > ff02::fb.mdns: 0 PTR (QU)? 4.6.9.2.c.d.e.f.f.f.a.e.c.e.0.9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
11:34:35.376295 IP6 mohiths-macbook-pro.local.mdns > ff02::fb.mdns: 0 PTR (QU)? 4.6.9.2.c.d.e.f.f.f.a.e.c.e.0.9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
11:34:35.376333 IP6 mohiths-macbook-pro.local.mdns > ff02::fb.mdns: 0 PTR (QU)? 4.6.9.2.c.d.e.f.f.f.a.e.c.e.0.9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
11:34:36.379599 IP localhost.mdns > mdns.mcast.net.mdns: 0 PTR (QM)? 4.6.9.2.c.d.e.f.f.f.a.e.c.e.0.9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
11:34:36.379645 IP localhost.mdns > mdns.mcast.net.mdns: 0 PTR (QM)? 4.6.9.2.c.d.e.f.f.f.a.e.c.e.0.9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
11:34:36.379787 IP6 mohiths-macbook-pro.local.mdns > ff02::fb.mdns: 0 PTR (QM)? 4.6.9.2.c.d.e.f.f.f.a.e.c.e.0.9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
11:34:36.379808 IP6 mohiths-macbook-pro.local.mdns > ff02::fb.mdns: 0 PTR (QM)? 4.6.9.2.c.d.e.f.f.f.a.e.c.e.0.9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
11:34:36.379868 IP6 mohiths-macbook-pro.local.mdns > ff02::fb.mdns: 0 PTR (QM)? 4.6.9.2.c.d.e.f.f.f.a.e.c.e.0.9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
11:34:36.379879 IP6 mohiths-macbook-pro.local.mdns > ff02::fb.mdns: 0 PTR (QM)? 4.6.9.2.c.d.e.f.f.f.a.e.c.e.0.9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
11:34:36.379907 IP6 mohiths-macbook-pro.local.mdns > ff02::fb.mdns: 0 PTR (QM)? 4.6.9.2.c.d.e.f.f.f.a.e.c.e.0.9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
11:34:36.379964 IP 192.0.0.2.mdns > mdns.mcast.net.mdns: 0 PTR (QM)? 4.6.9.2.c.d.e.f.f.f.a.e.c.e.0.9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
11:34:36.379987 IP 192.0.0.2.mdns > mdns.mcast.net.mdns: 0 PTR (QM)? 4.6.9.2.c.d.e.f.f.f.a.e.c.e.0.9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
11:34:36.380028 IP 192.0.0.2.mdns > mdns.mcast.net.mdns: 0 PTR (QM)? 4.6.9.2.c.d.e.f.f.f.a.e.c.e.0.9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
11:34:36.380103 IP6 mohiths-macbook-pro.local.mdns > ff02::fb.mdns: 0 PTR (QM)? 4.6.9.2.c.d.e.f.f.f.a.e.c.e.0.9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
11:34:36.380114 IP6 mohiths-macbook-pro.local.mdns > ff02::fb.mdns: 0 PTR (QM)? 4.6.9.2.c.d.e.f.f.f.a.e.c.e.0.9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
11:34:36.380135 IP6 mohiths-macbook-pro.local.mdns > ff02::fb.mdns: 0 PTR (QM)? 4.6.9.2.c.d.e.f.f.f.a.e.c.e.0.9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
11:34:37.190818 IP6 2409:40f2:104a:5da8:28a5:b99a:7035:d420 > 2409:40f2:104a:5da8:c77:3eeb:f89d:74a1: ICMP6, neighbor solicitation, who has 2409:40f2:104a:5da8:c77:3eeb:f89d:74a1, length 32
11:34:38.418924 IP6 2409:40f2:104a:5da8:28a5:b99a:7035:d420 > 2409:40f2:104a:5da8:c77:3eeb:f89d:74a1: ICMP6, neighbor solicitation, who has 2409:40f2:104a:5da8:c77:3eeb:f89d:74a1, length 32
11:34:39.340218 IP6 2409:40f2:104a:5da8:28a5:b99a:7035:d420 > 2409:40f2:104a:5da8:c77:3eeb:f89d:74a1: ICMP6, neighbor solicitation, who has 2409:40f2:104a:5da8:c77:3eeb:f89d:74a1, length 32
11:34:39.386370 IP localhost.mdns > mdns.mcast.net.mdns: 0 PTR (QM)? 4.6.9.2.c.d.e.f.f.f.a.e.c.e.0.9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
11:34:39.386417 IP localhost.mdns > mdns.mcast.net.mdns: 0 PTR (QM)? 4.6.9.2.c.d.e.f.f.f.a.e.c.e.0.9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
11:34:39.386651 IP6 mohiths-macbook-pro.local.mdns > ff02::fb.mdns: 0 PTR (QM)? 4.6.9.2.c.d.e.f.f.f.a.e.c.e.0.9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
11:34:39.386671 IP6 mohiths-macbook-pro.local.mdns > ff02::fb.mdns: 0 PTR (QM)? 4.6.9.2.c.d.e.f.f.f.a.e.c.e.0.9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
```

Step-4 : To filter packets based on protocol, specifying the protocol in the command line. For

example, capture ICMP packets only by using this command:

sudo tcpdump -i any -c5 icmp

```
(base) vvmohith@Mohiths-MacBook-Pro ~ % sudo tcpdump -i any -c5 icmp
tcpdump: data link type PKTAP
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on any, link-type PKTAP (Apple DLT_PKTAP), snapshot length 524288 bytes
11:36:53.371714 IP localhost > localhost: ICMP localhost udp port 32376 unreachable, length 36
11:36:53.371719 IP localhost > localhost: ICMP localhost udp port 32376 unreachable, length 36
11:36:53.371844 IP localhost > localhost: ICMP localhost udp port 32376 unreachable, length 36
11:36:53.371845 IP localhost > localhost: ICMP localhost udp port 32376 unreachable, length 36
11:36:53.371987 IP localhost > localhost: ICMP localhost udp port 32376 unreachable, length 36
5 packets captured
2043 packets received by filter
0 packets dropped by kernel
(base) vvmohith@Mohiths-MacBook-Pro ~ %
```

Step 5: Check the packet content. For example, inspect the HTTP content of a web request

like this:

sudo tcpdump -i any -c10 -nn -A port 80

```
(base) vvmohith@Mohiths-MacBook-Pro ~ % sudo tcpdump -i any -c10 -nn -A port 80
tcpdump: data link type PKTAP
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on any, link-type PKTAP (Apple DLT_PKTAP), snapshot length 524288 bytes
12:02:49.588287 IP6 2409:40f2:100e:c650:fd64:e76d:4a34:c776.54142 > 64:ff9b::12ec:241c.80: Flags [SEW], seq 1504209167, win 65535, options [mss 1240,nop,wscale 6,nop,nop,TS val
0
`....,.@$       @....P.d.mJ4.v.d............$..~.PY.i.........6.............
.."..........
12:02:49.588548 IP6 2409:40f2:100e:c650:fd64:e76d:4a34:c776.54143 > 64:ff9b::12ec:241c.80: Flags [SEW], seq 2104956510, win 65535, options [mss 1240,nop,wscale 6,nop,nop,TS val
0
`....,.@$       @....P.d.mJ4.v.d............$....P}w.^.......................
............
12:02:49.845070 IP6 64:ff9b::12ec:241c.80 > 2409:40f2:100e:c650:fd64:e76d:4a34:c776.54142: Flags [S.E], seq 837676144, ack 1504209168, win 26847, options [mss 1260,sackOK,TS val
 8], length 0
`....(...d............$.$       @....P.d.mJ4.v.P.~1..pY.i..Rh.n?.........
.J....".....
12:02:49.845182 IP6 2409:40f2:100e:c650:fd64:e76d:4a34:c776.54142 > 64:ff9b::12ec:241c.80: Flags [.], ack 1, win 2053, options [nop,nop,TS val 3740476329 ecr 2622141868], length
`.... .@$       @....P.d.mJ4.v.d............$..~.PY.i.1..q.....].....
..#..J..
12:02:49.859128 IP6 64:ff9b::12ec:241c.80 > 2409:40f2:100e:c650:fd64:e76d:4a34:c776.54143: Flags [S.E], seq 3532510883, ack 2104956511, win 26847, options [mss 1260,sackOK,TS va
e 8], length 0
`....(...d............$.$       @....P.d.mJ4.v.P......}w._.Rh............
.J..........
12:02:49.859232 IP6 2409:40f2:100e:c650:fd64:e76d:4a34:c776.54143 > 64:ff9b::12ec:241c.80: Flags [.], ack 1, win 2053, options [nop,nop,TS val 2964691756 ecr 2622141881], length
`.... .@$       @....P.d.mJ4.v.d............$....P}w._........W......
...,.J..
12:02:50.769559 IP6 2409:40f2:100e:c650:fd64:e76d:4a34:c776.54142 > 64:ff9b::12ec:241c.80: Flags [P.], seq 1:491, ack 1, win 2053, options [nop,nop,TS val 3740477253 ecr 2622141
1
`....
.@$     @....P.d.mJ4.v.d............$..~.PY.i.1..q....b[.....
..'E.J..GET / HTTP/1.1
```

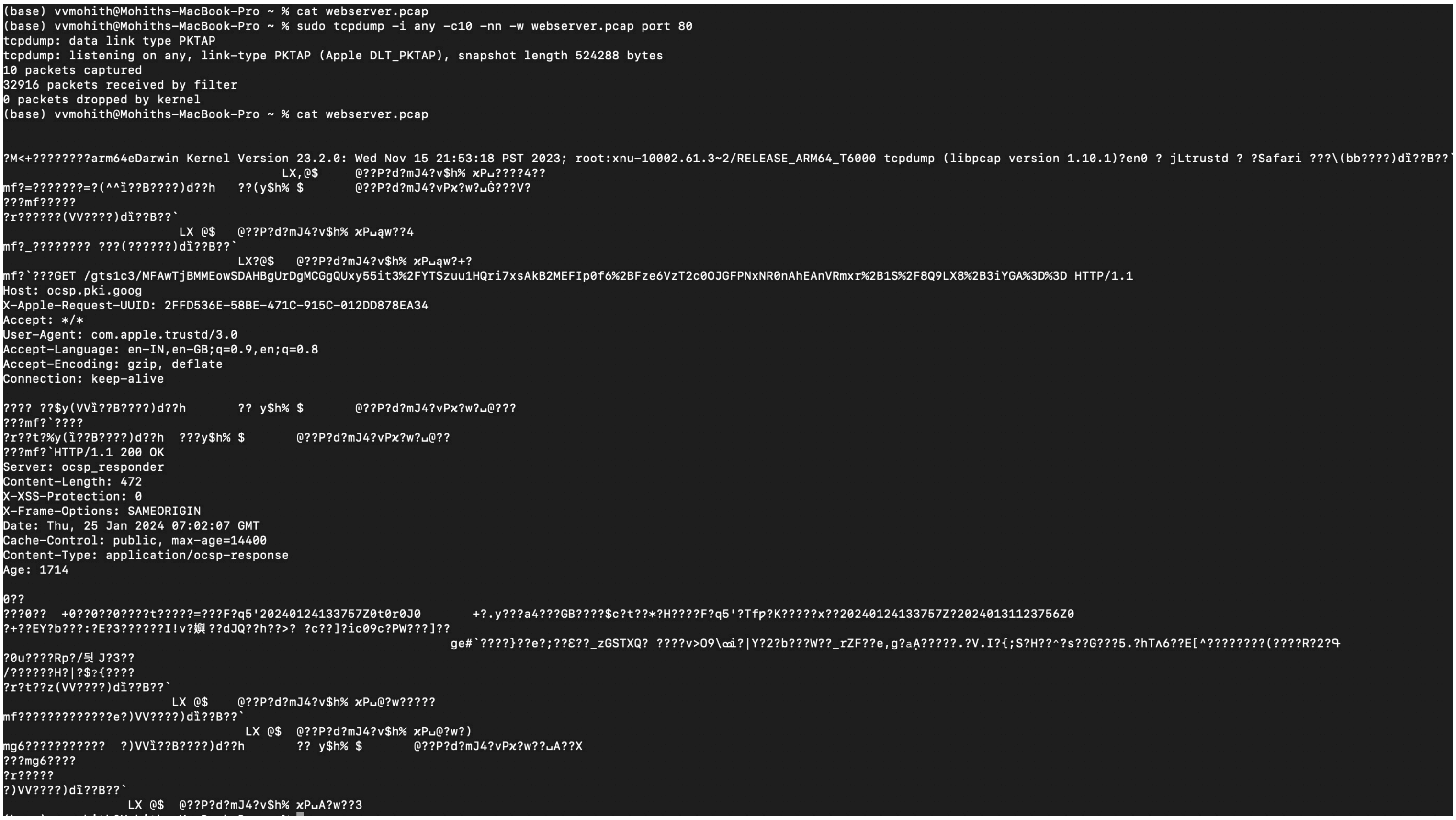
```
..'E.J..GET / HTTP/1.1
Host: www.testingmcafeesites.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: https://www.google.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,es;q=0.8


12:02:50.953785 IP6 2409:40f2:100e:c650:fd64:e76d:4a34:c776.54142 > 64:ff9b::12ec:241c.80: Flags [F.], seq 491, ack 1, win 2053, options [nop,nop,TS val 3740477437 ecr 26221418
`.... .@$       @....P.d.mJ4.v.d............$..~.PY.j.1..q...........
..'..J..
12:02:51.318158 IP6 64:ff9b::12ec:241c.80 > 2409:40f2:100e:c650:fd64:e76d:4a34:c776.54142: Flags [.], ack 1, win 105, options [nop,nop,TS val 2622143302 ecr 3740476329,nop,nop,
`...,...d............$.$       @....P.d.mJ4.v.P.~1..qY.i....i?......
.J.F..#....
Y.j.Y.j.
12:02:51.318270 IP6 2409:40f2:100e:c650:fd64:e76d:4a34:c776.54142 > 64:ff9b::12ec:241c.80: Flags [FP.], seq 1:491, ack 1, win 2053, options [nop,nop,TS val 3740477802 ecr 26221
.1
`....
.@$     @....P.d.mJ4.v.d............$..~.PY.i.1..q....Z......
..)j.J.FGET / HTTP/1.1
Host: www.testingmcafeesites.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: https://www.google.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,es;q=0.8


10 packets captured
3058 packets received by filter
0 packets dropped by kernel
```

<u>Step 6</u>: To save packets to a file instead of displaying them on screen, use the option -w:

sudo tcpdump -i any -c10 -nn -w webserver.pcap port 80

```
(base) vvmohith@Mohiths-MacBook-Pro ~ % sudo tcpdump -i any -c10 -nn -w webserve
r.pcap port 80
tcpdump: data link type PKTAP
tcpdump: listening on any, link-type PKTAP (Apple DLT_PKTAP), snapshot length 52
4288 bytes
10 packets captured
32916 packets received by filter
0 packets dropped by kernel
```

Command:-cat web server.pcap

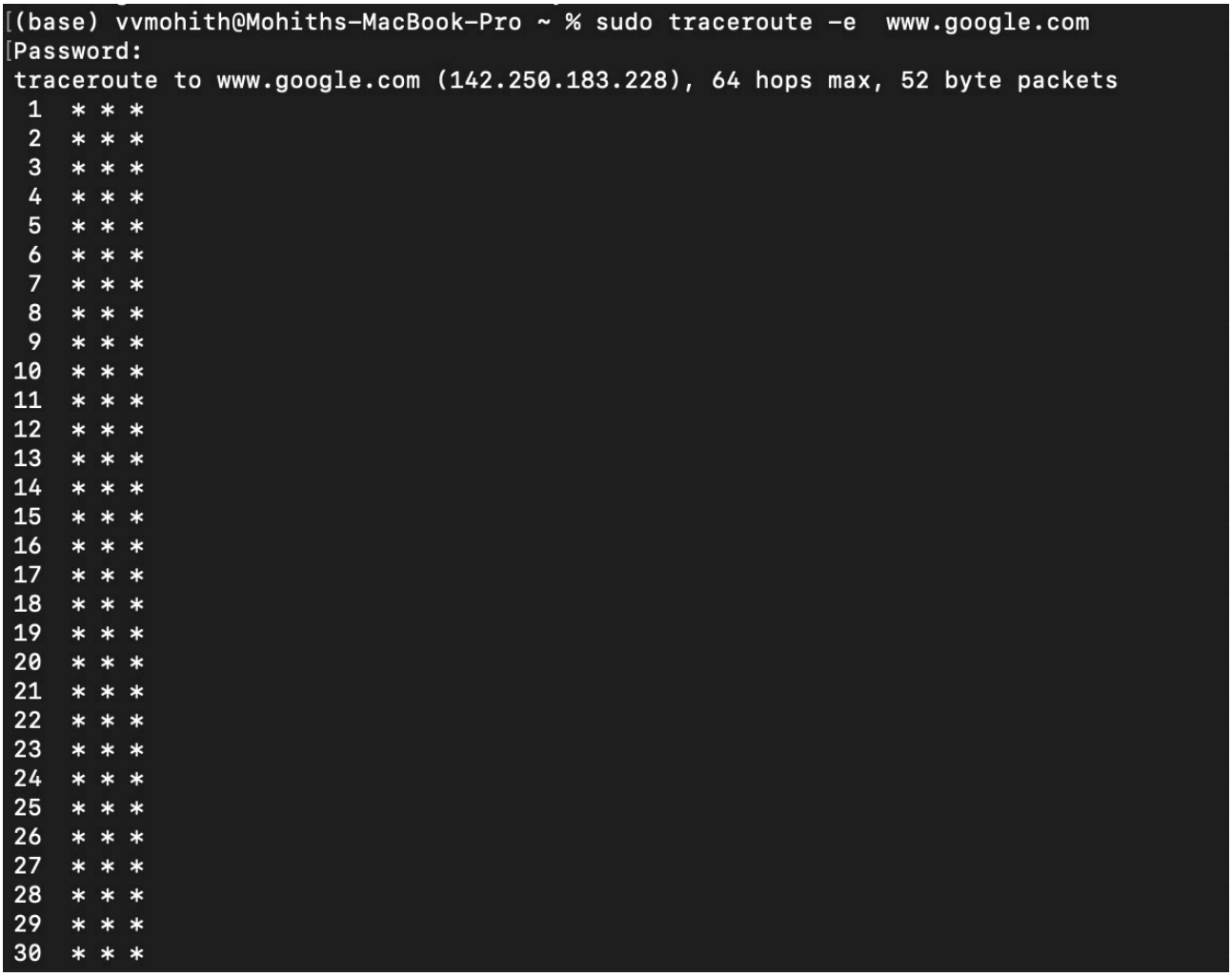


```
(base) vvmohith@Mohiths-MacBook-Pro ~ % cat webserver.pcap
(base) vvmohith@Mohiths-MacBook-Pro ~ % sudo tcpdump -i any -c10 -nn -w webserver.pcap port 80
tcpdump: data link type PKTAP
tcpdump: listening on any, link-type PKTAP (Apple DLT_PKTAP), snapshot length 524288 bytes
10 packets captured
32916 packets received by filter
0 packets dropped by kernel
(base) vvmohith@Mohiths-MacBook-Pro ~ % cat webserver.pcap


?M<+????????arm64eDarwin Kernel Version 23.2.0: Wed Nov 15 21:53:18 PST 2023; root:xnu-10002.61.3~2/RELEASE_ARM64_T6000 tcpdump (libpcap version 1.10.1)?en0 ? jLtrustd ? ?Safari ???\(bb????)dì??B??`
                                      LX,@$     @??P?d?mJ4?v$h% xP␣????4??
mf?=???????=?(^^ì??B????)d??h   ??(y$h% $       @??P?d?mJ4?vPx?w?␣Ġ???V?
???mf?????
?r??????(VV????)dì??B??`
                        LX @$   @??P?d?mJ4?v$h% xP␣ąw??4
mf?_???????? ???(??????)dì??B??`
                                LX?@$   @??P?d?mJ4?v$h% xP␣ąw?+?
mf?`???GET /gts1c3/MFAwTjBMMEowSDAHBgUrDgMCGgQUxy55it3%2FYTSzuu1HQri7xsAkB2MEFIp0f6%2BFze6VzT2c0OJGFPNxNR0nAhEAnVRmxr%2B1S%2F8Q9LX8%2B3iYGA%3D%3D HTTP/1.1
Host: ocsp.pki.goog
X-Apple-Request-UUID: 2FFD536E-58BE-471C-915C-012DD878EA34
Accept: */*
User-Agent: com.apple.trustd/3.0
Accept-Language: en-IN,en-GB;q=0.9,en;q=0.8
Accept-Encoding: gzip, deflate
Connection: keep-alive

???? ??$y(VVì??B????)d??h       ?? y$h% $       @??P?d?mJ4?vPx?w?␣@???
???mf?`????
?r??t?%y(ì??B????)d??h  ???y$h% $       @??P?d?mJ4?vPx?w?␣@??
???mf?`HTTP/1.1 200 OK
Server: ocsp_responder
Content-Length: 472
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
Date: Thu, 25 Jan 2024 07:02:07 GMT
Cache-Control: public, max-age=14400
Content-Type: application/ocsp-response
Age: 1714

0??
???0??  +0??0??0????t?????=???F?q5'20240124133757Z0t0r0J0       +?.y???a4???GB????$c?t??*?H????F?q5'?Tfp?K?????x??20240124133757Z?20240131123756Z0
?+??EY?b???:?E?3??????I!v?嬩??dJQ??h??>? ?c??]?ic09c?PW???]??
                                                             ge#`????}??e?;??Ɛ??_zGSTXQ? ????v>O9\ꝏi?|Y?2?b???W??_rZF??e,g?aẠ?????.?V.I?{;S?H??^?s??G???5.?hTʌ6??E[^????????(????R?2?
?0u????Rp?/뒷 J?3??
/??????H?|?$?{????
?r?t??z(VV????)dì??B??`
                       LX @$    @??P?d?mJ4?v$h% xP␣@?w?????
mf?????????????e?)VV????)dì??B??`
                                 LX @$  @??P?d?mJ4?v$h% xP␣@?w?)
mg6???????????  ?)VVì??B????)d??h       ?? y$h% $       @??P?d?mJ4?vPx?w??␣A??X
???mg6????
?r?????
?)VV????)dì??B??`
                 LX @$  @??P?d?mJ4?v$h% xP␣A?w??3
```

Task 5: Perform Traceroute checks

<u>Step 1</u>: Run the traceroute using the following command.

sudo traceroute www.google.com



Step 2: Analyze destination address of google.com and no. of hops

Observations => Destination adds:-142.250.183.228

Hops:-64

Step 3: To speed up the process, you can disable the mapping of IP addresses with hostnames by using the -n option

sudo traceroute -n www.google.com

```
(base) vvmohith@Mohiths-MacBook-Pro ~ % sudo traceroute -n www.google.com
Password:
traceroute to www.google.com (142.250.196.68), 64 hops max, 52 byte packets
 1  * * *
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
```

Step 4: The -I option is necessary so that the traceroute uses ICMP.

sudo traceroute -I www.google.com

```
(base) vvmohith@Mohiths-MacBook-Pro ~ % sudo traceroute -I www.google.com
Password:
traceroute to www.google.com (142.250.195.164), 64 hops max, 72 byte packets
 1  * * *
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  maa03s41-in-f4.1e100.net (142.250.195.164)  39.694 ms  23.745 ms  31.833 ms
```

Step 5: By default, traceroute uses icmp (ping) packets. If you'd rather test a TCP connection
to gather data more relevant to web server, you can use the -T flag.

sudo traceroute -T www.google.com

```
(base) vvmohith@Mohiths-MacBook-Pro ~ % sudo traceroute -I www.google.com
Password:
traceroute to www.google.com (142.250.195.164), 64 hops max, 72 byte packets
 1  * * *
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  maa03s41-in-f4.1e100.net (142.250.195.164)  39.694 ms  23.745 ms  31.833 ms
```

Task 6: Explore an entire network for information (Nmap)

Step 1: You can scan a host using its host name or IP address, for instance.

Command -> nmap www.pes.edu

```
(base) vvmohith@Mohiths-MacBook-Pro ~ % nmap www.pes.edu
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-25 13:23 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.30 seconds
```

Step 2: Alternatively, use an IP address to scan.
nmap 163.53.78.128

Command -> map 163.53.78.128

```
(base) vvmohith@Mohiths-MacBook-Pro ~ % nmap 163.53.78.128
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-25 13:25 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.11 seconds
```

Step 3: Scan multiple IP address or subnet (IPv4)

Command -> nmap 192.168.1.1 192.168.1.2 192.168.1.3

```
(base) vvmohith@Mohiths-MacBook-Pro ~ % nmap 192.168.1.1 192.168.1.2 192.168.1.3
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-25 13:26 IST
Strange read error from 192.168.1.2 (4 - 'Interrupted system call')
Strange read error from 192.168.1.3 (4 - 'Interrupted system call')
Strange read error from 192.168.1.1 (4 - 'Interrupted system call')
Strange read error from 192.168.1.2 (4 - 'Interrupted system call')
Strange read error from 192.168.1.3 (4 - 'Interrupted system call')
Strange read error from 192.168.1.1 (4 - 'Interrupted system call')
Nmap done: 3 IP addresses (0 hosts up) scanned in 0.08 seconds
```

Disclaimer:

- The programs and output submitted is duly written, verified and executed by me.
- I have not copied from any of my peers nor from the external resource such as internet.
- If found plagiarized, I will abide with the disciplinary action of the University.

Signature:

SRN:PES2UG22CS641

Section: K

Date:25-01-2024

Name:V V Mohith