CS 430 Lab 1 - Bradley Chang

1.2: ARP, Wireshark, Netsim

1. ARP

```
brachang@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 fq_codel 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 7472sec preferred_lft 7472sec
brachang@ada:~$
```

```
brachang@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
brachang@ada:~$
```

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

131.252.208.1

```
brachang@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
brachang@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
brachang@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

How many entries are there in the ARP table?

38 Entries

2.-

List any IP addresses that share the same hardware address

```
brachang@ada:~$ arp -a | sort -k 4
router.seas.pdx.edu (131.252.208.1) at 00:00:5e:00:01:01 [ether] on ens3
adns1.cat.pdx.edu (131.252.208.38) at 00:00:5e:00:01:26 [ether] on ens3
vhost-users.cat.pdx.edu (131.252.208.59) at 00:00:5e:00:01:3b [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
cs299lab.cs.pdx.edu (131.252.208.86) at 00:00:5e:00:01:56 [ether] on ens3
vhost-therest.cat.pdx.edu (131.252.208.114) at 00:00:5e:00:01:72 [ether] on ens3
gitlab.cecs.pdx.edu (131.252.208.138) at 00:00:5e:00:01:8a [ether] on ens3
glados.cat.pdx.edu (131.252.208.21) at 3c:08:cd:4a:26:a0 [ether] on ens3
web-users-cherry.cat.pdx.edu (131.252.208.66) at 52:54:00:1a:16:f0 [ether] on ens3
omr-rdns-01.cat.pdx.edu (131.252.208.118) at 52:54:00:30:e3:f2 [ether] on ens3
rdns.cat.pdx.edu (131.252.208.53) at 52:54:00:30:e3:f2 [ether] on ens3
quizor5.cs.pdx.edu (131.252.208.55) at 52:54:00:58:b5:8e [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
mirrors.cat.pdx.edu (131.252.208.20) at 52:54:00:5f:45:5f [ether] on ens3
simirror.cat.pdx.edu (131.252.208.121) at 52:54:00:5f:45:5f [ether] on ens3
host-wireguard-a-02.cat.pdx.edu (131.252.208.135) at 52:54:00:6c:49:67 [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
busdata.cs.pdx.edu (131.252.208.115) at 52:54:00:a6:7a:ce [ether] on ens3
dc-rdns-01.cat.pdx.edu (131.252.208.117) at 52:54:00:a9:30:9f [ether] on ens3
dc-adns-01.cat.pdx.edu (131.252.208.113) at 52:54:00:ac:54:9a [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
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
quizortest.cs.pdx.edu (131.252.208.124) at cc:aa:77:2f:fa:de [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
web-therest-lum.cat.pdx.edu (131.252.208.100) at cc:aa:77:8f:61:cb [ether] on ens3
warpgate.cat.pdx.edu (131.252.208.4) at cc:aa:77:b9:a1:fc [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
brachang@ada:~$
```

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

```
brachang@ada:~$ arp -a | sort -k 4 | awk '{print $4}' | uniq | wc -l
36
brachang@ada:~$
```

There are 2 less hardware addresses

Include the command in your lab notebook

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

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

```
brachang@ada:~/CS430$ cat arp_entries
131.252.208.84
131.252.208.138
131.252.208.28
131.252.208.86
131.252.208.34
131.252.208.1
131.252.208.124
131.252.208.38
131.252.208.5
131.252.208.4
131.252.208.94
131.252.208.43
131.252.208.100
131.252.208.66
131.252.208.11
131.252.208.17
131.252.208.53
131.252.208.55
131.252.208.113
131.252.208.54
131.252.208.21
131.252.208.20
131.252.208.115
131.252.208.23
131.252.208.110
131.252.208.59
131.252.208.114
131.252.208.77
131.252.208.81
131.252.208.117
131.252.208.135
131.252.208.171
131.252.208.83
131.252.208.60
131.252.208.63
131.252.208.118
131.252.208.85
131.252.208.121
brachang@ada:~/CS430$
```

They all have 131.242.208 as the prefix

3. ARP (Cloud)

Include both in your lab notebook

```
brachang@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 86145sec preferred_lft 86145sec
    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:b2:54:2b:a6 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
brachang@course-vm:~$
```

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

```
brachang@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
brachang@course-vm:~$
```

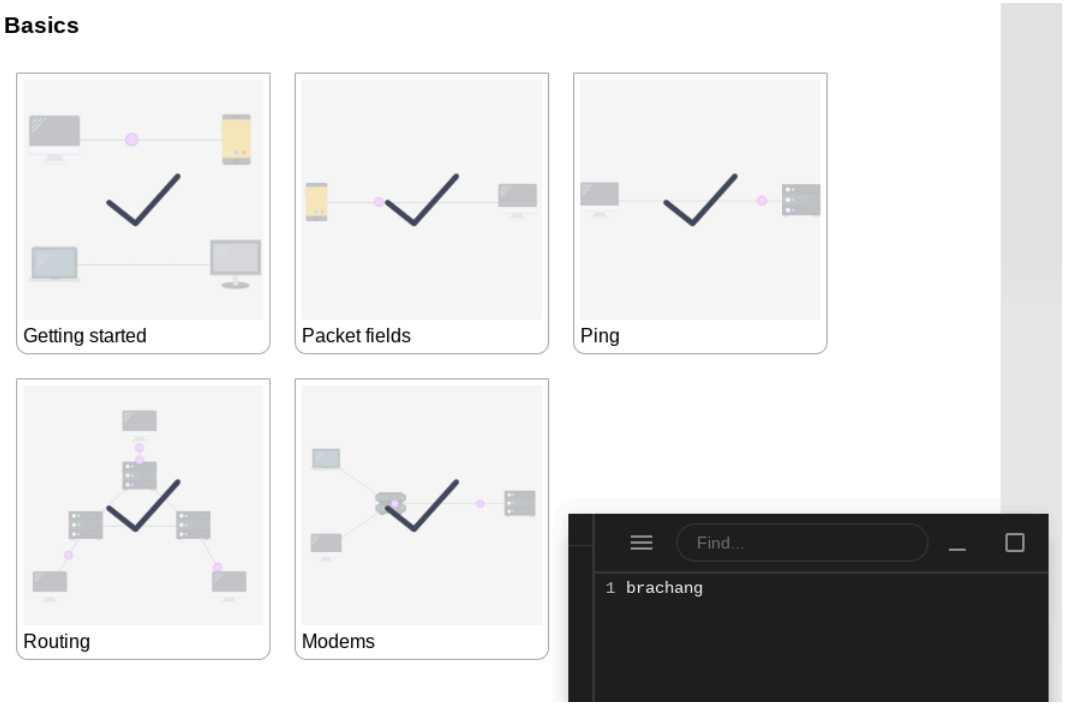
Default router's IP address is 10.138.0.1

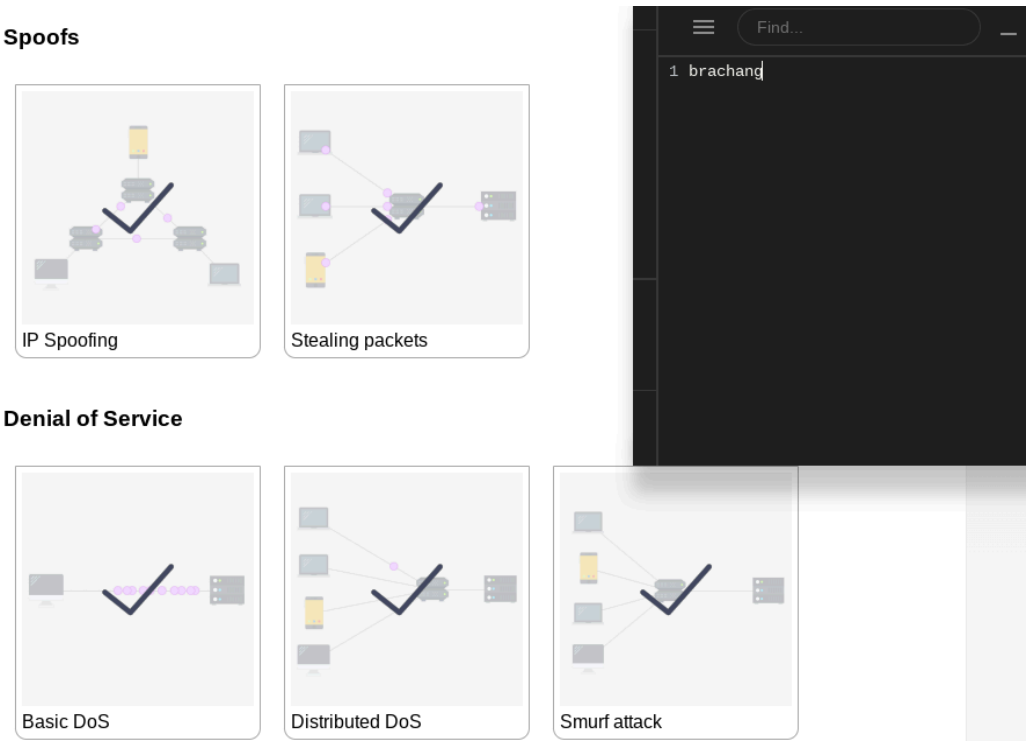
What is the default router's hardware address?

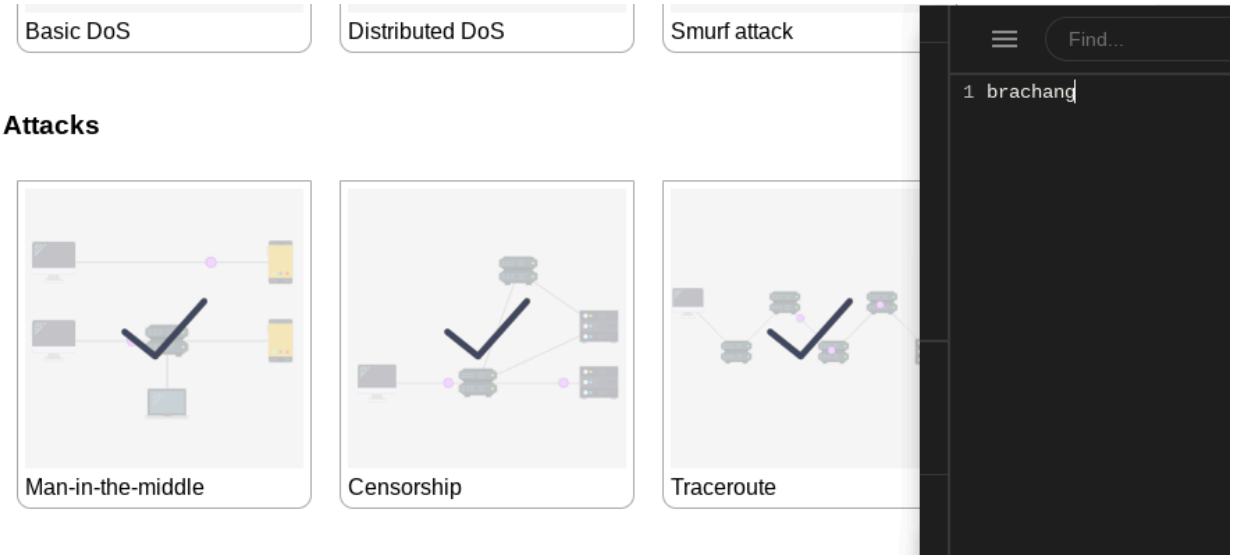
```
brachang@course-vm:~$ arp 10.138.0.1
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   42:01:0a:8a:00:01   C                     ens4
brachang@course-vm:~$
```

Hardware address is 42:01:0a:8a:00:01

4. Netsim


Basics
Getting started
Packet fields
Ping
Routing
Modems
Find...
1 brachang


Spoofs
IP Spoofing
Stealing packets
Find...
1 brachang
Denial of Service
Basic DoS
Distributed DoS
Smurf attack



1.3: Cloud networking

2. Launch Targets

3. Scan targets for services

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

```
brachang@course-vm:~$ nmap 10.138.0.2/24
Starting Nmap 7.80 ( https://nmap.org ) at 2025-01-14 02:05 UTC
Nmap scan report for course-vm.c.cloud-chang-brachang.internal (10.138.0.2)
Host is up (0.00085s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
3389/tcp open  ms-wbt-server

Nmap scan report for rails-1-vm.c.cloud-chang-brachang.internal (10.138.0.3)
Host is up (0.00090s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap scan report for ruby-1-vm.c.cloud-chang-brachang.internal (10.138.0.4)
Host is up (0.00032s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap scan report for apache-1-vm.c.cloud-chang-brachang.internal (10.138.0.5)
Host is up (0.00090s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3306/tcp open  mysql

Nmap done: 256 IP addresses (4 hosts up) scanned in 7.67 seconds
brachang@course-vm:~$
```

5. Navigating default networks

```
brachang@cloudshell:~ (cloud-chang-brachang)$ gcloud compute networks list
NAME: default
SUBNET_MODE: AUTO
BGP_ROUTING_MODE: REGIONAL
IPV4_RANGE:
GATEWAY_IPV4:
brachang@cloudshell:~ (cloud-chang-brachang)$
```

```
brachang@cloudshell:~ (cloud-chang-brachang)$ 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:

NAME: default
REGION: asia-northeast1
```

How many subnetworks are created initially on the default network? How many regions does this correspond to?

```
brachang@cloudshell:~ (cloud-chang-brachang)$ gcloud compute networks subnets list | grep 'NETWORK: default' | wc -l
41
brachang@cloudshell:~ (cloud-chang-brachang)$
```

41 subnetworks which correspond to 41 regions.

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

Each subnet address has the prefix length /20. This gives us $2^{32-20} = 2^{12} = 4096$ addresses

```
brachang@cloudshell:~ (cloud-chang-brachang)$ gcloud compute instances list
NAME: instance-2
ZONE: us-west1-a
MACHINE_TYPE: n1-standard-1
PREEMPTIBLE:
INTERNAL_IP: 10.138.0.6
EXTERNAL_IP: 104.196.243.115
STATUS: RUNNING

NAME: course-vm
ZONE: us-west1-b
MACHINE_TYPE: e2-medium
PREEMPTIBLE:
INTERNAL_IP: 10.138.0.2
EXTERNAL_IP: 34.105.7.174
STATUS: RUNNING

NAME: instance-1
ZONE: us-east1-b
MACHINE_TYPE: n1-standard-1
PREEMPTIBLE:
INTERNAL_IP: 10.142.0.2
EXTERNAL_IP: 35.237.96.240
STATUS: RUNNING
brachang@cloudshell:~ (cloud-chang-brachang)$
```

Which CIDR subnetworks are these instances brought up in? Do they correspond to the appropriate region based on the prior commands?

Instance 1 is in us-east1-b which corresponds to the range depicted in the subnet list

```
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:
```

Instance 2 is in us-west1-a which corresponds to the range depicted in the subnet list

```
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:
```

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

```
brachang@instance-1:~$ ping 10.138.0.6
PING 10.138.0.6 (10.138.0.6) 56(84) bytes of data.
64 bytes from 10.138.0.6: icmp_seq=1 ttl=64 time=64.2 ms
64 bytes from 10.138.0.6: icmp_seq=2 ttl=64 time=64.3 ms
64 bytes from 10.138.0.6: icmp_seq=3 ttl=64 time=64.4 ms
64 bytes from 10.138.0.6: icmp_seq=4 ttl=64 time=64.4 ms
64 bytes from 10.138.0.6: icmp_seq=5 ttl=64 time=64.4 ms
```

From the figure in the previous step. What facilitates this connectivity: the virtual switch or the VPN Gateway?

Virtual switch

6. Creating custom networks

```
brachang@cloudshell:~ (cloud-chang-brachang)$ gcloud compute networks subnets list --network custom-network1
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:

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:
brachang@cloudshell:~ (cloud-chang-brachang)$
```

```
brachang@cloudshell:~ (cloud-chang-brachang)$ 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:
brachang@cloudshell:~ (cloud-chang-brachang)$
```

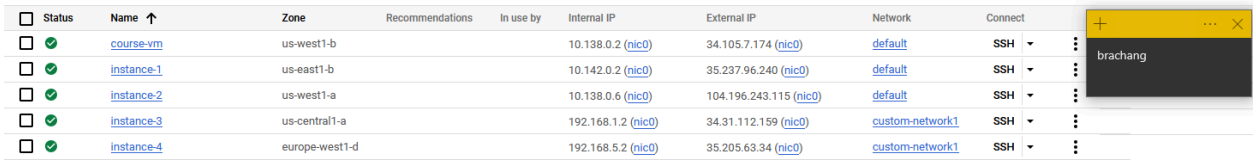
```
brachang@instance-1:~$ ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
^C
--- 192.168.1.2 ping statistics ---
51 packets transmitted, 0 received, 100% packet loss, time 51194ms
```

```
brachang@instance-1:~$ ping 192.168.5.2
PING 192.168.5.2 (192.168.5.2) 56(84) bytes of data.
^C
--- 192.168.5.2 ping statistics ---
19 packets transmitted, 0 received, 100% packet loss, time 18428ms
```

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

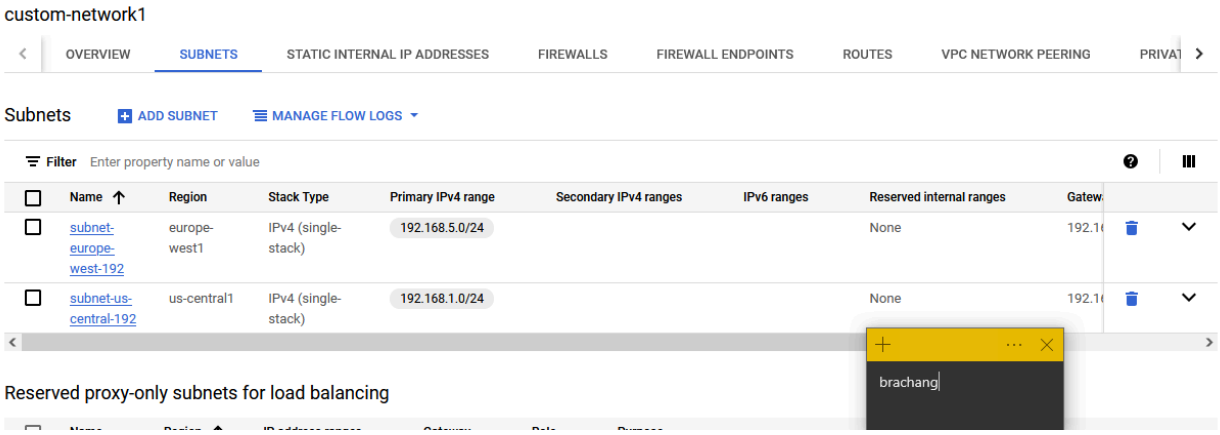
It's different because it doesn't send anything back and we're pinging different regions

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)	34.105.7.174 (nic0)	default	SSH
✓	instance-1	us-east1-b			10.142.0.2 (nic0)	35.237.96.240 (nic0)	default	SSH
✓	instance-2	us-west1-a			10.138.0.6 (nic0)	104.196.243.115 (nic0)	default	SSH
✓	instance-3	us-central1-a			192.168.1.2 (nic0)	34.31.112.159 (nic0)	custom-network1	SSH
✓	instance-4	europe-west1-d			192.168.5.2 (nic0)	35.205.63.34 (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.



default

OVERVIEW | SUBNETS | STATIC INTERNAL IP ADDRESSES | FIREWALLS | FIREWALL ENDPOINTS | ROUTES | VPC NETWORK PEERING | PRI

brachang

Subnets

ADD SUBNET | MANAGE FLOW LOGS

Filter Enter property name or value

Name	Region	Stack Type	Primary IPv4 range	Secondary IPv4 ranges	IPv6 ranges	Reserved internal ranges	G
default	africa-south1	IPv4 (single-stack)	10.218.0.0/20			None	1
default	asia-east1	IPv4 (single-stack)	10.140.0.0/20			None	1
default	asia-east2	IPv4 (single-stack)	10.170.0.0/20			None	1
default	asia-northeast1	IPv4 (single-stack)	10.146.0.0/20			None	1
default	asia-northeast2	IPv4 (single-stack)	10.174.0.0/20			None	1
default	asia-northeast3	IPv4 (single-stack)	10.178.0.0/20			None	1
default	asia-south1	IPv4 (single-stack)	10.160.0.0/20			None	1
default	asia-south2	IPv4 (single-stack)	10.190.0.0/20			None	1
default	asia-southeast1	IPv4 (single-stack)	10.148.0.0/20			None	1
default	asia-southeast2	IPv4 (single-stack)	10.184.0.0/20			None	1
default	australia-southeast1	IPv4 (single-stack)	10.152.0.0/20			None	1