Lab 1 Notebook

01.2

1. IPV4: 131.252.208.103/24
   Physical MAC Address: 52:54:00:13:a0:c6

```
khod2@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 10334sec preferred_lft 10334sec
khod2@ada:~$
```

   Default router's IP: 131.252.208.1

```
khod2@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
khod2@ada:~$
```

   Name of default router: router.seas.pdx.edu

   Hardware address of default router: 00:00:5e:00:01:01

```
131.252.208.5            ether   52:54:00:87:21:c4   C                     ens3
131.252.208.1            ether   00:00:5e:00:01:01   C                     ens3
131.252.208.78           ether   cc:aa:77:5a:ee:d5   C                     ens3
131.252.208.13           ether   52:54:00:68:7f:45   C                     ens3
131.252.208.54           ether   52:54:00:f6:f8:54   C                     ens3
131.252.208.127                  (incomplete)                              ens3
131.252.208.38           ether   00:00:5e:00:01:26   C                     ens3
131.252.208.99           ether   cc:aa:77:e0:d5:93   C                     ens3
131.252.208.172          ether   cc:aa:77:06:98:2b   C                     ens3
131.252.208.83           ether   00:00:5e:00:01:53   C                     ens3
131.252.208.75           ether   cc:aa:77:3c:a8:f6   C                     ens3
131.252.208.55           ether   52:54:00:58:b5:8e   C                     ens3
131.252.208.112          ether   52:54:00:a5:68:d1   C                     ens3
131.252.208.63           ether   cc:aa:77:f1:d3:21   C                     ens3
131.252.208.124          ether   cc:aa:77:2f:fa:de   C                     ens3
131.252.208.59           ether   00:00:5e:00:01:3b   C                     ens3
131.252.208.250          ether   e0:89:9d:a8:0a:dd   C                     ens3
131.252.208.100          ether   cc:aa:77:8f:61:cb   C                     ens3
131.252.208.96           ether   cc:aa:77:5b:a1:c8   C                     ens3
131.252.208.43           ether   cc:aa:77:ed:72:3e   C                     ens3
131.252.208.23           ether   52:54:00:5c:6f:6e   C                     ens3
131.252.208.84           ether   00:00:5e:00:01:54   C                     ens3
131.252.208.7            ether   cc:aa:77:2e:16:a0   C                     ens3
131.252.208.3            ether   f4:cc:55:0c:71:00   C                     ens3
khod2@ada:~$
```

There are 48 entries in the ARP table.

```
khod2@ada:~$ arp -a | wc -l
48
khod2@ada:~$
```

2. IP addresses that share the same hardware address:
   mirrors.cat.pdx.edu (131.252.208.20) and simirror.cat.pdx.edu (131.252.208.121)
   rocket-01.cat.pdx.edu (131.252.208.15) and rocket.cat.pdx.edu (131.252.208.7)

```
khod2@ada:~$ arp -a | sort -k 3
router.seas.pdx.edu (131.252.208.1) at 00:00:5e:00:01:01 [ether] on ens3
walt.ee.pdx.edu (131.252.208.38) at 00:00:5e:00:01:26 [ether] on ens3
rdns.cat.pdx.edu (131.252.208.53) at 00:00:5e:00:01:35 [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
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
? (169.254.169.254) at 30:e4:db:f9:26:37 [ether] on ens3
radiant.seas.pdx.edu (131.252.208.212) at 30:e4:db:f9:26:37 [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
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
quizor3.cs.pdx.edu (131.252.208.13) at 52:54:00:68:7f:45 [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
aarl-web.mme.pdx.edu (131.252.208.105) at 52:54:00:93:91:b9 [ether] on ens3
quizor6.cs.pdx.edu (131.252.208.60) at 52:54:00:a3:46:7f [ether] on ens3
omr-adns-01.cat.pdx.edu (131.252.208.112) at 52:54:00:a5:68:d1 [ether] on ens3
dc-rdns-01.cat.pdx.edu (131.252.208.117) at 52:54:00:a9:30:9f [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
quizor2.cs.pdx.edu (131.252.208.172) at cc:aa:77:06:98:2b [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
rocket-01.cat.pdx.edu (131.252.208.15) at cc:aa:77:2e:16:a0 [ether] on ens3
rocket.cat.pdx.edu (131.252.208.7) at cc:aa:77:2e:16:a0 [ether] on ens3
quizortest.cs.pdx.edu (131.252.208.124) at cc:aa:77:2f:fa:de [ether] on ens3
web-users-ataru.cat.pdx.edu (131.252.208.75) at cc:aa:77:3c:a8:f6 [ether] on ens3
destiny.cat.pdx.edu (131.252.208.17) at cc:aa:77:50:b9:5d [ether] on ens3
termite.cat.pdx.edu (131.252.208.78) at cc:aa:77:5a:ee:d5 [ether] on ens3
web-users-lum.cat.pdx.edu (131.252.208.96) at cc:aa:77:5b:a1:c8 [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
concertina.cat.pdx.edu (131.252.208.73) at cc:aa:77:91:be:3f [ether] on ens3
web-therest-ataru.cat.pdx.edu (131.252.208.99) at cc:aa:77:e0:d5:93 [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
? (131.252.208.250) 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
support.cat.pdx.edu (131.252.208.127) at <incomplete> on ens3
khod2@ada:~$
```

There are 45 unique hardware addresses. There are three less hardware addresses than IP addresses in the ARP table.

```
khod2@ada:~$ arp -a | sort -k 4 | awk '{print $4}' | uniq | wc -l
45
khod2@ada:~$
```

```
khod2@ada:~$ arp -a | sort -k 2 | awk '{print $2}' | uniq | wc -l
48
khod2@ada:~$
```

List of IP addresses into file command: arp -an | awk -F '[()]' '{print $2}' > arp_entries

Most of the IP addresses in the arp_entries file share the *131.252.208* network prefix.

3. Local ethernet card interface IP address: 10.138.0.2/32
   Local ethernet card interface MAC address: 42:01:0a:8a:00:02

```
khod2@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
    altname enp0s4
    inet 10.138.0.2/32 metric 100 scope global dynamic ens4
       valid_lft 81458sec preferred_lft 81458sec
    inet6 fe80::4001:aff:fe8a:2/64 scope link
       valid_lft forever preferred_lft forever
khod2@course-vm:~$
```

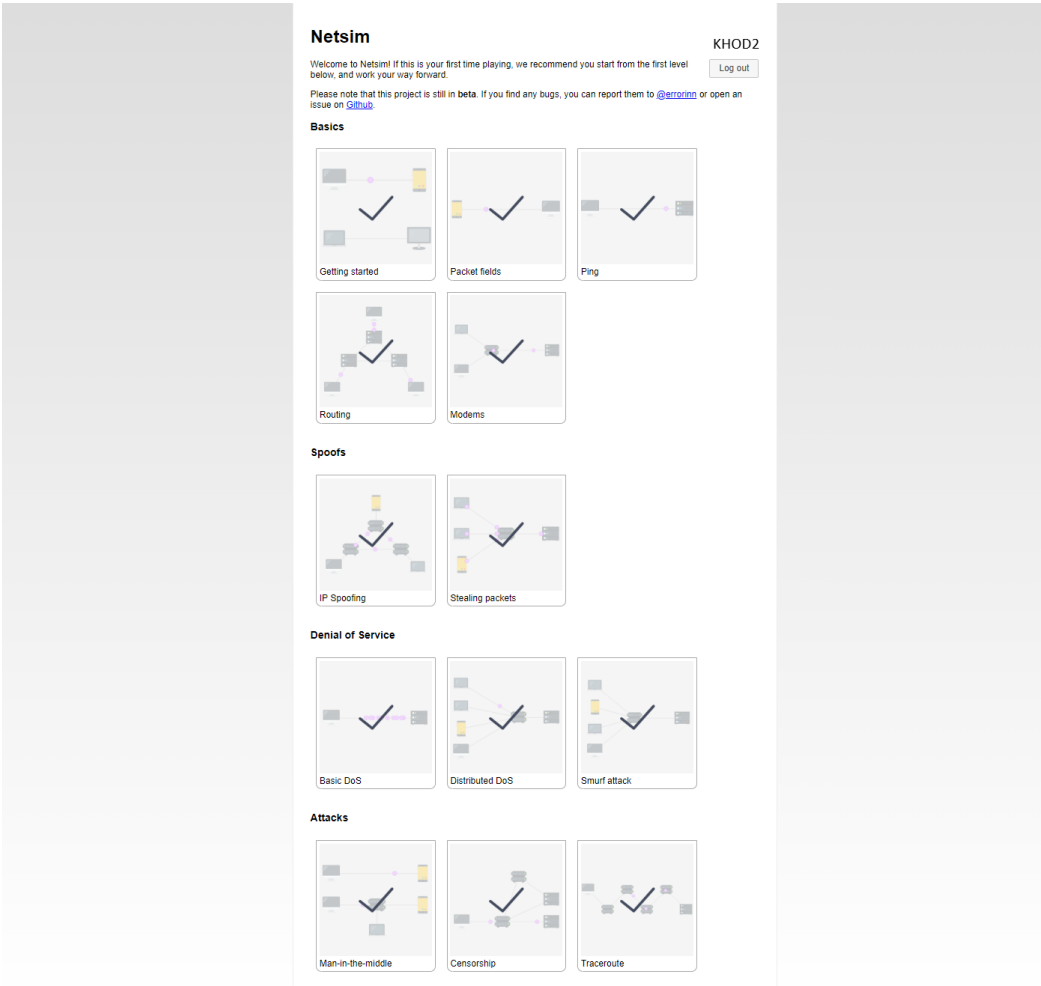
The default router's IP address (gateway address) is 10.138.0.1.

```
khod2@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
khod2@course-vm:~$
```

The default router's hardware address: 42:01:0a:8a:00:01

```
khod2@course-vm:~$ arp 10.138.0.1
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   42:01:0a:8a:00:01   C                     ens4
khod2@course-vm:~$
```

4. All levels completed



01.3

3. Output of nmap:

```
khod2@course-vm:~$ nmap 10.140.0.4/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-03 04:50 UTC
Nmap scan report for grav-30-september-2019-1-vm.c.cloud-khodakovskiy-khod2.internal (10.140.0.3)
Host is up (0.0011s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap scan report for course-vm.c.cloud-khodakovskiy-khod2.internal (10.140.0.4)
Host is up (0.0010s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
3389/tcp open  ms-wbt-server

Nmap scan report for joomla-4-vm.c.cloud-khodakovskiy-khod2.internal (10.140.0.5)
Host is up (0.00032s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap scan report for wordpress-redis-2-vm.c.cloud-khodakovskiy-khod2.internal (10.140.0.6)
Host is up (0.093s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
10000/tcp open  snet-sensor-mgmt

Nmap done: 256 IP addresses (4 hosts up) scanned in 36.11 seconds
khod2@course-vm:~$
```

5. There are 39 subnetworks created on the *default* network. There are 18 regions with subnetworks in the list.

```
khod2@cloudshell:~ (cloud-khodakovskiy-khod2)$ gcloud compute networks subnets list | grep 'NETWORK: default' | wc -l
39
khod2@cloudshell:~ (cloud-khodakovskiy-khod2)$
```

The CIDR /20 suffix denotes the 2^12 (4096) hosts available on each subnetwork.

Based on the ranges in the subnets list, the two instances would be on the australia-southest1 and asia-east1 subnetworks, with a cider suffix of /20. They correspond directly to the appropriate regions specified with the previous commands.

```
khod2@cloudshell:~ (cloud-khodakovskiy-khod2)$ gcloud compute ssh instance-1
khod2@instance-1:~$ ping 10.140.0.2
PING 10.140.0.2 (10.140.0.2) 56(84) bytes of data.
64 bytes from 10.140.0.2: icmp_seq=1 ttl=64 time=132 ms
64 bytes from 10.140.0.2: icmp_seq=2 ttl=64 time=130 ms
64 bytes from 10.140.0.2: icmp_seq=3 ttl=64 time=130 ms
64 bytes from 10.140.0.2: icmp_seq=4 ttl=64 time=130 ms
64 bytes from 10.140.0.2: icmp_seq=5 ttl=64 time=130 ms
64 bytes from 10.140.0.2: icmp_seq=6 ttl=64 time=130 ms
```

I think the virtual switch facilitates this connectivity, since it connects routes between each of the virtual subnets that the instances are on.

6. Custom subnets created in the custom network:

```
NAME: subnet-us-central-192
REGION: us-central1
NETWORK: custom-network1
RANGE: 192.168.1.0/24
STACK_TYPE: IPV4_ONLY
IPV6_ACCESS_TYPE:          KHOD2
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: 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:
```

The result of pinging instance-3 and -4 from instance-1 is different from pinging instance-2 because instance-2 is on the same private network as -1, and IP addresses have access to other internal IPs from within the same network. Instance-1 can't ping instance-3 because it's attempting to ping the private internal IP of an instance on another network.

VM instances

Filter Enter property name or value

Status	Name	Zone	Recommendations	In use by	Internal IP	External IP	Network	Connect
✓	course-vm	us-west1-b			10.138.0.2 (nic0)	34.105.85.33 (nic0)	default	SSH
✓	instance-1	australia-southeast1-b			10.152.0.2 (nic0)	35.189.50.179 (nic0)	default	SSH
✓	instance-2	asia-east1-a			10.140.0.2 (nic0)	35.201.232.124 (nic0)	default	SSH
✓	instance-3	us-central1-a			192.168.1.2 (nic0)	35.239.244.246 (nic0)	custom-network1	SSH
✓	instance-4	europe-west1-d			192.168.5.2 (nic0)	34.38.61.157 (nic0)	custom-network1	SSH

Subnets for custom network:

Subnets ADD SUBNET FLOW LOGS

Filter Enter property name or value

Name	Region	Stack Type	Internal IP ranges	External IP ranges	Secondary IPv4 ranges	Gateway
subnet-europe-west-192	europe-west1	IPv4	192.168.5.0/24	None	None	192.168.5.1
subnet-us-central-192	us-central1	IPv4	192.168.1.0/24	None	None	192.168.1.1

Subnets for default network:

Subnets ADD SUBNET FLOW LOGS

Filter Enter property name or value

Name	Region	Stack Type	Internal IP ranges	External IP ranges	Secondary IPv4 ranges	Gateway
default	us-central1	IPv4	10.128.0.0/20	None	None	10.128.0.1
default	europe-west1	IPv4	10.132.0.0/20	None	None	10.132.0.1
default	us-west1	IPv4	10.138.0.0/20	None	None	10.138.0.1
default	asia-east1	IPv4	10.140.0.0/20	None	None	10.140.0.1
default	us-east1	IPv4	10.142.0.0/20	None	None	10.142.0.1
default	asia-northeast1	IPv4	10.146.0.0/20	None	None	10.146.0.1
default	asia-southeast1	IPv4	10.148.0.0/20	None	None	10.148.0.1
default	us-east4	IPv4	10.150.0.0/20	None	None	10.150.0.1
default	australia-southeast1	IPv4	10.152.0.0/20	None	None	10.152.0.1
default	europe-west2	IPv4	10.154.0.0/20	None	None	10.154.0.1