AHMAD ZAFAR AGAH LAB1 10/8/24

1.2 ARP, Wireshark, Netsim

1.2.1 ARP

```
agah@ada:~$ ip address
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: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 52:54:00:13:a0:c6 brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    inet 131.252.208.103/24 metric 100 brd 131.252.208.255 scope global dynamic ens3
       valid_lft 12671sec preferred_lft 12671sec
agah@ada:~$
```

- What is the default router's IP address (e.g. the gateway address for the default route 0.0.0.0/0)

```
agah@ada:~$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         131.252.208.1   0.0.0.0         UG        0 0          0 ens3
10.218.208.100  131.252.208.1   255.255.255.255 UGH       0 0          0 ens3
10.218.208.108  131.252.208.1   255.255.255.255 UGH       0 0          0 ens3
131.252.110.102 131.252.208.1   255.255.255.255 UGH       0 0          0 ens3
131.252.110.103 131.252.208.1   255.255.255.255 UGH       0 0          0 ens3
131.252.208.0   0.0.0.0         255.255.255.0   U         0 0          0 ens3
131.252.208.1   0.0.0.0         255.255.255.255 UH        0 0          0 ens3
131.252.208.53  0.0.0.0         255.255.255.255 UH        0 0          0 ens3
agah@ada:~$
```

- What is the name of the default router and its hardware address?

```
agah@ada:~$ arp 131.252.208.1
Address    default router       HWtype  HWaddress hardware address  Flags Mask            Iface
router.seas.pdx.edu             ether   00:00:5e:00:01:01   C                     ens3
agah@ada:~$ arp -n 131.252.208.1
Address                  HWtype  HWaddress           Flags Mask            Iface
131.252.208.1            ether   00:00:5e:00:01:01   C                     ens3
agah@ada:~$
```

- How many entries are there in the ARP table?

```
agah@ada:~$ arp -a | wc -l
25
agah@ada:~$
```

1.2.2 ARP2

- List any IP addresses share the same hardware address

None of the IP addresses share the same hardware address (MAC)

```
agah@ada:~$ arp -a | sort -k 4
router.seas.pdx.edu (131.252.208.1) at 00:00:5e:00:01:01 [ether] on ens3
mirrors.cat.pdx.edu (131.252.208.20) at 00:00:5e:00:01:14 [ether] on ens3
cs162lab.cs.pdx.edu (131.252.208.81) at 00:00:5e:00:01:51 [ether] on ens3
cs302lab.cs.pdx.edu (131.252.208.83) at 00:00:5e:00:01:53 [ether] on ens3
cs163lab.cs.pdx.edu (131.252.208.84) at 00:00:5e:00:01:54 [ether] on ens3
gitlab.cecs.pdx.edu (131.252.208.138) at 00:00:5e:00:01:8a [ether] on ens3
jammy.cecs.pdx.edu (131.252.208.11) at 52:54:00:59:3e:39 [ether] on ens3
babbage.cs.pdx.edu (131.252.208.23) at 52:54:00:5c:6f:6e [ether] on ens3
focal.cecs.pdx.edu (131.252.208.94) at 52:54:00:78:73:00 [ether] on ens3
tanto.cs.pdx.edu (131.252.208.5) at 52:54:00:87:21:c4 [ether] on ens3
quizor6.cs.pdx.edu (131.252.208.60) at 52:54:00:a3:46:7f [ether] on ens3
dc-rdns-01.cat.pdx.edu (131.252.208.117) at 52:54:00:a9:30:9f [ether] on ens3
rdns.cat.pdx.edu (131.252.208.53) at 52:54:00:a9:30:9f [ether] on ens3
danimoth.cat.pdx.edu (131.252.208.34) at 52:54:00:b4:6e:05 [ether] on ens3
gitlab-01.cecs.pdx.edu (131.252.208.137) at 52:54:00:c2:05:63 [ether] on ens3
quizor4.cs.pdx.edu (131.252.208.36) at 52:54:00:cf:4c:1b [ether] on ens3
rita.cecs.pdx.edu (131.252.208.28) at 52:54:00:eb:9a:42 [ether] on ens3
ruby.cecs.pdx.edu (131.252.208.85) at 52:54:00:f2:09:bc [ether] on ens3
mircle.cat.pdx.edu (131.252.208.54) at 52:54:00:f6:f8:54 [ether] on ens3
quizor1.cs.pdx.edu (131.252.208.171) at cc:aa:77:07:f2:7a [ether] on ens3
silverfish.cat.pdx.edu (131.252.208.77) at cc:aa:77:0b:76:be [ether] on ens3
destiny.cat.pdx.edu (131.252.208.17) at cc:aa:77:50:b9:5d [ether] on ens3
expn.cat.pdx.edu (131.252.208.110) at cc:aa:77:5f:de:0e [ether] on ens3
stargate.cat.pdx.edu (131.252.208.43) at cc:aa:77:ed:72:3e [ether] on ens3
mirapo.cat.pdx.edu (131.252.208.63) at cc:aa:77:f1:d3:21 [ether] on ens3
agah@ada:~$ arp -a | sort -k 4 | awk '{print $4, $2}' | uniq -D -f 0
agah@ada:~$ arp -a | sort -k 4 | awk '{print $4, $2}' | uniq -D -f 0
agah@ada:~$
```

The output is null, which means no duplicate values in hardware addresses

The result of arp "**-a | wc -l"** and "**arp -a | sort -k 4 | awk '{print $4, $2}' | uniq | wc -l"** is 25, they are equal which means there are equal number of IP addresses and MAC addresses

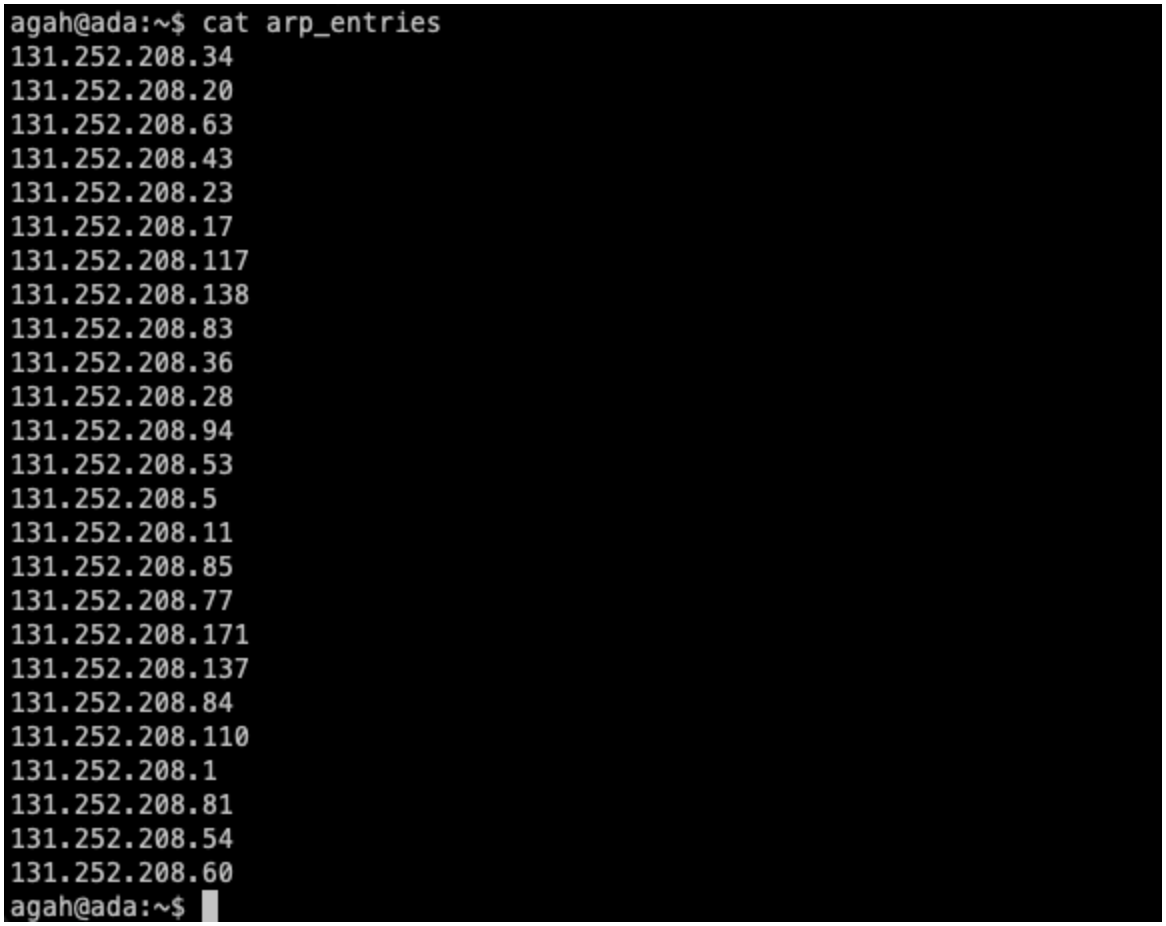
```
agah@ada:~$ arp -a | sort -k 4 | awk '{print $4, $2}' | uniq
00:00:5e:00:01:01 (131.252.208.1)
00:00:5e:00:01:14 (131.252.208.20)
00:00:5e:00:01:51 (131.252.208.81)
00:00:5e:00:01:53 (131.252.208.83)
00:00:5e:00:01:54 (131.252.208.84)
00:00:5e:00:01:8a (131.252.208.138)
52:54:00:59:3e:39 (131.252.208.11)
52:54:00:5c:6f:6e (131.252.208.23)
52:54:00:78:73:00 (131.252.208.94)
52:54:00:87:21:c4 (131.252.208.5)
52:54:00:a3:46:7f (131.252.208.60)
52:54:00:a9:30:9f (131.252.208.117)
52:54:00:a9:30:9f (131.252.208.53)
52:54:00:b4:6e:05 (131.252.208.34)
52:54:00:c2:05:63 (131.252.208.137)
52:54:00:cf:4c:1b (131.252.208.36)
52:54:00:eb:9a:42 (131.252.208.28)
52:54:00:f2:09:bc (131.252.208.85)
52:54:00:f6:f8:54 (131.252.208.54)
cc:aa:77:07:f2:7a (131.252.208.171)
cc:aa:77:0b:76:be (131.252.208.77)
cc:aa:77:50:b9:5d (131.252.208.17)
cc:aa:77:5f:de:0e (131.252.208.110)
cc:aa:77:ed:72:3e (131.252.208.43)
cc:aa:77:f1:d3:21 (131.252.208.63)
agah@ada:~$ arp -a | sort -k 4 | awk '{print $4, $2}' | uniq  | wc -l
25
agah@ada:~$
```

- create a file that contains each IP address that appears in the machine's ARP table and places the results in a file called `arp_entries`

```
arp -an | awk -F '[()]' '{print $2}' > arp_entries
```

- What network prefix do most of the IP addresses in the ARP table share?

In the `arp_entries` output, most of the IP addresses share the network prefix `131.252.208`. This prefix represents the first three octets of each IP address in the list, indicating that these addresses are likely on the same subnet within the `131.252.208.0/24` range.



1.2.3 ARP (Cloud)

- Find the IP address and hardware address of the local ethernet card interface (Typically beginning with `eth`, `ens`, or `enp`).

```
ahmadagah@course-vm:~/Desktop/cloud-agah-agah$ ip address
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
       valid_lft forever preferred_lft forever
2: ens4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 42:01:0a:8a:00:02 brd ff:ff:ff:ff:ff:ff
    inet 10.138.0.2/32 metric 100 scope global dynamic ens4
       valid_lft 82096sec preferred_lft 82096sec
    inet6 fe80::4001:aff:fe8a:2/64 scope link
       valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:b0:f6:25:6f brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
ahmadagah@course-vm:~/Desktop/cloud-agah-agah$
```

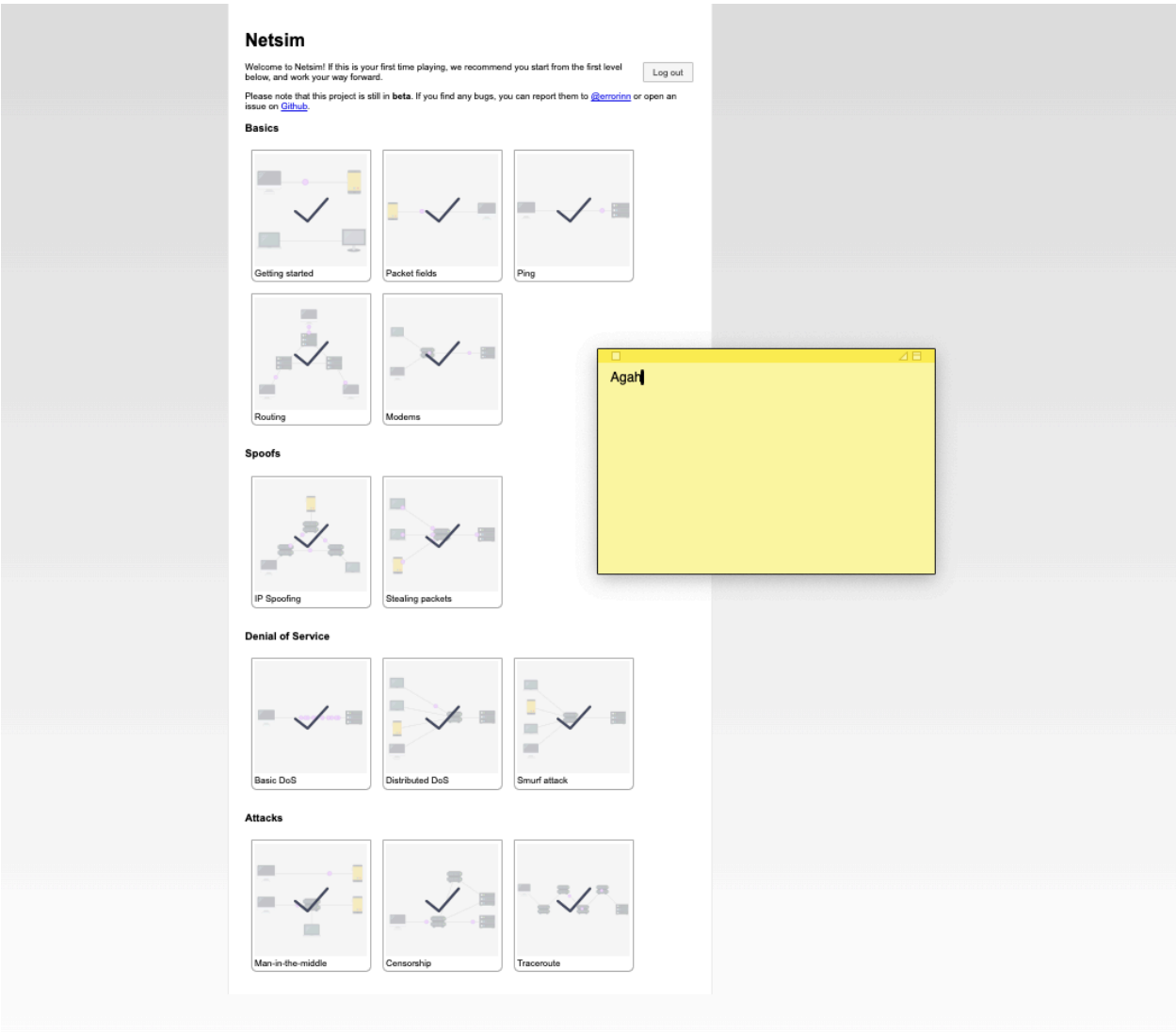
- What is the default router's IP address (e.g. the gateway address for the default route 0.0.0.0/0)

```
ahmadagah@course-vm:~/Desktop/cloud-agah-agah$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         10.138.0.1      0.0.0.0         UG        0 0          0 ens4
10.138.0.1      0.0.0.0         255.255.255.255 UH        0 0          0 ens4
169.254.169.254 10.138.0.1      255.255.255.255 UGH       0 0          0 ens4
172.17.0.0      0.0.0.0         255.255.0.0     U         0 0          0 docker0
ahmadagah@course-vm:~/Desktop/cloud-agah-agah$
```

- What is the default router's hardware address?

```
ahmadagah@course-vm:~/Desktop/cloud-agah-agah$ arp 10.138.0.1
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   42:01:0a:8a:00:01   C                     ens4
```

1.2.4 Netsim



1.3 Cloud Computing

1.3.3 Scan targets for services

- run nmap on the internal subnet the instances have been placed on:

```
ahmadagah@course-vm:~/Desktop/cloud-agah-agah$ sudo nmap 10.138.0.0/20
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-08 06:03 UTC
Nmap scan report for apache-1-vm.c.cloud-agah-agah.internal (10.138.0.3)
Host is up (0.00010s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap scan report for django-1-vm.c.cloud-agah-agah.internal (10.138.0.4)
Host is up (0.000078s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap scan report for secured-wordpress-on-ubuntu-14-04-lts-1-vm.c.cloud-agah-agah.internal (10.138.0.5)
Host is up (0.000092s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap scan report for _gateway (10.138.0.1)
Host is up (0.0011s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 42:01:0A:8A:00:01 (Unknown)

Nmap scan report for course-vm.c.cloud-agah-agah.internal (10.138.0.2)
Host is up (0.0000080s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
3389/tcp open  ms-wbt-server

Nmap done: 4096 IP addresses (5 hosts up) scanned in 45.35 seconds
ahmadagah@course-vm:~/Desktop/cloud-agah-agah$
```

1.3.5 Navigating default networks

- How many subnetworks are created initially on the `default` network? How many regions does this correspond to? (Use a pipe to pass output to `grep` in order to return specific lines of output and then another to pass output to `wc` to count them: `| grep default | wc -l`)

```
→  ~ gcloud compute networks subnets list
NAME     REGION                   NETWORK  RANGE          STACK_TYPE  IPV6_ACCESS_TYPE  INTERNAL_IPV6_PREFIX  EXTERNAL_IPV6_PREFIX
default  us-central1              default  10.128.0.0/20  IPV4_ONLY
default  europe-west1             default  10.132.0.0/20  IPV4_ONLY
default  us-west1                 default  10.138.0.0/20  IPV4_ONLY
default  asia-east1               default  10.140.0.0/20  IPV4_ONLY
default  us-east1                 default  10.142.0.0/20  IPV4_ONLY
default  asia-northeast1          default  10.146.0.0/20  IPV4_ONLY
default  asia-southeast1          default  10.148.0.0/20  IPV4_ONLY
default  us-east4                 default  10.150.0.0/20  IPV4_ONLY
default  australia-southeast1     default  10.152.0.0/20  IPV4_ONLY
default  europe-west2             default  10.154.0.0/20  IPV4_ONLY
default  europe-west3             default  10.156.0.0/20  IPV4_ONLY
default  southamerica-east1       default  10.158.0.0/20  IPV4_ONLY
default  asia-south1              default  10.160.0.0/20  IPV4_ONLY
default  northamerica-northeast1  default  10.162.0.0/20  IPV4_ONLY
default  europe-west4             default  10.164.0.0/20  IPV4_ONLY
default  europe-north1            default  10.166.0.0/20  IPV4_ONLY
default  us-west2                 default  10.168.0.0/20  IPV4_ONLY
default  asia-east2               default  10.170.0.0/20  IPV4_ONLY
default  europe-west6             default  10.172.0.0/20  IPV4_ONLY
default  asia-northeast2          default  10.174.0.0/20  IPV4_ONLY
default  asia-northeast3          default  10.178.0.0/20  IPV4_ONLY
default  us-west3                 default  10.180.0.0/20  IPV4_ONLY
default  us-west4                 default  10.182.0.0/20  IPV4_ONLY
default  asia-southeast2          default  10.184.0.0/20  IPV4_ONLY
default  europe-central2          default  10.186.0.0/20  IPV4_ONLY
default  northamerica-northeast2  default  10.188.0.0/20  IPV4_ONLY
default  asia-south2              default  10.190.0.0/20  IPV4_ONLY
default  australia-southeast2     default  10.192.0.0/20  IPV4_ONLY
default  southamerica-west1       default  10.194.0.0/20  IPV4_ONLY
default  us-east7                 default  10.196.0.0/20  IPV4_ONLY
default  europe-west8             default  10.198.0.0/20  IPV4_ONLY
default  europe-west9             default  10.200.0.0/20  IPV4_ONLY
default  us-east5                 default  10.202.0.0/20  IPV4_ONLY
default  europe-southwest1        default  10.204.0.0/20  IPV4_ONLY
default  us-south1                default  10.206.0.0/20  IPV4_ONLY
default  me-west1                 default  10.208.0.0/20  IPV4_ONLY
default  europe-west12            default  10.210.0.0/20  IPV4_ONLY
default  me-central1              default  10.212.0.0/20  IPV4_ONLY
default  europe-west10            default  10.214.0.0/20  IPV4_ONLY
default  africa-south1            default  10.218.0.0/20  IPV4_ONLY
default  us-west8                 default  10.220.0.0/20  IPV4_ONLY
default  northamerica-south1      default  10.224.0.0/20  IPV4_ONLY
→  ~ gcloud compute networks subnets list | grep default | wc -l
      42
→  ~
```

there are **42 subnetworks** created initially on the **default network**.Each line with `default` represents a different **subnetwork**.
Since each subnetwork is in a specific **region**, the number of subnetworks corresponds directly to the number of regions for the **default network**.

- Given the CIDR prefix associated with each subnetwork, how many hosts does each subnetwork support?

- **Total Bits for IP Addressing**: IPv4 addresses have 32 bits.
- **Network Bits in /20**: The `/20` prefix means the first 20 bits are used for the network.
- **Host Bits**: 32−20=1232 - 20 = 1232−20=12 bits are available for host addresses.
- **Calculating Hosts**:

    - The number of host addresses is calculated by 212−22^{12} - 2212−2.
    - **2** addresses are subtracted because one address is reserved for the network address and one for the broadcast address.
    - Therefore, 2^12−2=4096−2=40942-2 = 4094.

- Create two instances in different zones in separate regions of your choice:
- List both instances.
- Which CIDR subnetworks are these instances brought up in? Do they correspond to the appropriate region based on the prior commands?

```
→  ~ gcloud compute instances list
NAME        ZONE        MACHINE_TYPE   PREEMPTIBLE  INTERNAL_IP  EXTERNAL_IP     STATUS
course-vm   us-west1-b  e2-medium                   10.138.0.2   34.19.41.230    RUNNING
instance-2  us-east1-b  n1-standard-1               10.142.0.2   35.237.127.195  RUNNING
instance-1  us-east4-c  n1-standard-1               10.150.0.2   34.21.32.117    RUNNING
→  ~
```

Instance: `course-vm`

- **Zone**: `us-west1-b`
- **CIDR Subnetwork**: `10.138.0.0/20`
- **Corresponding Region**: `us-west1`
- **Check**: This matches the subnet range `10.138.0.0/20` for the `us-west1` region from the subnetwork list.

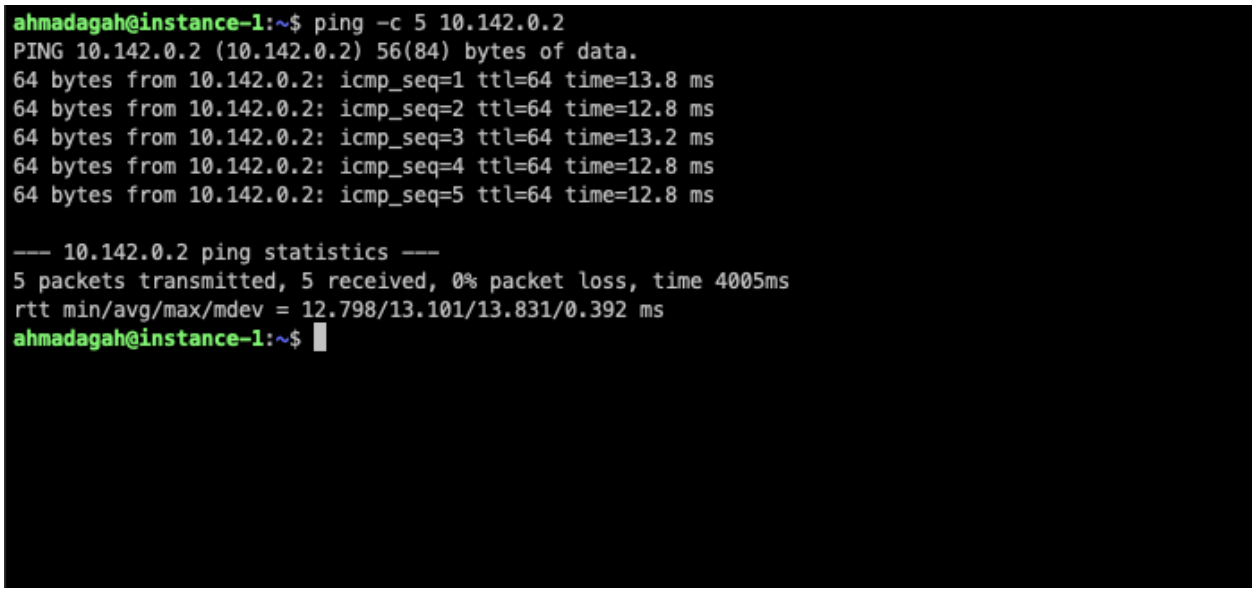
Instance: `instance-2`

- **Zone**: `us-east1-b`
- **CIDR Subnetwork**: `10.142.0.0/20`
- **Corresponding Region**: `us-east1`
- **Check**: This matches the subnet range `10.142.0.0/20` for the `us-east1` region from the subnetwork list.

Instance: `instance-1`

- **Zone**: `us-east4-c`
- **CIDR Subnetwork**: `10.150.0.0/20`
- **Corresponding Region**: `us-east4`
- **Check**: This matches the subnet range `10.150.0.0/20` for the `us-east4` region from the subnetwork list.

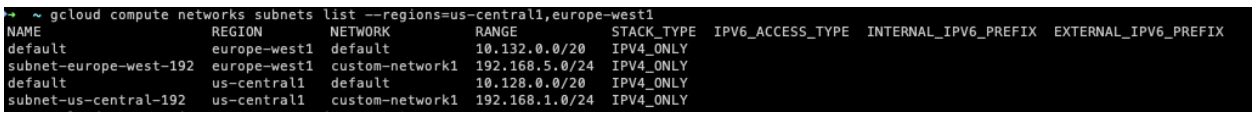
- From instance-1, perform a ping to the Internal IP address of instance-2. Take a screenshot of the output.
- From the figure in the previous step. What facilitates this connectivity: the virtual switch or the VPN Gateway?



The **virtual switch** within the Google Cloud VPC is what facilitates the internal connectivity shown in `ping` command, allowing direct communication between `10.142.0.2` and other instances within the same VPC network.

1.3.6 Creating custom networks

- Take a screenshot of the new subnets created in custom-network1 alongside the default subnetworks in those regions assigned to the default network.



- Explain why the result of this ping is different from when you performed the ping to instance-2.

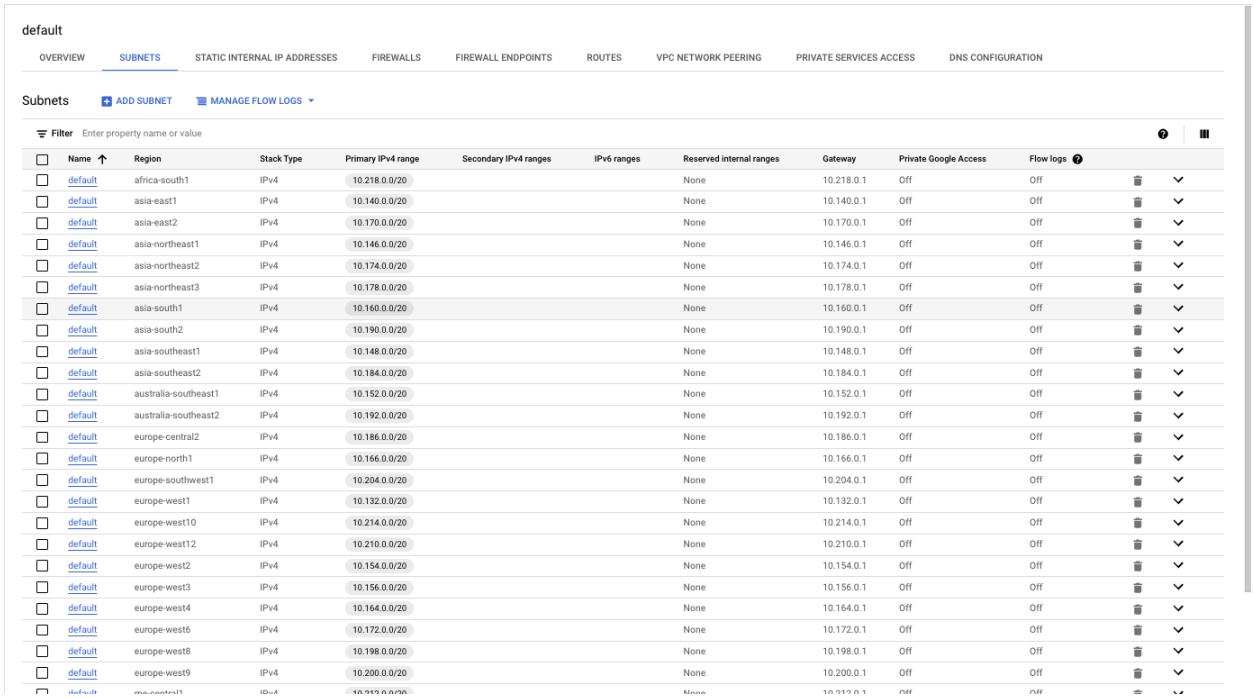
```
ahmadagah@course-vm:~$ ping -c 5 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.

--- 192.168.1.2 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4089ms

ahmadagah@course-vm:~$ ping -c 5 192.168.5.2
PING 192.168.5.2 (192.168.5.2) 56(84) bytes of data.

--- 192.168.5.2 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4100ms
```

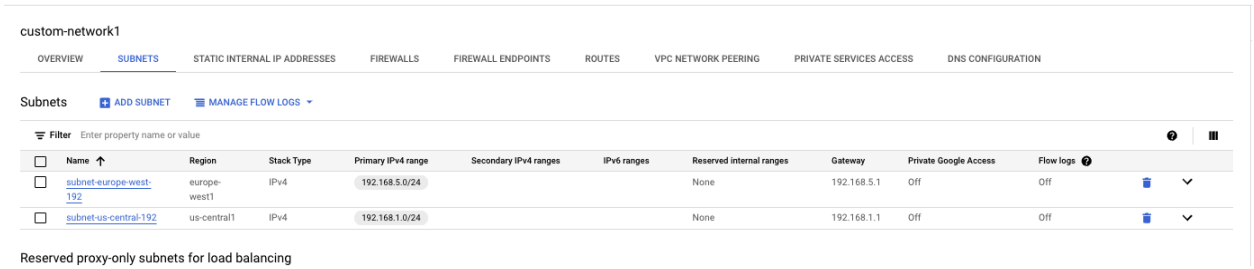
The successful `ping` to **instance-2** (10.142.0.2) occurred within the **10.x.y.z** IP range, which is part of the **default VPC network** in Google Cloud. Instances in the same VPC network, Google Cloud's default or custom subnetworks, can communicate with each other over their internal IP addresses.
The IP addresses **192.168.1.2** and **192.168.5.2** belong to a **different IP range** that is not part of the **default Google Cloud VPC network**. These are in a private IP range commonly used for internal networks, but they are not accessible from the **10.x.y.z** subnet without additional routing or VPN configurations.

- Take screenshots of all 4 instances in the UI including the network they belong to.

Status	Name	Zone	Recommendations	In use by	Internal IP	External IP	Network	Connect
✓	course-vm	us-west1-b			10.138.0.2 (nic0)	34.19.41.230 (nic0)	default	SSH
✓	instance-1	us-east4-c			10.150.0.2 (nic0)	34.21.32.117 (nic0)	default	SSH
✓	instance-2	us-east1-b			10.142.0.2 (nic0)	35.237.127.195 (nic0)	default	SSH
✓	instance-3	us-central1-a			192.168.1.2 (nic0)	34.122.145.160 (nic0)	custom-network1	SSH
✓	instance-4	europe-west1-d			192.168.5.2 (nic0)	34.78.11.54 (nic0)	custom-network1	SSH

- Take a screenshot of the subnetworks created for the custom-network1 network and some of the subnetworks of the default network showing their regions, internal IP ranges and Gateways.





Reserved proxy-only subnets for load balancing