Lab 1.2

1. ARP (linux.cs.pdx.edu)

a. Use the ip address command to find the IPv4 address and hardware address of the local ethernet card interface
IPv4 address: 131.252.208.103
Hardware address: 52:54:00:13:a0:c6

```
nbui@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
       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 brd 131.252.208.255 scope global dynamic ens3
       valid_lft 13761sec preferred_lft 13761sec
nbui@ada:~$
```

b. What is the default router's IP address: 131.252.208.1

```
       valid_lft 13761sec preferred_lft 13761sec
nbui@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
131.252.208.0   0.0.0.0         255.255.255.0   U         0 0          0 ens3
169.254.0.0     0.0.0.0         255.255.0.0     U         0 0          0 ens3
nbui@ada:~$
```

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

   i. Default router: router.seas.pdx.edu

   ii. Its hardware address: 00:00:5e:00:01:01

```
nbui@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
131.252.208.0   0.0.0.0         255.255.255.0   U         0 0          0 ens3
169.254.0.0     0.0.0.0         255.255.0.0     U         0 0          0 ens3
nbui@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
nbui@ada:~$
```

d. How many entries are there in the ARP table?

```
nbui@ada:~$ arp -a | wc -l
26
nbui@ada:~$
```

2. -

List any IP addresses share the same hardware address:

131.252.208.117 and 131.252.208.53

```
nbui@ada:~$ arp -a | sort -k 4,4 | awk '{print $4}' | uniq -d
52:54:00:a9:30:9f
nbui@ada:~$ arp -a | sort -k 4,4
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
cs302lab.cs.pdx.edu (131.252.208.83) at 00:00:5e:00:01:53 [ether] on ens3
glados.cat.pdx.edu (131.252.208.21) at 3c:08:cd:4a:26:a0 [ether] on ens3
linuxlab.cs.pdx.edu (131.252.208.125) at 52:54:00:25:06:08 [ether] on ens3
omr-rdns-01.cat.pdx.edu (131.252.208.118) 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
simirror.cat.pdx.edu (131.252.208.121) at 52:54:00:5f:45:5f [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
rdns.cat.pdx.edu (131.252.208.53) at 52:54:00:a9:30:9f [ether] on ens3
gitlab.cecs.pdx.edu (131.252.208.138) at 52:54:00:c2:05:63 [ether] on ens3
cs163lab.cs.pdx.edu (131.252.208.84) 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
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
? (169.254.169.254) at e0:89:9d:a8:0a:dd [ether] on ens3
shodan.seas.pdx.edu (131.252.208.3) at f4:cc:55:0c:71:00 [ether] on ens3
nbui@ada:~$
```

How many less hardware addresses are there than IP addresses in the ARP table? 1

```
shodan.seas.pdx.edu (131.252.208.3) at f4:cc:55:0c:71:00 [ether] on
nbui@ada:~$ arp -a | sort -k 4.4 | awk '{print $4}' | uniq | wc -l
25
nbui@ada:~$ arp -a | wc -l
26
nbui@ada:~$
```

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? 131.252.208

```
nbui@ada:~$ cat arp_entries
131.252.208.138
131.252.208.77
131.252.208.21
131.252.208.11
131.252.208.63
131.252.208.121
131.252.208.3
131.252.208.55
131.252.208.85
131.252.208.28
131.252.208.94
131.252.208.53
131.252.208.1
131.252.208.20
131.252.208.43
131.252.208.110
131.252.208.125
131.252.208.54
131.252.208.83
131.252.208.17
131.252.208.117
131.252.208.84
169.254.169.254
131.252.208.23
131.252.208.118
131.252.208.5
```

3. ARP (Cloud)

Include both in your lab notebook

IPv4 address: 10.138.0.2
Hardware address: 42:01:0a:8a:00:02

```
No VM guests are running outdated hypervisor (qemu) binaries on this host.
nbui@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 80911sec preferred_lft 80911sec
    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 02:42:81:9a:21:ff 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
```

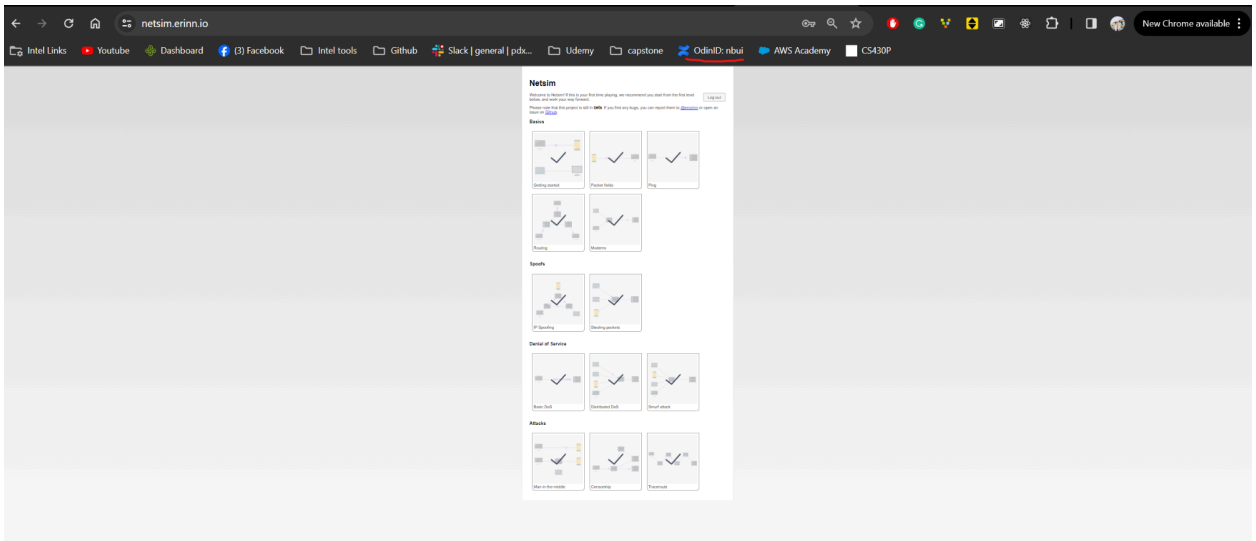
- What is the default router's IP address (e.g. the gateway address for the default route 0.0.0.0/0)

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

- What is the default router's hardware address?

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

4. NetSims


netsim.erinn.io
New Chrome available
Intel Links
Youtube
Dashboard
(3) Facebook
Intel tools
Github
Slack | general | pdx...
Udemy
capstone
OdinID: nbui
AWS Academy
CS430P
Netsim
Log out
Basics
Getting started
Packet fields
Ping
Routing
Mysteries
Spoofs
IP Spoofing
Stealing packets
Denial of Service
Basic DoS
Distributed DoS
Smurf attack
Attacks
Man in the middle
Censorship
Traceroute

Lab 01.3

3. Scan targets for services

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

ssh.cloud.google.com/v2/ssh/projects/cloud-bui-nbui/zones/us-west1-b/instances/course-vm?authuser=0&hl=en_US&projectNumber=476698362318&useAdmin

ssh.cloud.google.com/v2/ssh/projects/cloud-bui-nbui/zones/us-west1-b/instances/course-vm?authuser=0&hl=en_US&projectNumber=4

SSH-in-browser

```
nbui@course-vm:~$ nmap 10.138.0.4/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-01-10 09:30 UTC
Nmap scan report for course-vm.c.cloud-bui-nbui.internal (10.138.0.2)
Host is up (0.00077s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
3389/tcp open  ms-wbt-server

Nmap scan report for wordpress-1-vm.c.cloud-bui-nbui.internal (10.138.0.3)
Host is up (0.00031s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap scan report for rails-with-openlitespeed-1-vm.c.cloud-bui-nbui.internal (10.138.0.4)
Host is up (0.00086s 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 typo3-1-vm.c.cloud-bui-nbui.internal (10.138.0.5)
Host is up (0.00080s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap done: 256 IP addresses (4 hosts up) scanned in 7.26 seconds
nbui@course-vm:~$
```

5. Navigating default networks

- How many subnetworks are created initially on the `default` network? 42
- 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`): 42

```
nbui@cloudshell:~ (cloud-bui-nbui)$ gcloud compute networks subnets list | grep 'NETWORK: default' | wc -l
42
nbui@cloudshell:~ (cloud-bui-nbui)$ gcloud compute networks subnets list | grep REGION | wc -l
42
nbui@cloudshell:~ (cloud-bui-nbui)$
```

- Given the CIDR prefix associated with each subnetwork, how many hosts does each subnetwork support?
    - The range is: 10.220.0.0/20 => prefixed 20 => 12 bits available for host addresses => 2^12 = 4096
- Which CIDR subnetworks are these instances brought up in? Us-west3-a and us-west4-a (showed in bellowed screenshot)
- Do they correspond to the appropriate region based on the prior commands? Yes

```
nbui@cloudshell:~ (cloud-bui-nbui)$ gcloud compute instances create instance-1 --zone=us-west4-a
Created [https://www.googleapis.com/compute/v1/projects/cloud-bui-nbui/zones/us-west4-a/instances/instance-1].
NAME: instance-1
ZONE: us-west4-a
MACHINE_TYPE: n1-standard-1
PREEMPTIBLE:
INTERNAL_IP: 10.182.0.2
EXTERNAL_IP: 34.125.163.52
STATUS: RUNNING
nbui@cloudshell:~ (cloud-bui-nbui)$ gcloud compute instances create instance-1 --zone=us-west3-a
ERROR: (gcloud.compute.instances.create) Could not fetch resource:
 - The resource 'projects/cloud-bui-nbui/zones/us-west4-a/instances/instance-1' already exists

nbui@cloudshell:~ (cloud-bui-nbui)$ gcloud compute instances create instance-2 --zone=us-west3-a
Created [https://www.googleapis.com/compute/v1/projects/cloud-bui-nbui/zones/us-west3-a/instances/instance-2].
NAME: instance-2
ZONE: us-west3-a
MACHINE_TYPE: n1-standard-1
PREEMPTIBLE:
INTERNAL_IP: 10.180.0.2
EXTERNAL_IP: 34.106.94.99
STATUS: RUNNING
nbui@cloudshell:~ (cloud-bui-nbui)$
```

```
nbui@cloudshell:~ (cloud-bui-nbui)$ gcloud compute instances list
NAME: course-vm
ZONE: us-west1-b
MACHINE_TYPE: e2-medium
PREEMPTIBLE:
INTERNAL_IP: 10.138.0.2
EXTERNAL_IP: 34.82.221.201
STATUS: RUNNING

NAME: instance-2
ZONE: us-west3-a
MACHINE_TYPE: n1-standard-1
PREEMPTIBLE:
INTERNAL_IP: 10.180.0.2
EXTERNAL_IP: 34.106.94.99
STATUS: RUNNING

NAME: instance-1
ZONE: us-west4-a
MACHINE_TYPE: n1-standard-1
PREEMPTIBLE:
INTERNAL_IP: 10.182.0.2
EXTERNAL_IP: 34.125.163.52
STATUS: RUNNING
nbui@cloudshell:~ (cloud-bui-nbui)$
```

- From the figure in the previous step. What facilitates this connectivity: the virtual switch or the VPN Gateway? Virtual switch since it's handling internal connections

```
nbui@instance-1:~$ ping 10.180.0.2
PING 10.180.0.2 (10.180.0.2) 56(84) bytes of data.
64 bytes from 10.180.0.2: icmp_seq=1 ttl=64 time=9.29 ms
64 bytes from 10.180.0.2: icmp_seq=2 ttl=64 time=8.73 ms
```

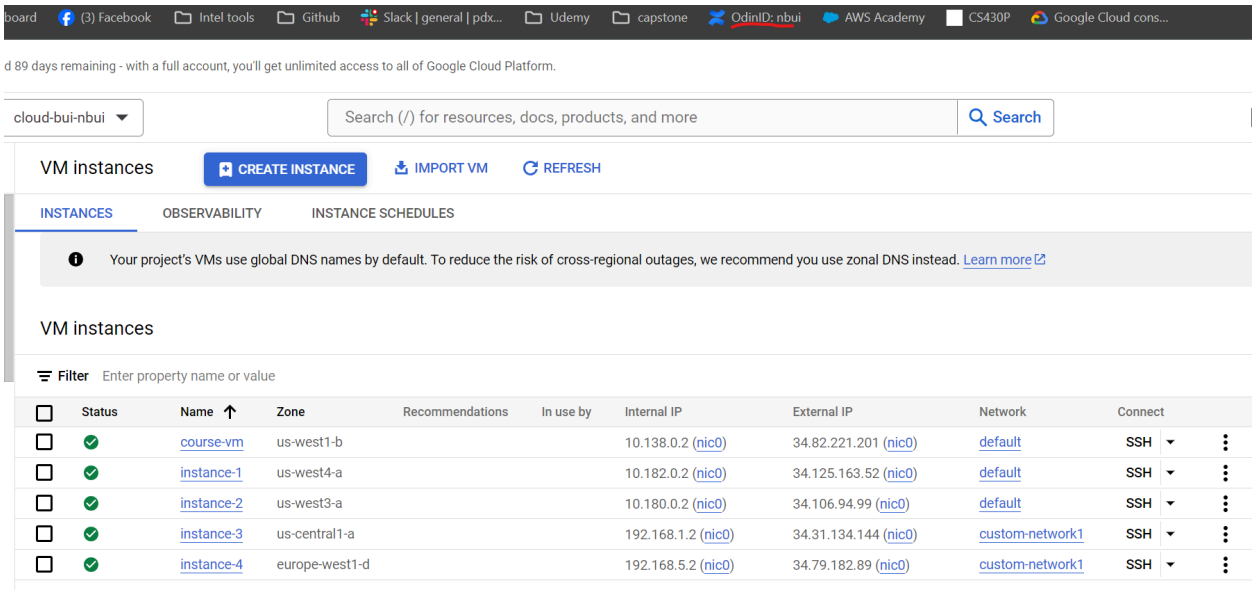
6. Creating custom networks

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

```
EXTERNAL_IPV6_PREFIX:
nbui@cloudshell:~ (cloud-bui-nbui)$ 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:
nbui@cloudshell:~ (cloud-bui-nbui)$
```

- Explain why the result of this ping is different from when you performed the ping to instance-2:
    - Because instances 3 & 4 are in different zones (e.g they are not able to communicate internally with instance 1 anymore) and the request got blocked by firewalls or subnet security layers.

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



- 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.