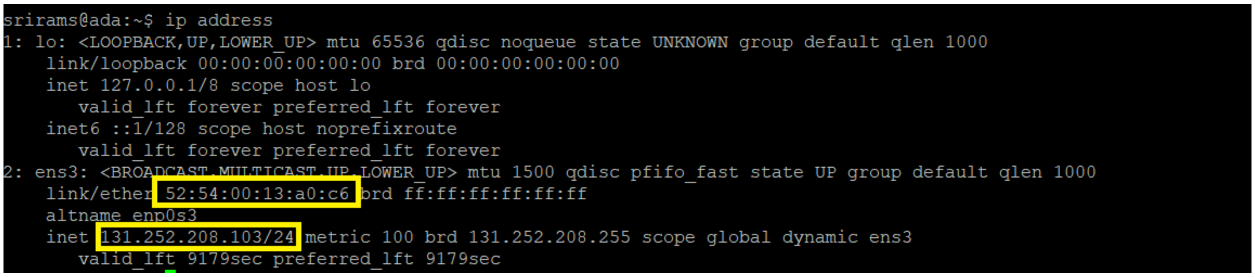
Table of Contents

1.2 ARP, Wireshark, Netsim

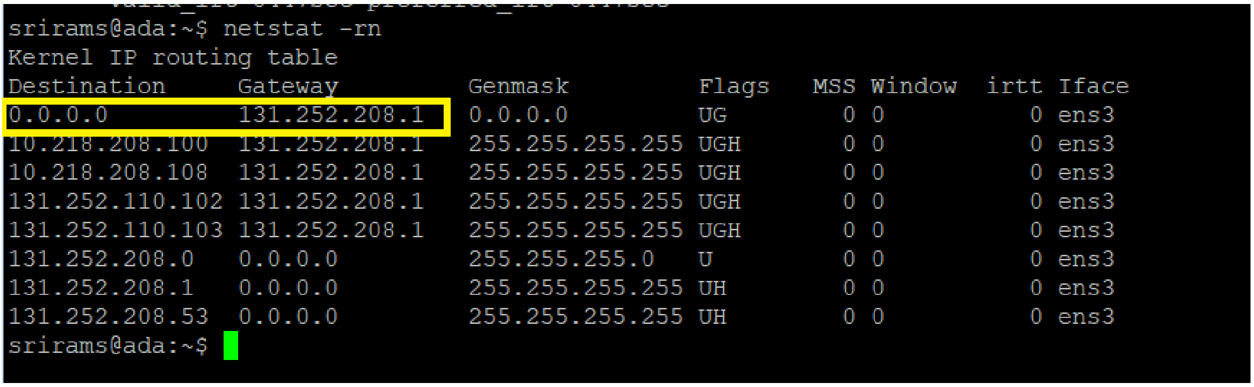
1.2.1 ARP (linux.cs.pdx.edu)

Include both in your lab notebook



```
sriramsc@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 9179sec preferred_lft 9179sec
```

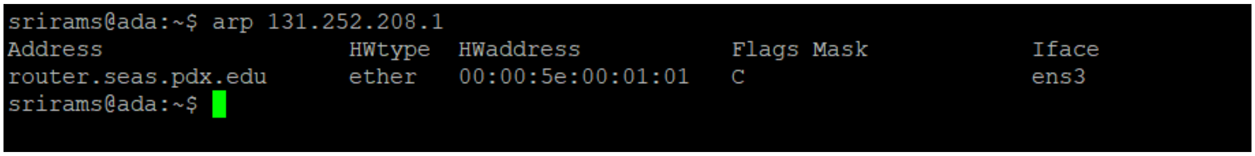
What is the default router's IP address (e.g. the gateway address for the default route 0.0.0.0/0)



```
sriramsc@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
sriramsc@ada:~$
```

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

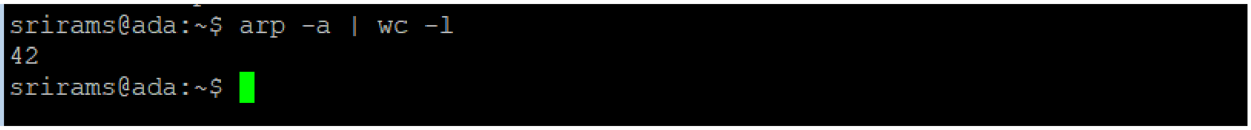
Name: router.seas.pdx.edu **Hardware address:** 00:00:5e:00:01:01



```
sriramsc@ada:~$ arp 131.252.208.1
Address                  HWtype  HWaddress           Flags Mask            Iface
router.seas.pdx.edu      ether   00:00:5e:00:01:01   C                     ens3
sriramsc@ada:~$
```

How many entries are there in the ARP table?

42

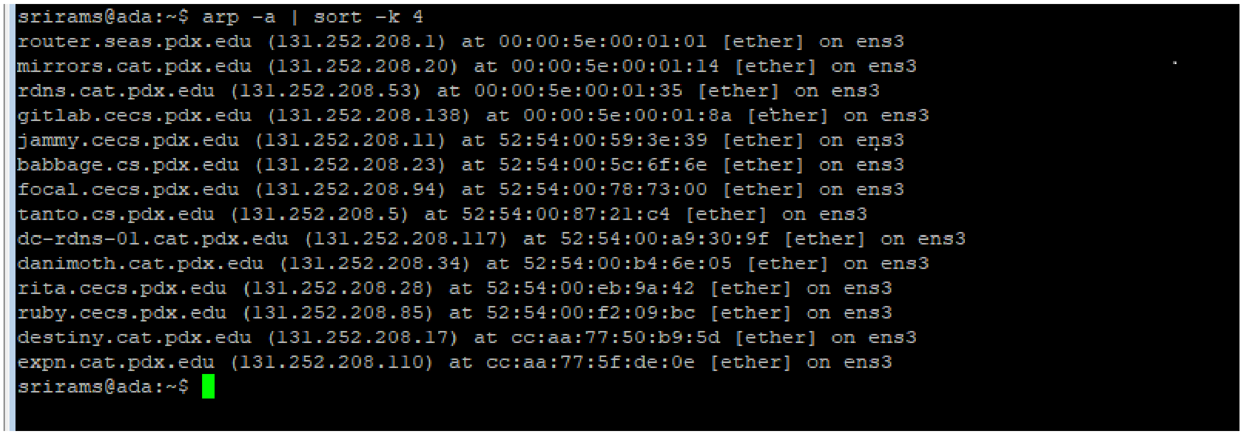


```
sriramsc@ada:~$ arp -a | wc -l
42
sriramsc@ada:~$
```

1.2.2 –

List any IP addresses that share the same hardware address

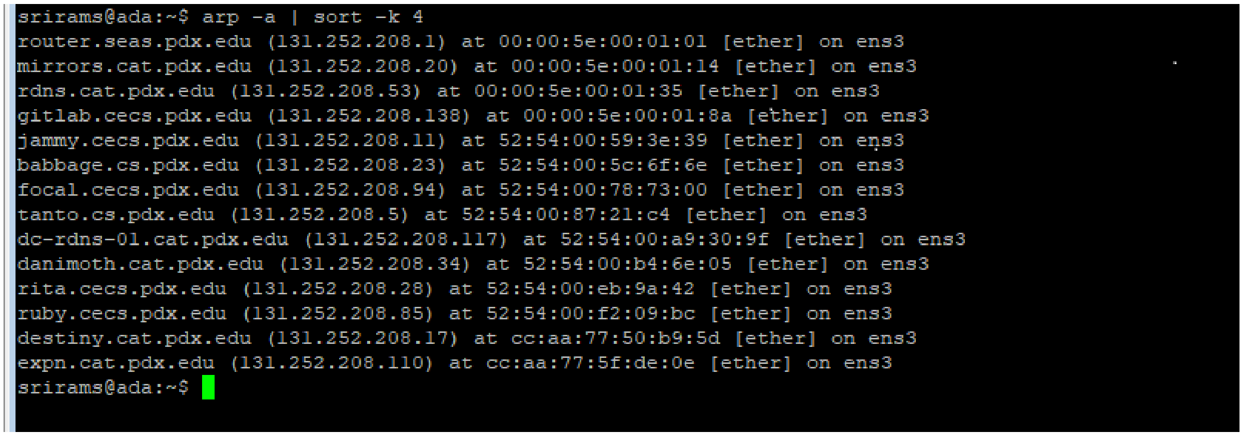
All IP address in our screenshot have their own hardware address.



```
sriramS@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
rdns.cat.pdx.edu (131.252.208.53) at 00:00:5e:00:01:35 [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
dc-rdns-01.cat.pdx.edu (131.252.208.117) 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
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
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
sriramS@ada:~$
```

How many less hardware addresses are there than IP addresses in the ARP table?

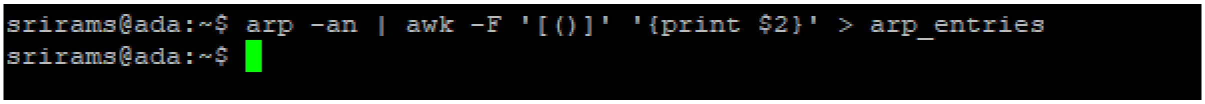
Both are equal number in our screenshot ie. 14 IP addresses mapped to 14 hardware addresses.



```
sriramS@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
rdns.cat.pdx.edu (131.252.208.53) at 00:00:5e:00:01:35 [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
dc-rdns-01.cat.pdx.edu (131.252.208.117) 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
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
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
sriramS@ada:~$
```

Include the command in your lab notebook

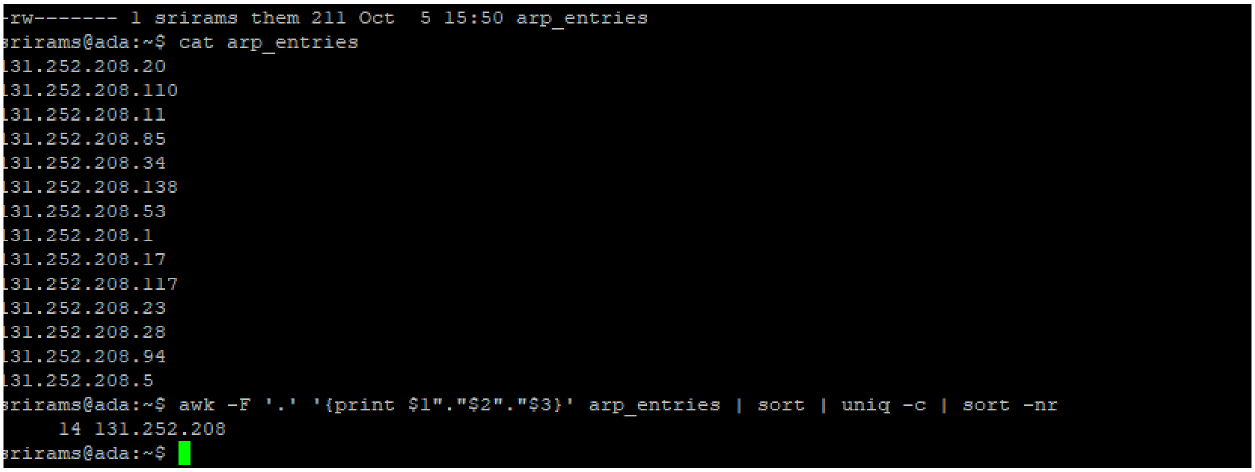
arp -an | awk -F '[()]' '{print $2}' > arp_entries



```
srirams@ada:~$ arp -an | awk -F '[()]' '{print $2}' > arp_entries
srirams@ada:~$ 
```

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

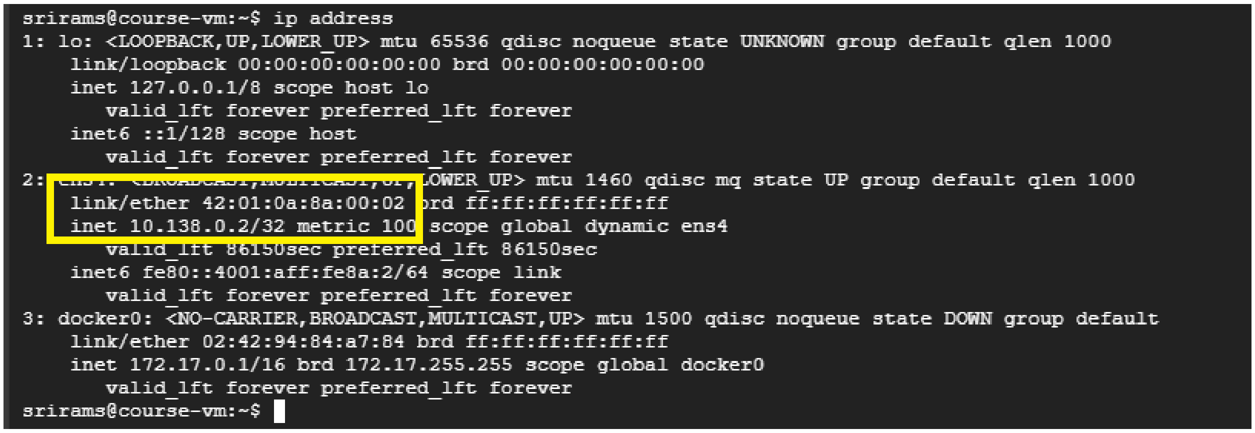
The common network prefix shared by most IP address is 131.252.208



```
-rw------- 1 srirams them 211 Oct  5 15:50 arp_entries
srirams@ada:~$ cat arp_entries
131.252.208.20
131.252.208.110
131.252.208.11
131.252.208.85
131.252.208.34
131.252.208.138
131.252.208.53
131.252.208.1
131.252.208.17
131.252.208.117
131.252.208.23
131.252.208.28
131.252.208.94
131.252.208.5
srirams@ada:~$ awk -F '.' '{print $1"."$2"."$3}' arp_entries | sort | uniq -c | sort -nr
     14 131.252.208
srirams@ada:~$ 
```

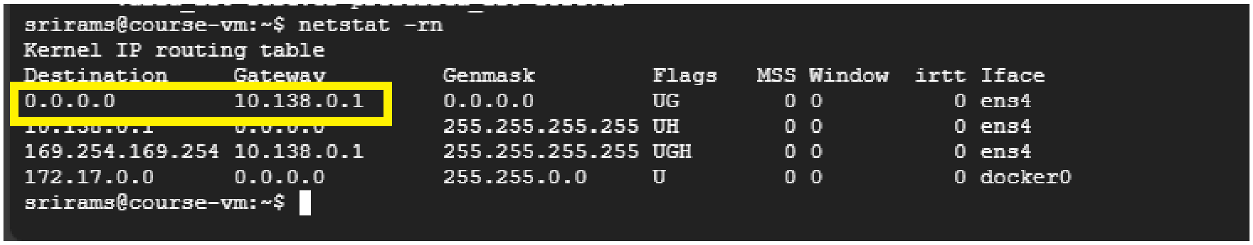
1.2.3 ARP (Cloud)

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



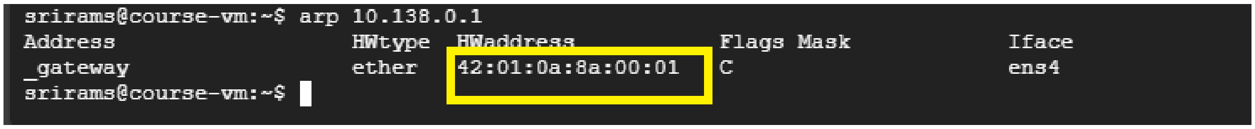
```
srirams@course-vm:~$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1460 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 86150sec preferred_lft 86150sec
    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 02:42:94:84:a7:84 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
srirams@course-vm:~$ █
```

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



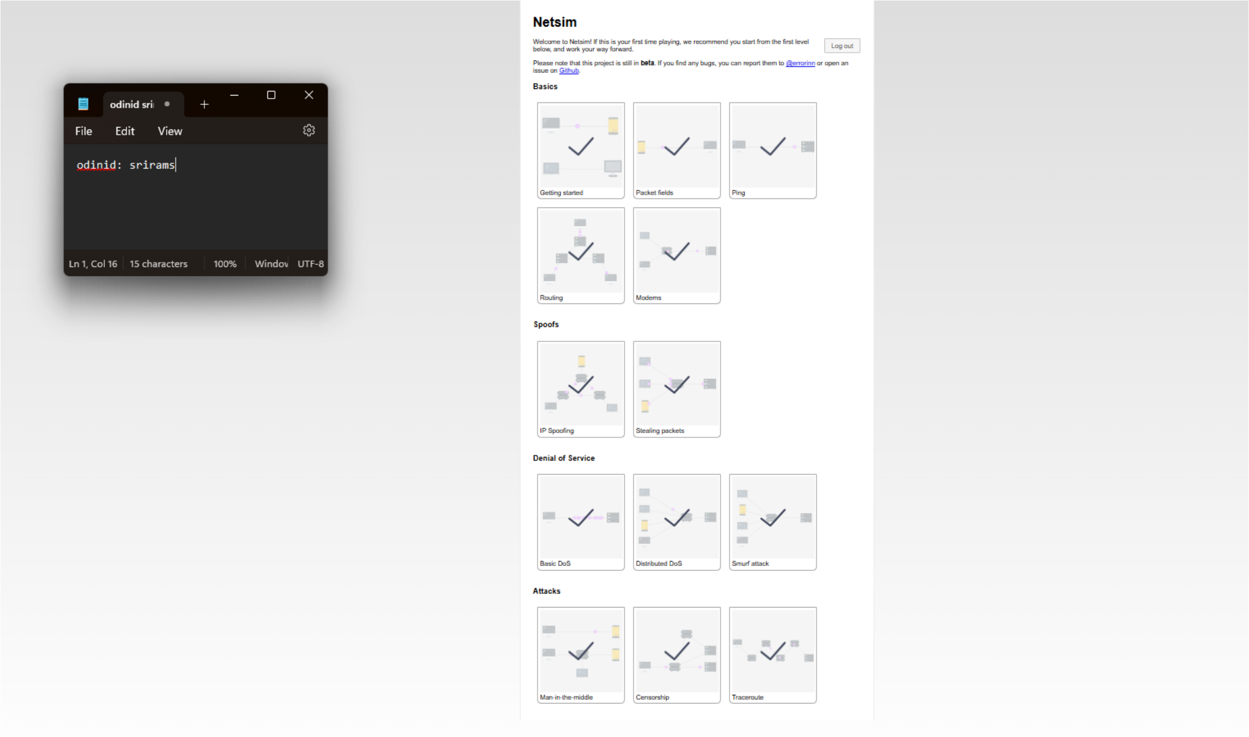
```
       valid_lft forever preferred_lft forever
srirams@course-vm:~$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         10.138.0.1      0.0.0.0         UG        0 0          0 ens4
10.138.0.1      0.0.0.0         255.255.255.255 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
srirams@course-vm:~$ █
```

What is the default router's hardware address?



```
srirams@course-vm:~$ arp 10.138.0.1
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   42:01:0a:8a:00:01   C                     ens4
srirams@course-vm:~$ █
```

1.2.4 Netsim



```
odinid: srirams
```

Netsim

Welcome to Netsim! If this is your first time playing, we recommend you start from the first level below, and work your way forward.

Please note that this project is still in **beta**. If you find any bugs, you can report them to @errorinn or open an issue on Github.

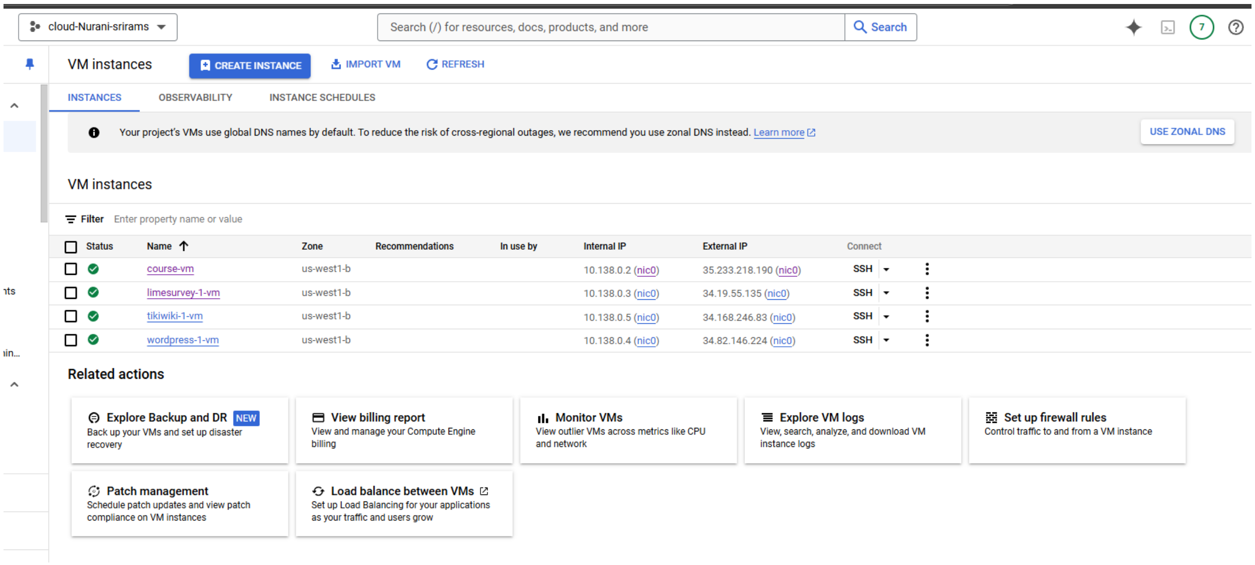
1.3: Cloud networking

1.3.1 Network scanning (nmap) #1

1.3.2 Launch targets

1.3.3 Scan targets for services

Show a screenshot of the output for the scan for your lab notebook.



Your project's VMs use global DNS names by default. To reduce the risk of cross-regional outages, we recommend you use zonal DNS instead. Learn more

VM instances

Status	Name ↑	Zone	Recommendations	In use by	Internal IP	External IP	Connect
✓	course-vm	us-west1-b			10.138.0.2 (nic0)	35.233.218.190 (nic0)	SSH
✓	limesurvey-1-vm	us-west1-b			10.138.0.3 (nic0)	34.19.55.135 (nic0)	SSH
✓	tikiwiki-1-vm	us-west1-b			10.138.0.5 (nic0)	34.168.246.83 (nic0)	SSH
✓	wordpress-1-vm	us-west1-b			10.138.0.4 (nic0)	34.82.146.224 (nic0)	SSH

Related actions

Explore Backup and DR NEW
Back up your VMs and set up disaster recovery

View billing report
View and manage your Compute Engine billing

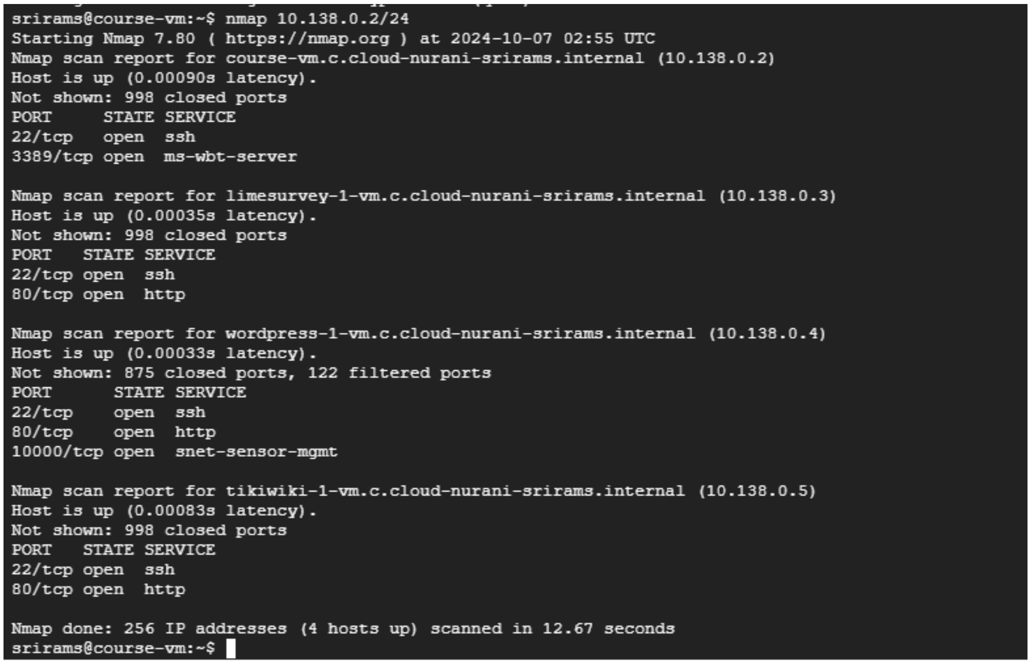
Monitor VMs
View outlier VMs across metrics like CPU and network

Explore VM logs
View, search, analyze, and download VM instance logs

Set up firewall rules
Control traffic to and from a VM instance

Patch management
Schedule patch updates and view patch compliance on VM instances

Load balance between VMs
Set up Load Balancing for your applications as your traffic and users grow

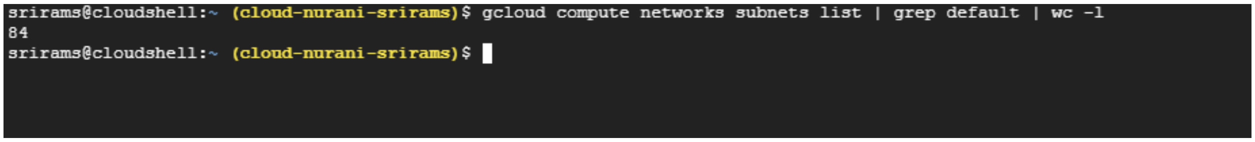


```
sriramss@course-vm:~$ nmap 10.138.0.2/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-07 02:55 UTC
Nmap scan report for course-vm.c.cloud-nurani-sriramss.internal (10.138.0.2)
Host is up (0.00090s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
3389/tcp open  ms-wbt-server

Nmap scan report for limesurvey-1-vm.c.cloud-nurani-sriramss.internal (10.138.0.3)
Host is up (0.00035s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap scan report for wordpress-1-vm.c.cloud-nurani-sriramss.internal (10.138.0.4)
Host is up (0.00033s latency).
Not shown: 875 closed ports, 122 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
10000/tcp open  snet-sensor-mgmt

Nmap scan report for tikiwiki-1-vm.c.cloud-nurani-sriramss.internal (10.138.0.5)
Host is up (0.00083s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 256 IP addresses (4 hosts up) scanned in 12.67 seconds
sriramss@course-vm:~$ █
```

1.3.4 CIDR and subnets #2

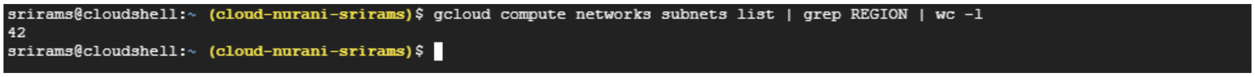
1.3.5 Navigating default networks

How many subnetworks are created initially on the default network? 84



```
srirams@cloudshell:~ (cloud-nurani-srirams)$ gcloud compute networks subnets list | grep default | wc -l
84
srirams@cloudshell:~ (cloud-nurani-srirams)$ 
```

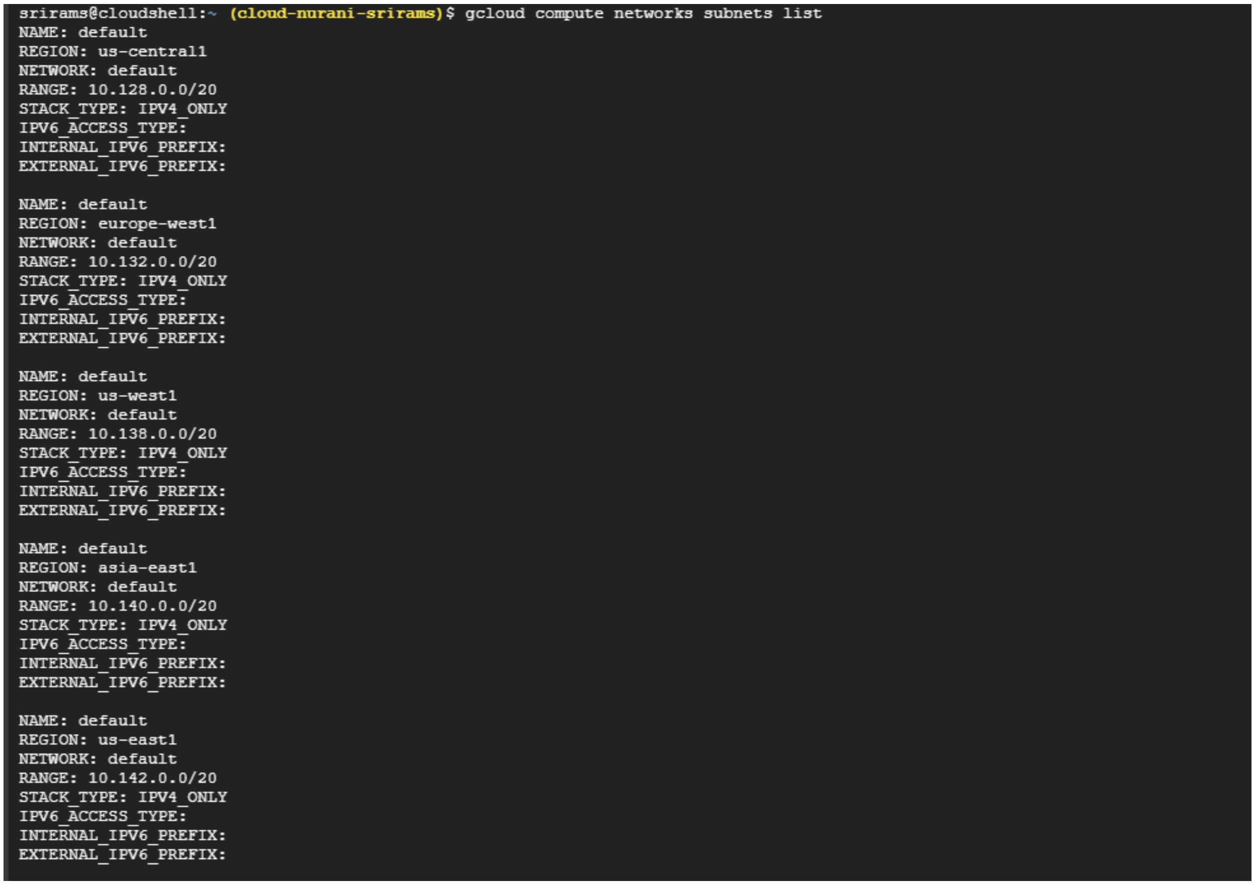
How many regions does this correspond to? 42



```
srirams@cloudshell:~ (cloud-nurani-srirams)$ gcloud compute networks subnets list | grep REGION | wc -l
42
srirams@cloudshell:~ (cloud-nurani-srirams)$ 
```

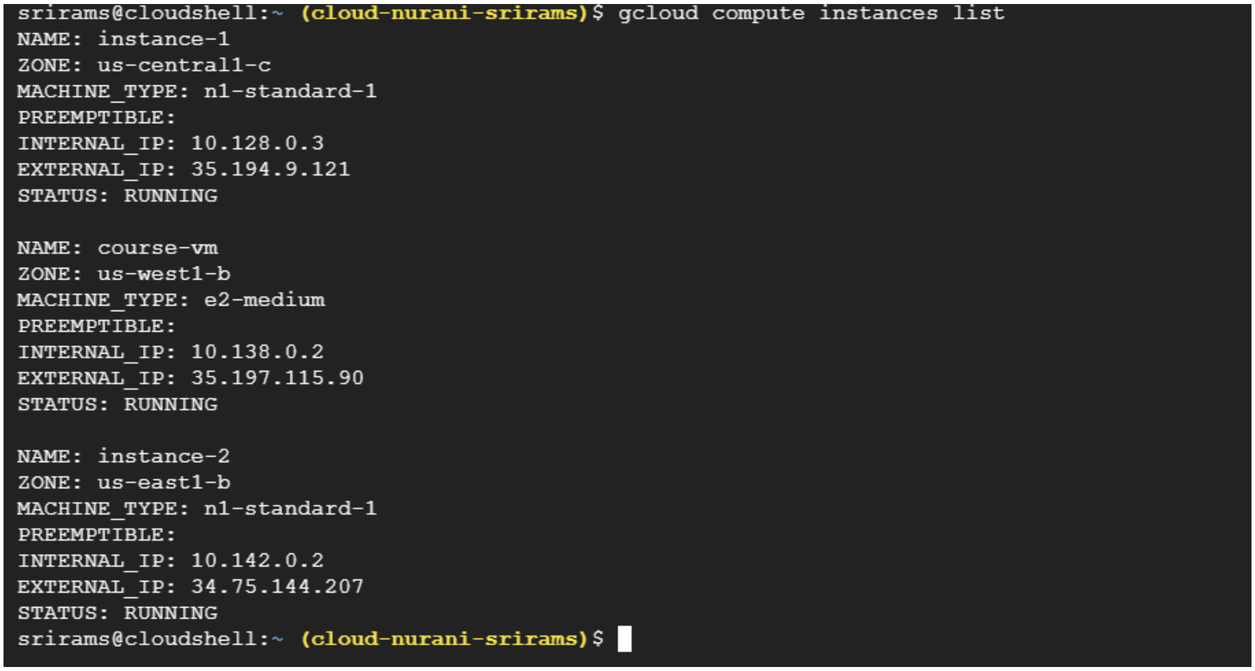
Given the CIDR prefix associated with each subnetwork, how many hosts does each subnetwork support?

CIDR Prefix associated is /20 that means 2 $^{(32-20)}$ -2 hosts i.e. 4094 hosts supported for each subnetwork



```
srirams@cloudshell:~ (cloud-nurani-srirams)$ gcloud compute networks subnets list
NAME: default
REGION: us-central1
NETWORK: default
RANGE: 10.128.0.0/20
STACK_TYPE: IPV4_ONLY
IPV6_ACCESS_TYPE:
INTERNAL_IPV6_PREFIX:
EXTERNAL_IPV6_PREFIX:

NAME: default
REGION: europe-west1
NETWORK: default
RANGE: 10.132.0.0/20
STACK_TYPE: IPV4_ONLY
IPV6_ACCESS_TYPE:
INTERNAL_IPV6_PREFIX:
EXTERNAL_IPV6_PREFIX:

NAME: default
REGION: us-west1
NETWORK: default
RANGE: 10.138.0.0/20
STACK_TYPE: IPV4_ONLY
IPV6_ACCESS_TYPE:
INTERNAL_IPV6_PREFIX:
EXTERNAL_IPV6_PREFIX:

NAME: default
REGION: asia-east1
NETWORK: default
RANGE: 10.140.0.0/20
STACK_TYPE: IPV4_ONLY
IPV6_ACCESS_TYPE:
INTERNAL_IPV6_PREFIX:
EXTERNAL_IPV6_PREFIX:

NAME: default
REGION: us-east1
NETWORK: default
RANGE: 10.142.0.0/20
STACK_TYPE: IPV4_ONLY
IPV6_ACCESS_TYPE:
INTERNAL_IPV6_PREFIX:
EXTERNAL_IPV6_PREFIX:
```

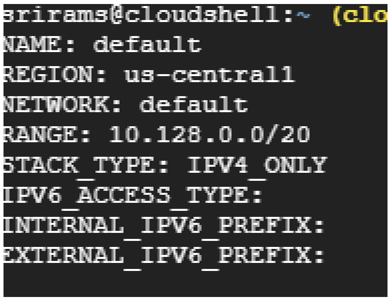
Which CIDR subnetworks are these instances brought up in?



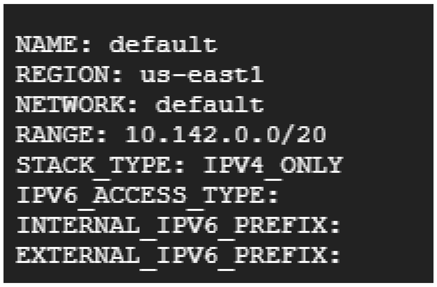
```
srirams@cloudshell:~ (cloud-nurani-srirams)$ gcloud compute instances list
NAME: instance-1
ZONE: us-central1-c
MACHINE_TYPE: n1-standard-1
PREEMPTIBLE:
INTERNAL_IP: 10.128.0.3
EXTERNAL_IP: 35.194.9.121
STATUS: RUNNING

NAME: course-vm
ZONE: us-west1-b
MACHINE_TYPE: e2-medium
PREEMPTIBLE:
INTERNAL_IP: 10.138.0.2
EXTERNAL_IP: 35.197.115.90
STATUS: RUNNING

NAME: instance-2
ZONE: us-east1-b
MACHINE_TYPE: n1-standard-1
PREEMPTIBLE:
INTERNAL_IP: 10.142.0.2
EXTERNAL_IP: 34.75.144.207
STATUS: RUNNING
srirams@cloudshell:~ (cloud-nurani-srirams)$
```

Do they correspond to the appropriate region based on the prior commands?

Yes

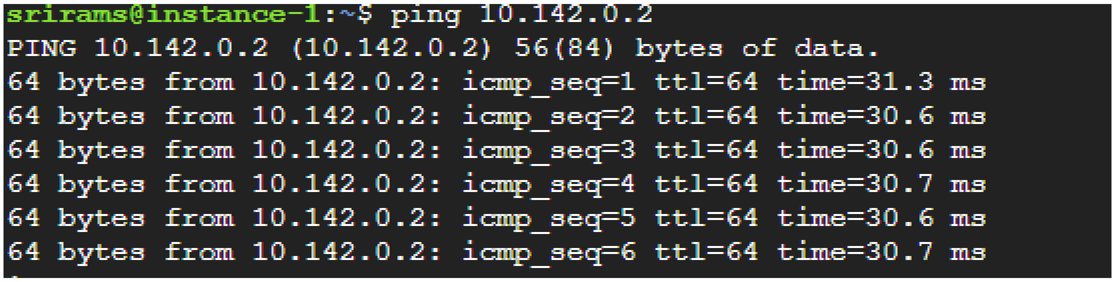


```
srirams@cloudshell:~  (clo
NAME: default
REGION: us-central1
NETWORK: default
RANGE: 10.128.0.0/20
STACK_TYPE: IPV4_ONLY
IPV6_ACCESS_TYPE:
INTERNAL_IPV6_PREFIX:
EXTERNAL_IPV6_PREFIX:
```



```
NAME: default
REGION: us-east1
NETWORK: default
RANGE: 10.142.0.0/20
STACK_TYPE: IPV4_ONLY
IPV6_ACCESS_TYPE:
INTERNAL_IPV6_PREFIX:
EXTERNAL_IPV6_PREFIX:
```

From instance-1, perform a ping to the Internal IP address of instance-2. Take a screenshot of the output.



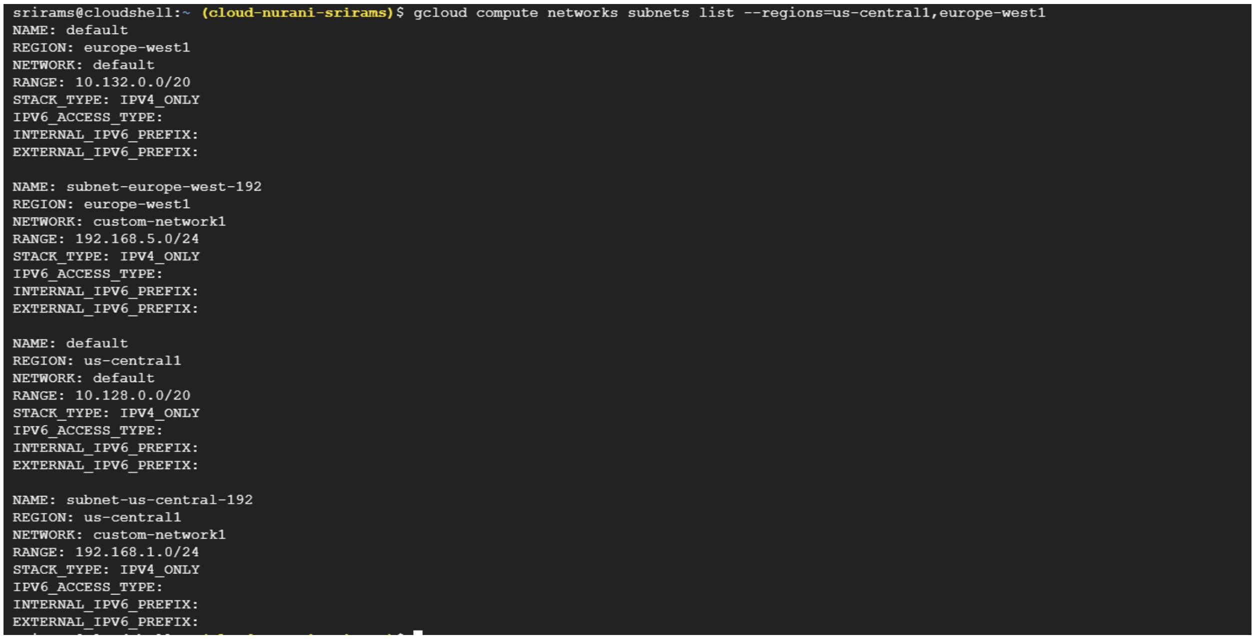
```
sriramS@instance-1:~$ ping 10.142.0.2
PING 10.142.0.2 (10.142.0.2) 56(84) bytes of data.
64 bytes from 10.142.0.2: icmp_seq=1 ttl=64 time=31.3 ms
64 bytes from 10.142.0.2: icmp_seq=2 ttl=64 time=30.6 ms
64 bytes from 10.142.0.2: icmp_seq=3 ttl=64 time=30.6 ms
64 bytes from 10.142.0.2: icmp_seq=4 ttl=64 time=30.7 ms
64 bytes from 10.142.0.2: icmp_seq=5 ttl=64 time=30.6 ms
64 bytes from 10.142.0.2: icmp_seq=6 ttl=64 time=30.7 ms
```

What facilitates this connectivity: the virtual switch or the VPN Gateway?

Virtual Switch

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.

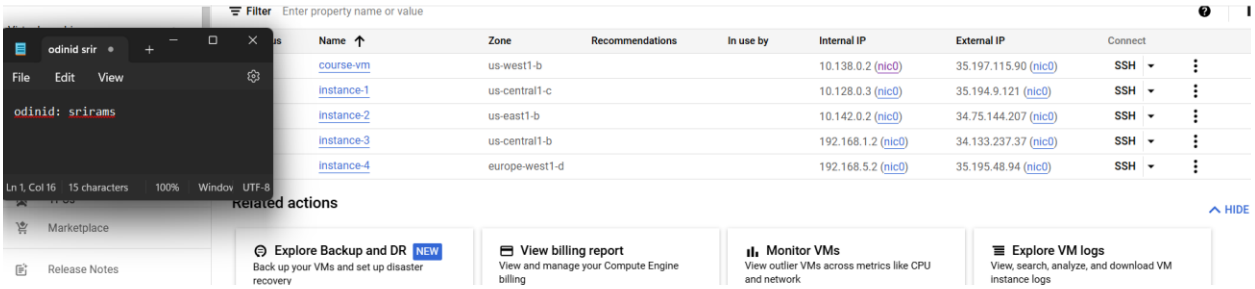


```
srirams@cloudshell:~ (cloud-nurani-srirams)$ gcloud compute networks subnets list --regions=us-central1,europe-west1
NAME: default
REGION: europe-west1
NETWORK: default
RANGE: 10.132.0.0/20
STACK_TYPE: IPV4_ONLY
IPV6_ACCESS_TYPE:
INTERNAL_IPV6_PREFIX:
EXTERNAL_IPV6_PREFIX:

NAME: subnet-europe-west-192
REGION: europe-west1
NETWORK: custom-network1
RANGE: 192.168.5.0/24
STACK_TYPE: IPV4_ONLY
IPV6_ACCESS_TYPE:
INTERNAL_IPV6_PREFIX:
EXTERNAL_IPV6_PREFIX:

NAME: default
REGION: us-central1
NETWORK: default
RANGE: 10.128.0.0/20
STACK_TYPE: IPV4_ONLY
IPV6_ACCESS_TYPE:
INTERNAL_IPV6_PREFIX:
EXTERNAL_IPV6_PREFIX:

NAME: subnet-us-central-192
REGION: us-central1
NETWORK: custom-network1
RANGE: 192.168.1.0/24
STACK_TYPE: IPV4_ONLY
IPV6_ACCESS_TYPE:
INTERNAL_IPV6_PREFIX:
EXTERNAL_IPV6_PREFIX:
```

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

In Previous case, ping occurred in servers where both are in the same network range while in this case instance-3 was on the custom network

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

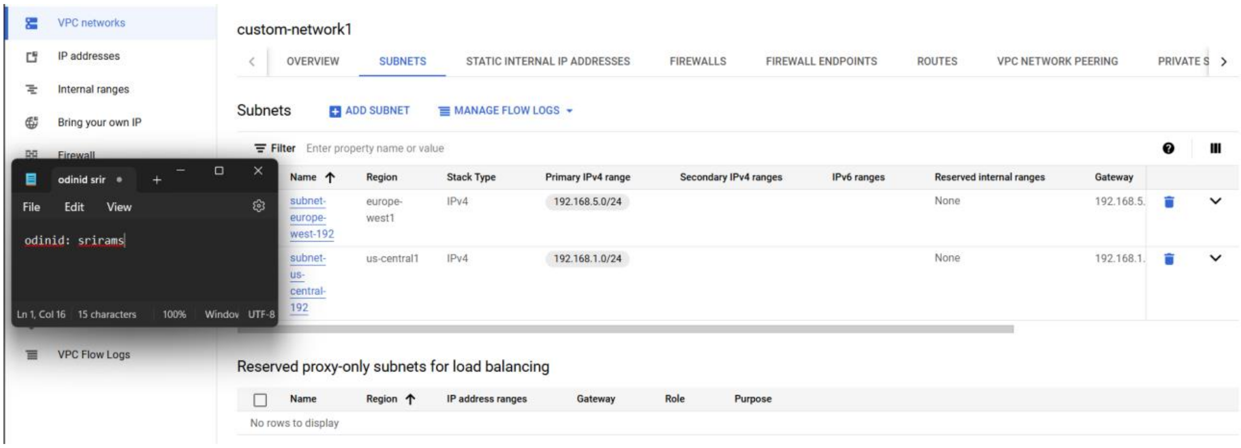


```
odinid: srirams
```

Name	Zone	Recommendations	In use by	Internal IP	External IP	Connect
course-vm	us-west1-b			10.138.0.2 (nic0)	35.197.115.90 (nic0)	SSH
instance-1	us-central1-c			10.128.0.3 (nic0)	35.194.9.121 (nic0)	SSH
instance-2	us-east1-b			10.142.0.2 (nic0)	34.75.144.207 (nic0)	SSH
instance-3	us-central1-b			192.168.1.2 (nic0)	34.133.237.37 (nic0)	SSH
instance-4	europe-west1-d			192.168.5.2 (nic0)	35.195.48.94 (nic0)	SSH

odinid srir
File
Edit
View
Ln 1, Col 16
15 characters
100%
Windov
UTF-8
Filter
Enter property name or value
Related actions
HIDE
Marketplace
Release Notes
Explore Backup and DR
NEW
Back up your VMs and set up disaster recovery
View billing report
View and manage your Compute Engine billing
Monitor VMs
View outlier VMs across metrics like CPU and network
Explore VM logs
View, search, analyze, and download VM instance logs

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.



custom-network1

```
odinid: srirams
```

Name	Region	Stack Type	Primary IPv4 range	Secondary IPv4 ranges	IPv6 ranges	Reserved internal ranges	Gateway
subnet-europe-west-192	europe-west1	IPv4	192.168.5.0/24			None	192.168.5.
subnet-us-central-192	us-central1	IPv4	192.168.1.0/24			None	192.168.1.

Reserved proxy-only subnets for load balancing

Name	Region	IP address ranges	Gateway	Role	Purpose

No rows to display

1.3.7 Clean up