NWEN243 Project 1 – Sahil Adwani

Q1)

```
[Wed Aug 07 10:33:37] adwanisahi@ip-172-31-94-211: ~$ ip address show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enX0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 12:a5:85:24:1e:a1 brd ff:ff:ff:ff:ff:ff
    inet 172.31.94.211/20 metric 100 brd 172.31.95.255 scope global dynamic enX0
       valid_lft 2431sec preferred_lft 2431sec
    inet6 fe80::10a5:85ff:fe24:1ea1/64 scope link
       valid_lft forever preferred_lft forever
[Wed Aug 07 10:34:31] adwanisahi@ip-172-31-94-211: ~$
```

a) The name of the network interface controller (NIC) is "enX0"
b) The Mac Address in Hex of the NIC is "12:a5:85:24:1e:a1"
c) The full MAC address in binary is:
   00010010:10100101:10000101:00100100:00011110:10100001
d) The length of the MAC address is 48 bits (6 bytes x 8 bits).
e) The broadcast MAC address is ff:ff:ff:ff:ff:ff. This address is composed of all bits set to 1.
   11111111:11111111:11111111:11111111:11111111:11111111

Q2)

```
[Wed Aug 07 10:33:37] adwanisahi@ip-172-31-94-211: ~$ ip address show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enX0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 12:a5:85:24:1e:a1 brd ff:ff:ff:ff:ff:ff
    inet 172.31.94.211/20 metric 100 brd 172.31.95.255 scope global dynamic enX0
       valid_lft 2431sec preferred_lft 2431sec
    inet6 fe80::10a5:85ff:fe24:1ea1/64 scope link
       valid_lft forever preferred_lft forever
[Wed Aug 07 10:34:31] adwanisahi@ip-172-31-94-211: ~$
```

```
[Wed Aug 07 11:25:21] adwanisahi@ip-172-31-94-211: ~$
```

i-06452d9912199551d (NWEN243_P1)

PublicIPs: 35.174.5.125 PrivateIPs: 172.31.94.211

a) Private IPv4: 172.31.94.211, Public IPv4: 35.174.5.125
b) Private IPv6 Address: fe80::10a5:85ff:fe24:1ea1
c) IPv4 Address Length is 32 bits (4x8)
d) IPv4 Binary: 00100011.10101110.00000101.01111101
e) Private IPv6 Address Length: IPv6 addresses are 128 bits long.

Q3)

```
[Wed Aug 07 10:33:37] adwanisahi@ip-172-31-94-211: ~$ ip address show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enX0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 12:a5:85:24:1e:a1 brd ff:ff:ff:ff:ff:ff
    inet 172.31.94.211/20 metric 100 brd 172.31.95.255 scope global dynamic enX0
       valid_lft 2431sec preferred_lft 2431sec
    inet6 fe80::10a5:85ff:fe24:1ea1/64 scope link
       valid_lft forever preferred_lft forever
[Wed Aug 07 10:34:31] adwanisahi@ip-172-31-94-211: ~$
```

a) The network portion is 172.31.80.0 (the first 20 bits) and the host portion is the remaining bits (12 bits and so 0.0.14.211)

b) Range: 172.31.80.0 to 172.31.95.255.

c) There can be 2^(32-20) - 2 = 4094 distinct IPv4 addresses in this LAN.

Q4)

```
[Thu Aug 08 12:37:56] adwanisahi@ip-172-31-94-211: ~$ ip address show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enX0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 12:a5:85:24:1e:a1 brd ff:ff:ff:ff:ff:ff
    inet 172.31.94.211/20 metric 100 brd 172.31.95.255 scope global dynamic enX0
       valid_lft 2525sec preferred_lft 2525sec
    inet6 fe80::10a5:85ff:fe24:1ea1/64 scope link
       valid_lft forever preferred_lft forever
```

a) Netmask: 255.255.240.0
b) broadcast IPv4 address: 172.31.95.255.
c) Calculate the broadcast address by applying the netmask to the IPv4 address to find the network portion, then set all host bits to 1 to get the broadcast address.

Q5)

```
[Thu Aug 08 12:47:25] adwanisahi@ip-172-31-94-211: ~$ ip route list
default via 172.31.80.1 dev enX0 proto dhcp src 172.31.94.211 metric 100
172.31.0.2 via 172.31.80.1 dev enX0 proto dhcp src 172.31.94.211 metric 100
172.31.80.0/20 dev enX0 proto kernel scope link src 172.31.94.211 metric 100
172.31.80.1 dev enX0 proto dhcp scope link src 172.31.94.211 metric 100
[Thu Aug 08 13:13:12] adwanisahi@ip-172-31-94-211: ~$
```

a) The default via 172.31.80.1 route directs all traffic not matching other routes to the gateway 172.31.80.1 through interface enX0. This route was set by DHCP, using IP 172.31.94.211 with a priority metric of 100. It is the default route for unspecified destinations.

```
[Thu Aug 08 13:13:12] adwanisahi@ip-172-31-94-211: ~$ ip neighbour show
172.31.80.1 dev enX0 lladdr 12:a9:d8:90:e6:cb REACHABLE
[Thu Aug 08 13:18:34] adwanisahi@ip-172-31-94-211: ~$
```

b) The IP neighbour show command shows IP 172.31.80.1 with MAC address 12:a9:d8:90:e6:cb. This mapping helps the VM use ARP to route (deliver) packets correctly within the LAN by associating IP addresses with MAC addresses.

Q6)

```
[Sat Aug 10 03:49:38] adwanisahi@ip-172-31-94-211: ~$ ping www.youtube.com
PING youtube-ui.l.google.com (142.251.16.91) 56(84) bytes of data.
64 bytes from bl-in-f91.1e100.net (142.251.16.91): icmp_seq=1 ttl=58 time=1.74 ms
64 bytes from bl-in-f91.1e100.net (142.251.16.91): icmp_seq=2 ttl=58 time=1.96 ms
64 bytes from bl-in-f91.1e100.net (142.251.16.91): icmp_seq=3 ttl=58 time=1.87 ms
64 bytes from bl-in-f91.1e100.net (142.251.16.91): icmp_seq=4 ttl=58 time=1.83 ms
^C
--- youtube-ui.l.google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 1.737/1.849/1.963/0.080 ms
[Sat Aug 10 03:54:41] adwanisahi@ip-172-31-94-211: ~$
```

a) IP Address from VM (IP1): 142.251.16.91

```
Windows PowerShell

PS C:\Users\adwan> ping www.youtube.com

Pinging youtube-ui.l.google.com [172.217.24.46] with 32 bytes of data:
Reply from 172.217.24.46: bytes=32 time=40ms TTL=115
Reply from 172.217.24.46: bytes=32 time=40ms TTL=115
Reply from 172.217.24.46: bytes=32 time=41ms TTL=115
Reply from 172.217.24.46: bytes=32 time=40ms TTL=115

Ping statistics for 172.217.24.46:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 40ms, Maximum = 41ms, Average = 40ms
PS C:\Users\adwan>
```

b) From the window terminal (PowerShell), shows an IP address of 172.217.24.46 (IP2).

c) The RTL from VM to IP1 is approximately 1.849 ms.

```
[Sat Aug 10 05:11:23] adwanisahi@ip-172-31-94-211: ~$ ping 172.217.24.46
PING 172.217.24.46 (172.217.24.46) 56(84) bytes of data.
64 bytes from 172.217.24.46: icmp_seq=1 ttl=107 time=198 ms
64 bytes from 172.217.24.46: icmp_seq=2 ttl=107 time=198 ms
64 bytes from 172.217.24.46: icmp_seq=3 ttl=107 time=198 ms
64 bytes from 172.217.24.46: icmp_seq=4 ttl=107 time=198 ms

--- 172.217.24.46 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 197.553/197.616/197.676/0.049 ms
^C[Sat Aug 10 05:14:49] adwanisahi@ip-172-31-94-211: ~$
```

The RTL from VM to IP2 is 198 ms.

```
PS C:\Users\adwan> ping 142.251.16.91

Pinging 142.251.16.91 with 32 bytes of data:
Reply from 142.251.16.91: bytes=32 time=254ms TTL=101
Reply from 142.251.16.91: bytes=32 time=234ms TTL=101
Reply from 142.251.16.91: bytes=32 time=232ms TTL=101
Reply from 142.251.16.91: bytes=32 time=234ms TTL=101

Ping statistics for 142.251.16.91:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 232ms, Maximum = 254ms, Average = 238ms
PS C:\Users\adwan>
```

The RTL from local machine(terminal) to IP1 is approximately 238ms

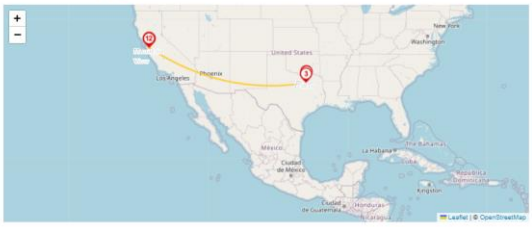
```
PS C:\Users\adwan> ping www.youtube.com

Pinging youtube-ui.l.google.com [172.217.24.46] with 32 bytes of data:
Reply from 172.217.24.46: bytes=32 time=40ms TTL=115
Reply from 172.217.24.46: bytes=32 time=40ms TTL=115
Reply from 172.217.24.46: bytes=32 time=41ms TTL=115
Reply from 172.217.24.46: bytes=32 time=40ms TTL=115

Ping statistics for 172.217.24.46:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 40ms, Maximum = 41ms, Average = 40ms
```

The RTL from local machine (terminal) to IP2 is approximately 40 ms.

d) The differing RTLs indicate that IP1 and IP2 are likely associated with different geographic locations or data centres. The VM and local machine experience varying latencies due to differences in network paths and load balancing, with IP1 closer to the VM and IP2 closer to the local machine.

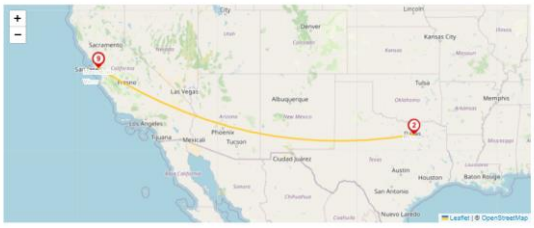
Q7)

Traceroute to 142.251.16.91 from United States of America



Hop	IP Address	Hostname	Location	ASN	Time
1	192.111.142.1	192.111.142.1	United States of America, Texas, Plano	AS 46562	0.257 ms
2	104.200.142.38	104.200.142.38	United States of America, Texas, Plano	AS 46562	0.261 ms
3	104.200.142.36	104.200.142.36	United States of America, Texas, Dallas	AS 46562	0.269 ms
4	209.85.251.253	209.85.251.253	United States of America, California, Mountain View	AS 15169	1.006 ms
5	142.251.253.102	142.251.253.102	United States of America, California, Mountain View	AS 15169	1.759 ms
6	142.251.253.102	142.251.253.102	United States of America, California, Mountain View	AS 15169	1.499 ms
7	108.170.225.111	108.170.225.111	United States of America, California, Mountain View	AS 15169	2.444 ms
8	142.250.233.171	142.250.233.171	United States of America, California, Mountain View	AS 15169	2.811 ms
9	142.251.254.59	142.251.254.59	United States of America, California, Mountain View	AS 15169	26.619 ms
11	209.85.253.3	209.85.253.3	United States of America, California, Mountain View	AS 15169	34.055 ms
12	142.251.227.135	142.251.227.135	United States of America, California, Mountain View	AS 15169	33.669 ms
13	142.251.66.227	142.251.66.227	United States of America, California, Mountain View	AS 15169	32.754 ms

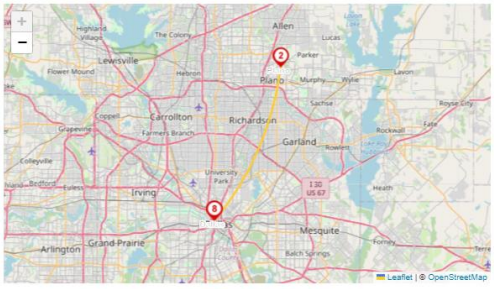
Traceroute to 172.217.24.46 from United States of America



Hop	IP Address	Hostname	Location	ASN	Time
1	192.111.142.1	192.111.142.1	United States of America, Texas, Plano	AS 46562	0.362 ms
2	199.36.220.176	199.36.220.176	United States of America, Texas, Plano	AS 46562	0.281 ms
4	172.253.73.17	172.253.73.17	United States of America, California, Mountain View	AS 15169	2.001 ms
5	216.239.59.79	216.239.59.79	United States of America, California, Mountain View	AS 15169	0.938 ms
6	108.170.228.79	108.170.228.79	United States of America, California, Mountain View	AS 15169	1.284 ms
9	192.178.245.7	192.178.245.7	United States of America, California, Mountain View	AS 15169	212.227 ms
10	192.178.97.69	192.178.97.69	United States of America, California, Mountain View	AS 15169	169.148 ms
11	216.239.57.119	216.239.57.119	United States of America, California, Mountain View	AS 15169	168.099 ms
12	216.239.56.69	216.239.56.69	United States of America, California, Mountain View	AS 15169	168.610 ms

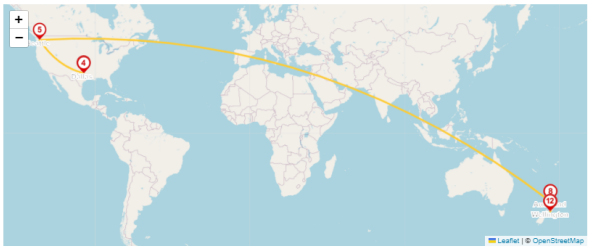
(a) Path to IP1 and IP2: Traceroute to IP1 (142.251.179.136) and IP2 (172.217.24.46) often shows routes through multiple U.S. states due to global network infrastructure. IP1 and IP2 may be located in different data centres, affecting routing paths. IP1 has 12 hops while IP2 has 9 hops.

Traceroute to 103.1.195.4 from United States of America



Hop	IP Address	Hostname	Location	ASN	Time
1	192.111.142.1	192.111.142.1	United States of America, Texas, Plano	AS 46562	0.271 ms
2	199.36.220.176	199.36.220.176	United States of America, Texas, Plano	AS 46562	0.213 ms
3	104.200.142.36	104.200.142.36	United States of America, Texas, Dallas	AS 46562	0.221 ms
4	141.101.74.205	141.101.74.205	United States of America, Texas, Dallas	AS 13335	2.007 ms
5	172.71.165.23	172.71.165.23	United States of America, Texas, Dallas	AS 13335	1.649 ms
6	172.71.173.105	172.71.173.105	United States of America, Texas, Dallas	AS 13335	1.570 ms
7	172.71.169.39	172.71.169.39	United States of America, Texas, Dallas	AS 13335	1.552 ms
8	172.68.25.209	172.68.25.209	United States of America, Texas, Dallas	AS 13335	1.573 ms

Traceroute to 130.195.6.22 from United States of America



Hop	IP Address	Hostname	Location	ASN	Time
1	192.111.142.1	192.111.142.1	United States of America, Texas, Plano	AS 46562	0.287 ms
2	104.200.142.38	104.200.142.38	United States of America, Texas, Plano	AS 46562	0.204 ms
3	69.174.3.53	et-3-0-0.cr8-dal3.ip4.gtt.net	United States of America, Texas, Dallas	AS 3257	1.113 ms
4	213.200.115.26	ae11.cr7-dal3.ip4.gtt.net	United States of America, Texas, Dallas	AS 3257	1.273 ms
7	4.53.158.194	RESEARCH-AN.ear2.Seattle1.Level3.net	United States of America, Washington, Seattle	AS 3356	43.518 ms
8	210.7.33.244	and33-hnl.reannz.co.nz	New Zealand, Auckland	AS 38022	91.723 ms
9	210.7.33.246	and31-mgw.reannz.co.nz	New Zealand, Auckland	AS 38022	172.724 ms
10	210.7.33.242	and12-nsh.reannz.co.nz	New Zealand, Auckland	AS 38022	174.150 ms
11	210.7.36.29	210.7.36.29	New Zealand, Greater Wellington, Wellington	AS 38022	183.440 ms
12	210.7.36.30	210.7.36.30	New Zealand, Greater Wellington, Wellington	AS 38022	184.076 ms
13	130.195.196.198	130.195.196.198	New Zealand, Greater Wellington, Wellington	AS 23905	183.587 ms
14	130.195.199.194	130.195.199.194	New Zealand, Greater Wellington, Wellington	AS 23905	184.182 ms

(b) Path to wgtn.ac.nz and barretts.ecs.vuw.ac.nz: Traceroute shows wgtn.ac.nz routed through Texas, indicating indirect routing. In contrast, barretts.ecs.vuw.ac.nz's path includes Texas, Washington, Auckland, and Wellington, reflecting a more direct route to New Zealand. Wgtn.ac.nz has 8 hops in U.S and Barretts.ecs.vuw.ac.nz has 12 hops (5 in US and 7 in NZ).

Q8)

```
[Sat Aug 10 06:29:35] adwanisahi@ip-172-31-94-211: ~$ sudo tcpdump -v -nn arp
tcpdump: listening on enX0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
06:33:16.395511 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 172.31.94.211 tell 172.31.80.1, length 28
06:33:16.395530 ARP, Ethernet (len 6), IPv4 (len 4), Reply 172.31.94.211 is-at 12:a5:85:24:1e:a1, length 28
06:34:13.797441 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 172.31.94.211 tell 172.31.80.1, length 28
06:34:13.797457 ARP, Ethernet (len 6), IPv4 (len 4), Reply 172.31.94.211 is-at 12:a5:85:24:1e:a1, length 28
06:35:13.816476 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 172.31.94.211 tell 172.31.80.1, length 28
06:35:13.816493 ARP, Ethernet (len 6), IPv4 (len 4), Reply 172.31.94.211 is-at 12:a5:85:24:1e:a1, length 28
^C
6 packets captured
6 packets received by filter
0 packets dropped by kernel
[Sat Aug 10 06:35:40] adwanisahi@ip-172-31-94-211: ~$
```

(a) Request-Reply Pair:

- Request: 172.31.80.1 asks "Who has IP 172.31.94.211?
  Sender: 172.31.80.1
  Purpose: Asking which device has IP address 172.31.94.211.
- Reply: 172.31.94.211 responds with its MAC address 12:a5:85:24:1e:a1
  Sender: 172.31.94.211
  Purpose: Responding with its MAC address (12:a5:85:24:1e:a1) for IP 172.31.94.211.

(b) Repeating ARP Requests: ARP requests are sent periodically to maintain up-to-date mappings of IP addresses to MAC addresses. This ensures that devices can quickly resolve addresses in case of network changes or timeouts.

c) ARP Request Interval: Based on the timestamps (06:33:16 to 06:34:13), ARP requests are sent approximately every 60 seconds.

Q9)

a)

```
[Sat Aug 10 09:03:25] adwanisahi@ip-172-31-94-211: ~$ journalctl | grep -i 'dhcp'
Aug 07 09:44:59 ubuntu dhcpcd[431]: dhcpcd-10.0.6 starting
Aug 07 09:44:59 ubuntu dhcpcd[434]: DUID 00:01:00:01:2e:45:fe:9b:12:a5:85:24:1e:a1
Aug 07 09:44:59 ubuntu dhcpcd[434]: enX0: IAID 85:24:1e:a1
Aug 07 09:45:01 ubuntu dhcpcd[434]: enX0: soliciting a DHCP lease
Aug 07 09:45:01 ubuntu dhcpcd[434]: enX0: offered 172.31.94.211 from 172.31.80.1
Aug 07 09:45:01 ubuntu dhcpcd[434]: enX0: leased 172.31.94.211 for 3600 seconds
Aug 07 09:45:01 ubuntu dhcpcd[434]: enX0: adding route to 172.31.80.0/20
Aug 07 09:45:01 ubuntu dhcpcd[434]: enX0: adding default route via 172.31.80.1
Aug 07 09:45:01 ubuntu dhcpcd[434]: control command: /usr/sbin/dhcpcd --dumplease --ipv4only enX0
Aug 07 09:45:02 ip-172-31-94-211 systemd-networkd[503]: enX0: DHCPv4 address 172.31.94.211/20, gateway 172.31.80.1 acquired from 172.31.80.1
Aug 07 11:56:15 ip-172-31-94-211 systemd-networkd[503]: enX0: DHCP lease lost
Aug 07 11:56:15 ip-172-31-94-211 systemd-networkd[503]: enX0: DHCPv6 lease lost
```

The 4-way DHCP interaction for the session includes:

1. Soliciting a DHCP Lease: The client sends a DHCP Discover message at Aug 07 09:45:01 to find DHCP servers.
2. Offered IP: 172.31.94.211 from DHCP server 172.31.80.1 to the client
3. Leased IP: The client accepts the offer and the IP address 172.31.94.211 is leased for 3600 seconds
4. Adding Routes: Indicates DHCP acknowledgment

The DHCP server is 172.31.80.1, and the lease duration is 3600 seconds.

b)

```
[Sat Aug 10 09:36:24] adwanisahi@ip-172-31-94-211: ~$ sudo netplan ip leases enX0
# This is private data. Do not parse.
ADDRESS=172.31.94.211
NETMASK=255.255.240.0
ROUTER=172.31.80.1
SERVER_ADDRESS=172.31.80.1
MTU=9001
T1=30min
T2=52min 30s
LIFETIME=1h
DNS=172.31.0.2
DOMAINNAME=ec2.internal
HOSTNAME=ip-172-31-94-211
CLIENTID=ffcde6748200020000ab1152a558663a27721b
[Sat Aug 10 09:36:48] adwanisahi@ip-172-31-94-211: ~$
```

Main Information:

- IP Address: Assigned address (172.31.94.211).
- Subnet Mask: Network portion (255.255.240.0).
- Default Gateway: Router address (72.31.80.1).
- Lease Duration: Validity period (1 hour).

Optional Information:

- DHCP Server Address: IP of the DHCP server (e.g., 172.31.80.1)
- Renewal Time (T1): Time to attempt lease renewal (e.g., 30 minutes)
- Rebinding Time (T2): Time to attempt rebind to any DHCP server (e.g., 52 minutes 30 seconds)
- DNS Server: IP address for DNS resolution (e.g., 172.31.0.2)
- Domain Name: Local network domain (e.g., ec2.internal)

Q10)

```
[Sat Aug 10 10:14:49] adwanisahi@ip-172-31-94-211: ~$ sudo tcpdump -nn -v port 53 > tcpdump.out 2>&1 &
[1] 2398
[Sat Aug 10 10:14:59] adwanisahi@ip-172-31-94-211: ~$ curl --silent https://www.wgtn.ac.nz/ > /dev/null
[Sat Aug 10 10:15:08] adwanisahi@ip-172-31-94-211: ~$ sudo killall tcpdump
[Sat Aug 10 10:15:20] adwanisahi@ip-172-31-94-211: ~$ cat tcpdump.out
tcpdump: listening on enX0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
10:15:08.092724 IP (tos 0x0, ttl 64, id 61191, offset 0, flags [none], proto UDP (17), length 71)
    172.31.94.211.54265 > 172.31.0.2.53: 58448+ [1au] A? www.wgtn.ac.nz. (43)
10:15:08.092875 IP (tos 0x0, ttl 64, id 33382, offset 0, flags [none], proto UDP (17), length 71)
    172.31.94.211.45123 > 172.31.0.2.53: 16696+ [1au] AAAA? www.wgtn.ac.nz. (43)
10:15:08.095619 IP (tos 0x0, ttl 255, id 49560, offset 0, flags [none], proto UDP (17), length 155)
    172.31.0.2.53 > 172.31.94.211.45123: 16696 0/1/1 (127)
10:15:08.096281 IP (tos 0x0, ttl 255, id 49561, offset 0, flags [none], proto UDP (17), length 135)
    172.31.0.2.53 > 172.31.94.211.54265: 58448 4/0/1 www.wgtn.ac.nz. A 151.101.2.49, www.wgtn.ac.nz. A 151.101.66.49, www.wgtn.ac.nz. A 151.101.130.49, www.wgtn.a
c.nz. A 151.101.194.49 (107)

4 packets captured
6 packets received by filter
0 packets dropped by kernel
[1]+  Done                    sudo tcpdump -nn -v port 53 > tcpdump.out 2>&1
```

a)

Packet 1: 172.31.94.211 (Client) to 172.31.0.2 (DNS Server). Purpose: DNS query for the A record of www.wgtn.ac.nz.

Packet 2: 172.31.94.211 (Client) to 172.31.0.2 (DNS Server). Purpose: DNS query for the AAAA record of www.wgtn.ac.nz.

Packet 3: 172.31.0.2 (DNS Server) to 172.31.94.211 (Client). Purpose: DNS response to AAAA query with no result (127).

Packet 4:172.31.0.2 (DNS Server) to 172.31.94.211 (Client). Purpose: DNS response to A record query with IP addresses for www.wgtn.ac.nz.

b) Protocol Used: UDP
Reason: UDP is chosen because DNS queries are typically short and require minimal overhead. It provides a fast, connectionless service suitable for small, quick requests and responses, fitting within a single UDP packet without the need for connection establishment. Also, UDP supports multiple application processes on each host using different port numbers.

Q11)

```
[Tue Aug 13 03:16:16] adwanisahi@ip-172-31-94-211: ~$ cat tcpdump.out
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enX0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
03:16:08.912515 IP 172.31.94.211.36636 > 151.101.66.49.443: Flags [S], seq 4125163794, win 62727, options [mss 8961,sackOK,TS val 1184714834 ecr 0,nop,wscale 7], length 0
03:16:08.913631 IP 151.101.66.49.443 > 172.31.94.211.36636: Flags [S.], seq 4060589607, ack 4125163795, win 65535, options [mss 1460,sackOK,TS val 2397600099 ecr 1184714834,nop,wscale 9], length 0
03:16:08.913643 IP 172.31.94.211.36636 > 151.101.66.49.443: Flags [.], ack 4060589608, win 491, options [nop,nop,TS val 1184714836 ecr 2397600099], length 0
03:16:08.915992 IP 172.31.94.211.36636 > 151.101.66.49.443: Flags [P.], seq 4125163795:4125164312, ack 4060589608, win 491, options [nop,nop,TS val 1184714838 ecr 2397600099], length 517
03:16:08.917120 IP 151.101.66.49.443 > 172.31.94.211.36636: Flags [.], ack 4125164312, win 285, options [nop,nop,TS val 2397600103 ecr 1184714838], length 0
03:16:08.918499 IP 151.101.66.49.443 > 172.31.94.211.36636: Flags [P.], seq 4060589608:4060592855, ack 4125164312, win 285, options [nop,nop,TS val 2397600104 ecr 1184714838], length 3247
03:16:08.918508 IP 172.31.94.211.36636 > 151.101.66.49.443: Flags [.], ack 4060592855, win 466, options [nop,nop,TS val 1184714840 ecr 2397600104], length 0
03:16:08.956689 IP 172.31.94.211.36636 > 151.101.66.49.443: Flags [P.], seq 4125164312:4125164397, ack 4060592855, win 466, options [nop,nop,TS val 1184714879 ecr 2397600104], length 85
03:16:08.957794 IP 151.101.66.49.443 > 172.31.94.211.36636: Flags [.], ack 4125164397, win 285, options [nop,nop,TS val 2397600144 ecr 1184714879], length 0
03:16:08.957988 IP 151.101.66.49.443 > 172.31.94.211.36636: Flags [P.], seq 4060592855:4060592898, ack 4125164397, win 285, options [nop,nop,TS val 2397600144 ecr 1184714879], length 43
03:16:08.958162 IP 172.31.94.211.36636 > 151.101.66.49.443: Flags [P.], seq 4125164397:4125164482, ack 4060592898, win 466, options [nop,nop,TS val 1184714880 ecr 2397600144], length 85
03:16:08.958236 IP 172.31.94.211.36636 > 151.101.66.49.443: Flags [P.], seq 4125164482:4125164543, ack 4060592898, win 466, options [nop,nop,TS val 1184714880 ecr 2397600144], length 61
03:16:08.959248 IP 151.101.66.49.443 > 172.31.94.211.36636: Flags [.], ack 4125164482, win 285, options [nop,nop,TS val 2397600145 ecr 1184714880], length 0
03:16:08.959289 IP 151.101.66.49.443 > 172.31.94.211.36636: Flags [P.], seq 4060592898:4060592962, ack 4125164482, win 285, options [nop,nop,TS val 2397600145 ecr 1184714880], length 64
03:16:08.959331 IP 151.101.66.49.443 > 172.31.94.211.36636: Flags [.], ack 4125164543, win 285, options [nop,nop,TS val 2397600145 ecr 1184714880], length 0
03:16:08.959352 IP 172.31.94.211.36636 > 151.101.66.49.443: Flags [P.], seq 4125164543:4125164573, ack 4060592962, win 466, options [nop,nop,TS val 1184714881 ecr 2397600145], length 30
03:16:08.960438 IP 151.101.66.49.443 > 172.31.94.211.36636: Flags [.], ack 4125164573, win 285, options [nop,nop,TS val 2397600146 ecr 1184714881], length 0
03:16:09.181038 IP 151.101.66.49.443 > 172.31.94.211.36636: Flags [P.], seq 4060592962:4060593461, ack 4125164573, win 285, options [nop,nop,TS val 2397600367 ecr 1184714881], length 499
03:16:09.181301 IP 151.101.66.49.443 > 172.31.94.211.36636: Flags [P.], seq 4060593461:4060615121, ack 4125164573, win 285, options [nop,nop,TS val 2397600367 ecr 1184714881], length 21660
03:16:09.181348 IP 172.31.94.211.36636 > 151.101.66.49.443: Flags [.], ack 4060615121, win 293, options [nop,nop,TS val 1184715103 ecr 2397600367], length 0
03:16:09.181796 IP 151.101.66.49.443 > 172.31.94.211.36636: Flags [P.], seq 4060615121:4060635337, ack 4125164573, win 285, options [nop,nop,TS val 2397600367 ecr 1184714881], length 20216
03:16:09.181843 IP 172.31.94.211.36636 > 151.101.66.49.443: Flags [.], ack 4060635337, win 136, options [nop,nop,TS val 1184715104 ecr 2397600367], length 0
03:16:09.184620 IP 151.101.66.49.443 > 172.31.94.211.36636: Flags [P.], seq 4060635337:4060652625, ack 4125164573, win 285, options [nop,nop,TS val 2397600370 ecr 1184715103], length 17288
03:16:09.184665 IP 172.31.94.211.36636 > 151.101.66.49.443: Flags [.], ack 4060652625, win 120, options [nop,nop,TS val 1184715107 ecr 2397600370], length 0
03:16:09.185959 IP 151.101.66.49.443 > 172.31.94.211.36636: Flags [P.], seq 4060652625:4060665661, ack 4125164573, win 285, options [nop,nop,TS val 2397600372 ecr 1184715107], length 13036
03:16:09.185972 IP 172.31.94.211.36636 > 151.101.66.49.443: Flags [.], ack 4060665661, win 137, options [nop,nop,TS val 1184715108 ecr 2397600372], length 0
03:16:09.185989 IP 151.101.66.49.443 > 172.31.94.211.36636: Flags [P.], seq 4060665661:4060667985, ack 4125164573, win 285, options [nop,nop,TS val 2397600372 ecr 1184715107], length 2324
03:16:09.186045 IP 172.31.94.211.36636 > 151.101.66.49.443: Flags [.], ack 4060667985, win 120, options [nop,nop,TS val 1184715108 ecr 2397600372], length 0
03:16:09.187255 IP 151.101.66.49.443 > 172.31.94.211.36636: Flags [P.], seq 4060667985:4060677932, ack 4125164573, win 285, options [nop,nop,TS val 2397600373 ecr 1184715108], length 9947
03:16:09.187267 IP 172.31.94.211.36636 > 151.101.66.49.443: Flags [.], ack 4060677932, win 162, options [nop,nop,TS val 1184715109 ecr 2397600373], length 0
03:16:09.187442 IP 172.31.94.211.36636 > 151.101.66.49.443: Flags [P.], seq 4125164573:4125164596, ack 4060677932, win 220, options [nop,nop,TS val 1184715109 ecr 2397600373], length 23
03:16:09.188334 IP 172.31.94.211.36636 > 151.101.66.49.443: Flags [F.], seq 4125164596, ack 4060677932, win 220, options [nop,nop,TS val 1184715110 ecr 2397600373], length 0
03:16:09.188937 IP 151.101.66.49.443 > 172.31.94.211.36636: Flags [.], ack 4125164596, win 285, options [nop,nop,TS val 2397600375 ecr 1184715109], length 0
03:16:09.189397 IP 151.101.66.49.443 > 172.31.94.211.36636: Flags [.], ack 4125164597, win 285, options [nop,nop,TS val 2397600375 ecr 1184715110], length 0
03:16:09.189442 IP 151.101.66.49.443 > 172.31.94.211.36636: Flags [P.], seq 4060677932:4060677955, ack 4125164597, win 285, options [nop,nop,TS val 2397600375 ecr 1184715110], length 23
03:16:09.189454 IP 172.31.94.211.36636 > 151.101.66.49.443: Flags [R], seq 4125164597, win 0, length 0
```

Packet 1

Source: 172.31.94.211 (Client)
Destination: 151.101.66.49 (Server)
Source Port: 36636
Destination Port: 443
TCP Flags: [S] (SYN)
Purpose: This is the initial SYN packet in a TCP handshake. The source (172.31.94.211) is trying to establish a connection to the destination (151.101.2.49) on port 443.

Packet 2

Source: 151.101.66.49 (Server)
Destination: 172.31.94.211 (Client)
Source Port: 443
Destination Port: 36636
TCP Flags: [S.] (SYN, ACK)
Purpose: This is the SYN-ACK response from the server (151.101.2.49) acknowledging the initial SYN request and agreeing to establish a connection.

Packet 3

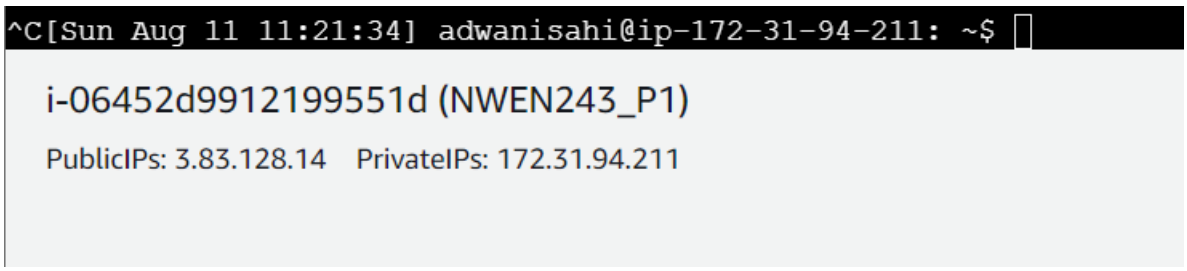
Source: 172.31.94.211 (Client)
Destination: 151.101.66.49 (Server)
Source Port: 36636
Destination Port: 443
TCP Flags: [.] (ACK)
Purpose: This is the final ACK packet from the client (172.31.94.211) completing the TCP handshake process. It acknowledges the receipt of the SYN-ACK from the server, finalizing the establishment of the connection.

Q12)

Packet 1: The client (172.31.94.211) initiates a connection with a SYN packet. The sequence number is 4125163794.
Packet 2: The server (151.101.66.49) responds with a SYN-ACK packet. The acknowledgment number is 4125163795 (client's sequence number + 1), and the server's sequence number is 4060589607.
Packet 3: The client acknowledges the server's SYN-ACK. The acknowledgment number is 4060589608 (server's sequence number + 1).
Packet 4: The client sends data (517 bytes) starting from sequence number 4125163795. The acknowledgment number is 4060589608 (unchanged).
Packet 5: The server acknowledges the client's data. The acknowledgment number is 4125164312 (client's sequence number + 517).
Packet 6: The server sends data (3247 bytes) starting from sequence number 4060589608. The acknowledgment number is 4125164312 (client's sequence number + 517).

Sequence numbers increment by the number of bytes sent, and ACK numbers reflect the next expected byte. This ensures reliable, ordered data transmission in TCP.

Q13)



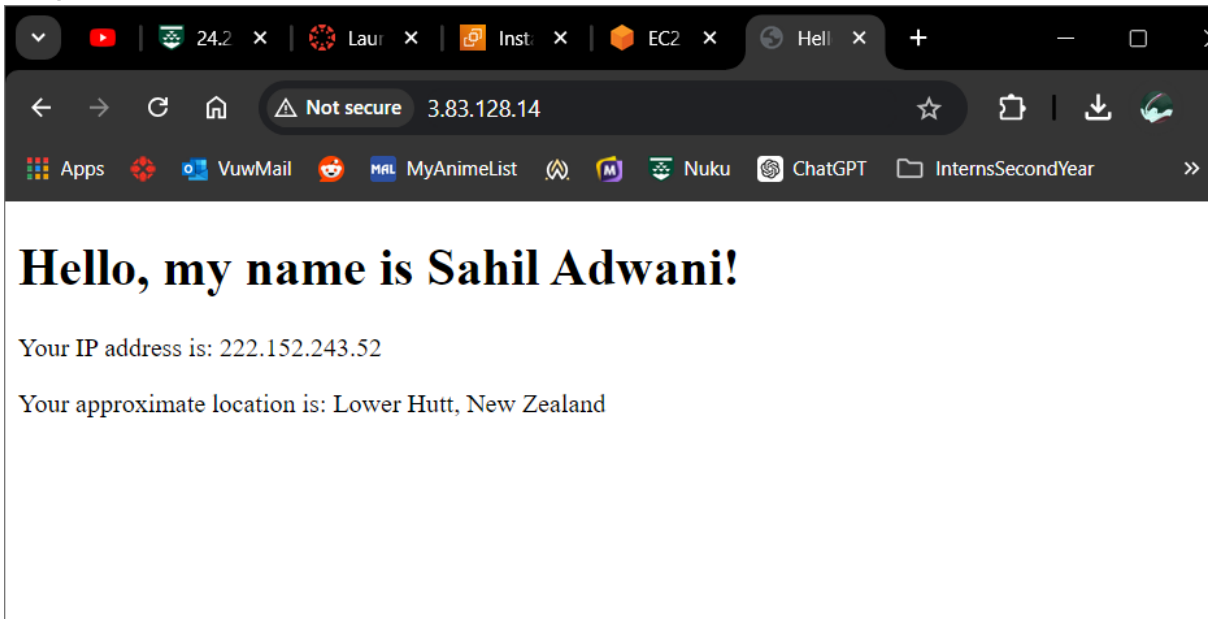
On August 11th , Public IP of VM is 3.83.128.14

Q14)


```java
import java.io.*;
import java.net.*;

public class SimpleWebServer {
    public static void main(String[] args) {
        int port = 8080;
        try {
            ServerSocket serverSocket = new ServerSocket(port);
            System.out.println("Server running at http://localhost:" + port);
            while (true) {
                Socket clientSocket = serverSocket.accept();
                System.out.println("Connection from " + clientSocket.getInetAddress());
                handleRequest(clientSocket);
                clientSocket.close();
            }
        } catch (IOException e) {
            e.printStackTrace();
        }
    }

    private static void handleRequest(Socket clientSocket) throws IOException {
        String clientIP = getHeader(clientSocket, "X-Real-IP");
        if (clientIP == null) {
            clientIP = clientSocket.getInetAddress().getHostAddress();
        }

        OutputStream outputStream = clientSocket.getOutputStream();
        PrintWriter out = new PrintWriter(outputStream, true);
        out.println("HTTP/1.1 200 OK");
        out.println("Content-Type: text/html");
        out.println();
        out.println("<!DOCTYPE html>");
        out.println("<html>");
        out.println("<head>");
        out.println("<title>Hello, my name is Sahil Adwani!</title>");
        out.println("</head>");
        out.println("<body>");
```

```java
        out.println("<h1>Hello, my name is Sahil Adwani!</h1>");
        out.println("<p>Your IP address is: " + clientIP + "</p>");
        out.println("</body>");
        out.println("</html>");

        out.close();
    }

    private static String getHeader(Socket clientSocket, String headerName) throws IOException {
        InputStream inputStream = clientSocket.getInputStream();
        BufferedReader in = new BufferedReader(new InputStreamReader(inputStream));
        String line;
        while ((line = in.readLine()) != null && !line.isEmpty()) {
            System.out.println(line);
            if (line.toLowerCase().startsWith(headerName.toLowerCase() + ":")) {
                return line.substring(headerName.length() + 1).trim();
            }
        }
        return null;
    }
}
```

Q15)




```java
import java.io.*;
import java.net.*;
import javax.net.ssl.HttpsURLConnection;

public class SimpleWebServer {
    public static void main(String[] args) {
        int port = 8080;
        try {
            ServerSocket serverSocket = new ServerSocket(port);
            System.out.println("Server running at http://localhost:" + port);
            while (true) {
                Socket clientSocket = serverSocket.accept();
                System.out.println("Connection from " + clientSocket.getInetAddress());
                handleRequest(clientSocket);
                clientSocket.close();
            }
        } catch (IOException e) {
            e.printStackTrace();
        }
    }

    private static void handleRequest(Socket clientSocket) throws IOException {
        String clientIP = getHeader(clientSocket, "X-Real-IP");
        if (clientIP == null) {
            clientIP = clientSocket.getInetAddress().getHostAddress();
        }

        String location = getLocation(clientIP);

        OutputStream outputStream = clientSocket.getOutputStream();
        PrintWriter out = new PrintWriter(outputStream, true);
        out.println("HTTP/1.1 200 OK");
        out.println("Content-Type: text/html");
        out.println();
        out.println("<!DOCTYPE html>");
        out.println("<html>");
        out.println("<head>");
```

```java
        out.println("<title>Hello, my name is Sahil Adwani!</title>");
        out.println("</head>");
        out.println("<body>");
        out.println("<h1>Hello, my name is Sahil Adwani!</h1>");
        out.println("<p>Your IP address is: " + clientIP + "</p>");
        out.println("<p>Your approximate location is: " + location + "</p>");
        out.println("</body>");
        out.println("</html>");
        out.close();
    }

    private static String getHeader(Socket clientSocket, String headerName) throws IOException {
        InputStream inputStream = clientSocket.getInputStream();
        BufferedReader in = new BufferedReader(new InputStreamReader(inputStream));
        String line;
        while ((line = in.readLine()) != null && !line.isEmpty()) {
            System.out.println(line);
            if (line.startsWith(headerName + ":")) {
                return line.substring(headerName.length() + 1).trim();
            }
        }
        return null;
    }
```

```java
    private static String getLocation(String ipAddress) throws IOException {
        String apiUrl = "http://ip-api.com/json/" + ipAddress;
        URL url = new URL(apiUrl);
        HttpURLConnection conn = (HttpURLConnection) url.openConnection();
        conn.setRequestMethod("GET");

        BufferedReader in = new BufferedReader(new InputStreamReader(conn.getInputStream()));
        StringBuilder response = new StringBuilder();
        String line;
        while ((line = in.readLine()) != null) {
            response.append(line);
        }
        in.close();

        String responseStr = response.toString();
        String city = "Unknown";
        String country = "Unknown";

        int cityIndex = responseStr.indexOf("\"city\":\"");
        if (cityIndex != -1) {
            int start = cityIndex + 8;
            int end = responseStr.indexOf("\"", start);
            if (end != -1) {
                city = responseStr.substring(start, end);
            }
        }

        int countryIndex = responseStr.indexOf("\"country\":\"");
        if (countryIndex != -1) {
            int start = countryIndex + 11;
            int end = responseStr.indexOf("\"", start);
```

```java
            if (end != -1) {
                country = responseStr.substring(start, end);
            }
        }

        return city + ", " + country;
    }
}
```