Lab 01

Stuart Rimel
CS530: Internet Web & Cloud, Fall 2023

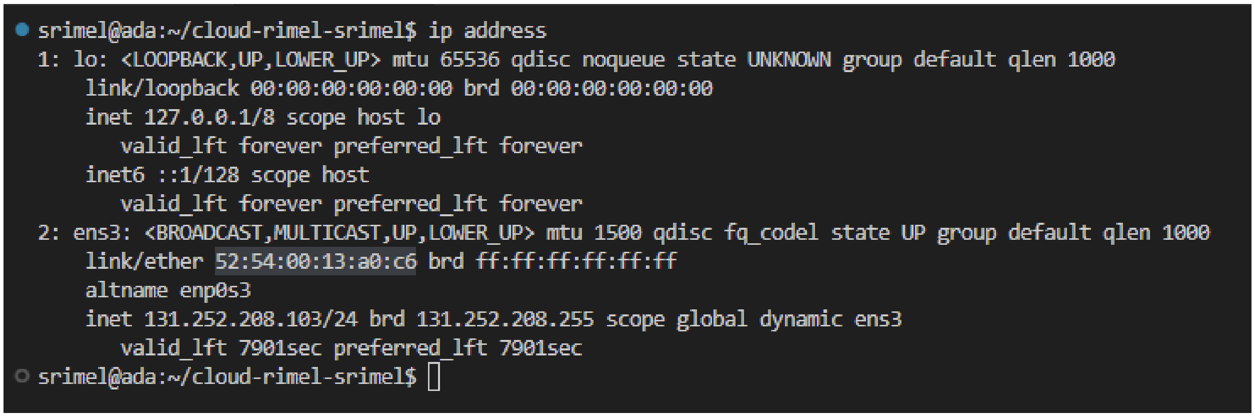
Odin: srimel
** In all the terminal screenshots my Odin name is in the terminal prompt **

Table of Contents:

1.2: ARP, Wireshark, Netsim

1.2.1: ARP

I ran the “ip address” command while ssh’d into linux.cs.pdx.edu and found the following results:



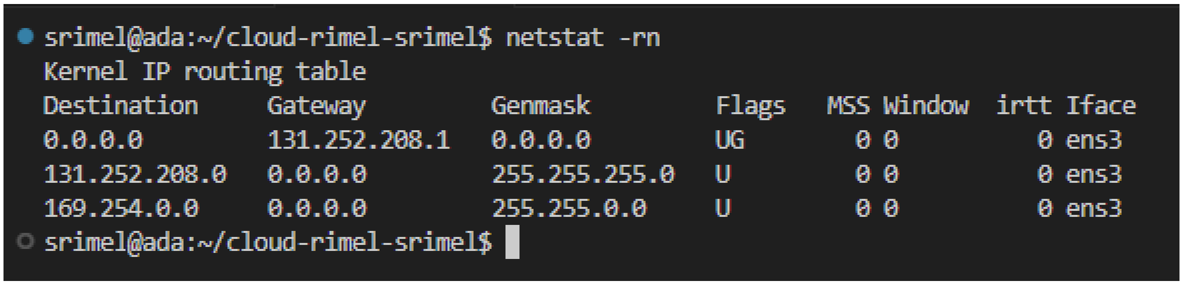
```
srimel@ada:~/cloud-rimel-srimel$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope 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 7901sec preferred_lft 7901sec
srimel@ada:~/cloud-rimel-srimel$ 
```

The inet field has the IPv4 address and the link/ether field has the hardware address.

Results for local ethernet card interface: ens3
IPv4: 131.252.208.103/24
MAC: 52:54:00:13:a0:c6

Netstat Command

Performed the following command of “netstat -rn” and received the following IP routing table:

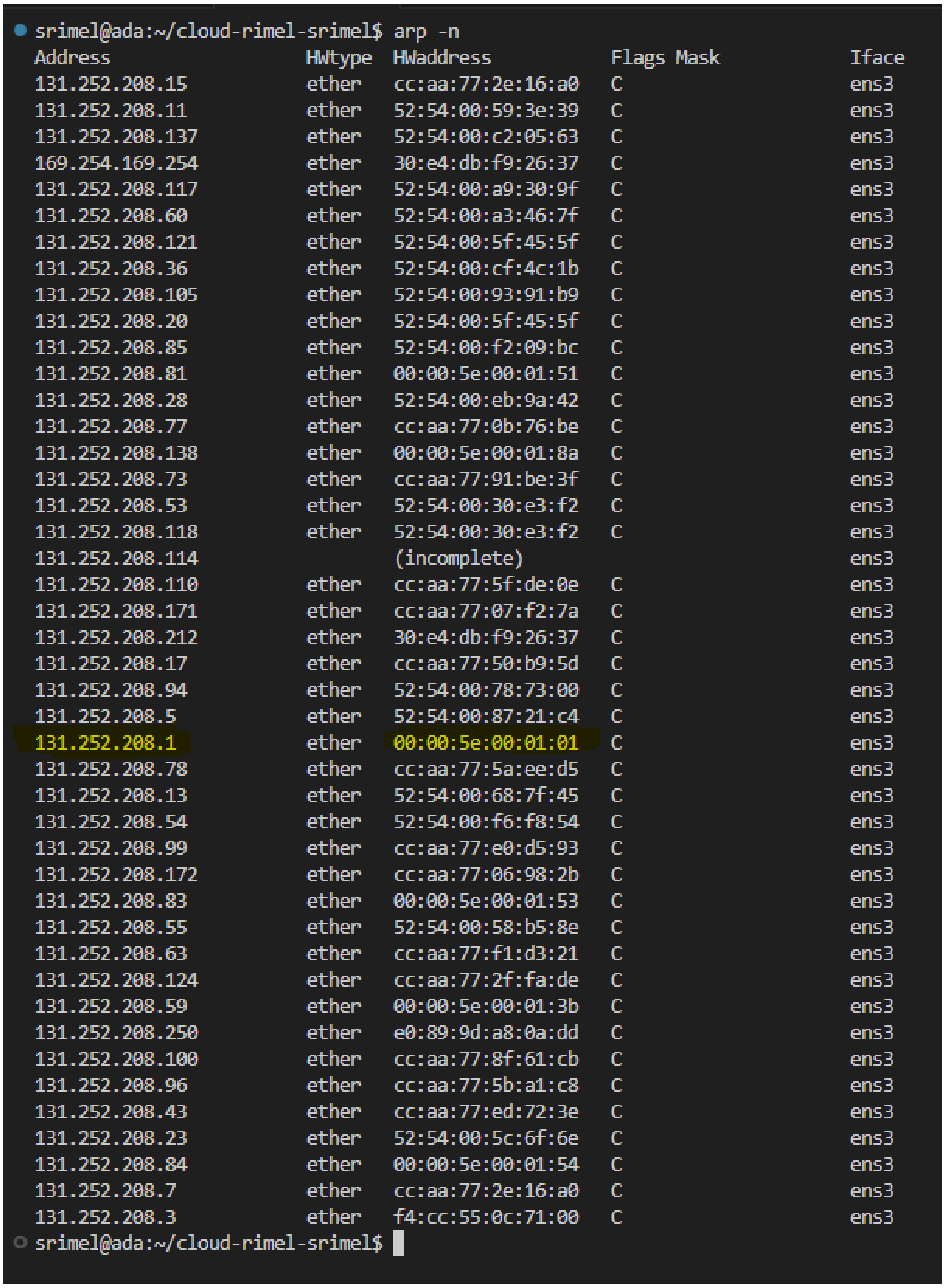


```
srimel@ada:~/cloud-rimel-srimel$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         131.252.208.1   0.0.0.0         UG        0 0          0 ens3
131.252.208.0   0.0.0.0         255.255.255.0   U         0 0          0 ens3
169.254.0.0     0.0.0.0         255.255.0.0     U         0 0          0 ens3
srimel@ada:~/cloud-rimel-srimel$
```

Default router’s IP address is: 131.252.208.1

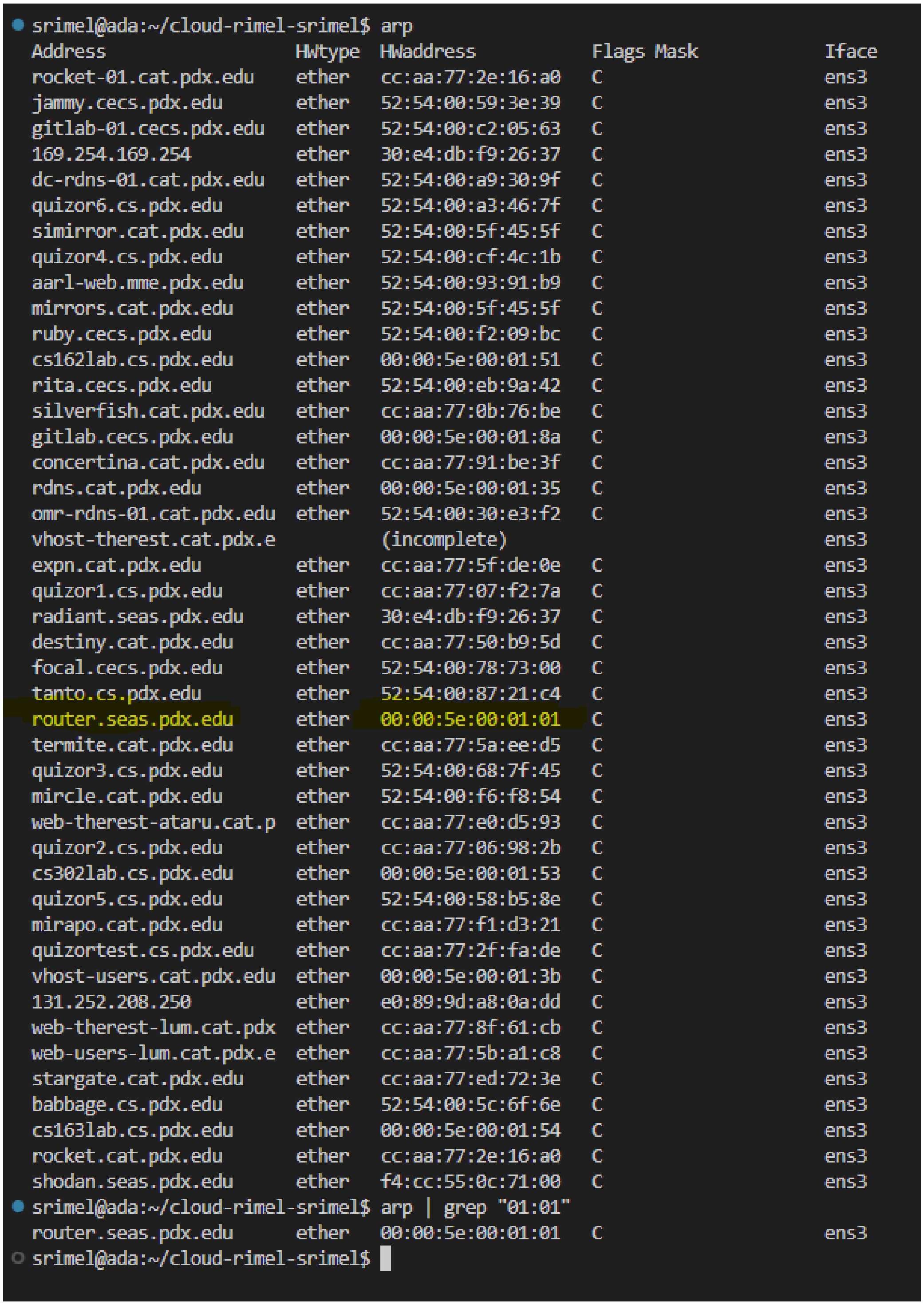
Arp Command

With “-n” gets the Hardware Address for the router: 00:00:5e:00:01:01



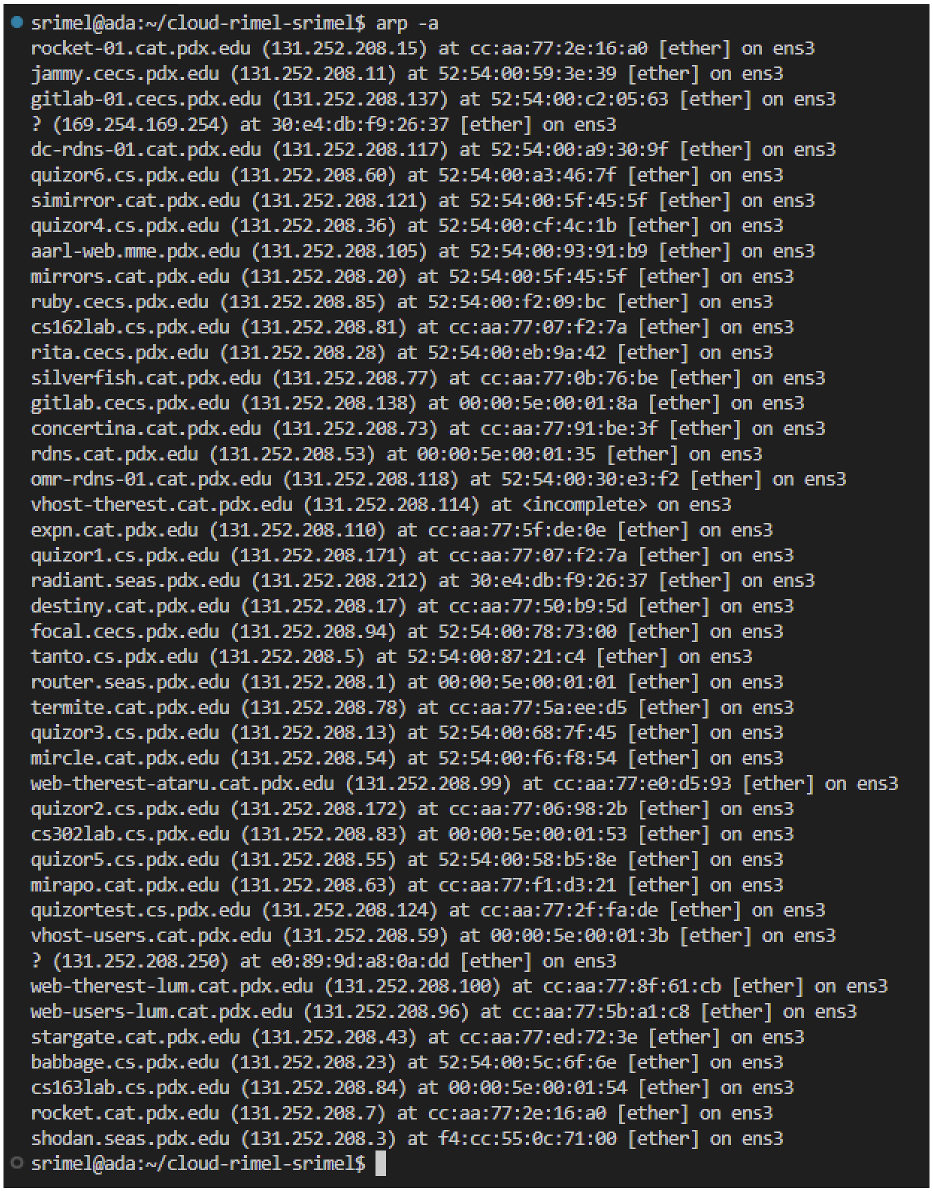
```
srimel@ada:~/cloud-rimel-srimel$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
131.252.208.15           ether   cc:aa:77:2e:16:a0   C                     ens3
131.252.208.11           ether   52:54:00:59:3e:39   C                     ens3
131.252.208.137          ether   52:54:00:c2:05:63   C                     ens3
169.254.169.254          ether   30:e4:db:f9:26:37   C                     ens3
131.252.208.117          ether   52:54:00:a9:30:9f   C                     ens3
131.252.208.60           ether   52:54:00:a3:46:7f   C                     ens3
131.252.208.121          ether   52:54:00:5f:45:5f   C                     ens3
131.252.208.36           ether   52:54:00:cf:4c:1b   C                     ens3
131.252.208.105          ether   52:54:00:93:91:b9   C                     ens3
131.252.208.20           ether   52:54:00:5f:45:5f   C                     ens3
131.252.208.85           ether   52:54:00:f2:09:bc   C                     ens3
131.252.208.81           ether   00:00:5e:00:01:51   C                     ens3
131.252.208.28           ether   52:54:00:eb:9a:42   C                     ens3
131.252.208.77           ether   cc:aa:77:0b:76:be   C                     ens3
131.252.208.138          ether   00:00:5e:00:01:8a   C                     ens3
131.252.208.73           ether   cc:aa:77:91:be:3f   C                     ens3
131.252.208.53           ether   52:54:00:30:e3:f2   C                     ens3
131.252.208.118          ether   52:54:00:30:e3:f2   C                     ens3
131.252.208.114                  (incomplete)                              ens3
131.252.208.110          ether   cc:aa:77:5f:de:0e   C                     ens3
131.252.208.171          ether   cc:aa:77:07:f2:7a   C                     ens3
131.252.208.212          ether   30:e4:db:f9:26:37   C                     ens3
131.252.208.17           ether   cc:aa:77:50:b9:5d   C                     ens3
131.252.208.94           ether   52:54:00:78:73:00   C                     ens3
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
131.252.208.99           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
131.252.208.55           ether   52:54:00:58:b5:8e   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
srimel@ada:~/cloud-rimel-srimel$
```

Without “-n” gets the name of the router: router.seas.pdx.edu



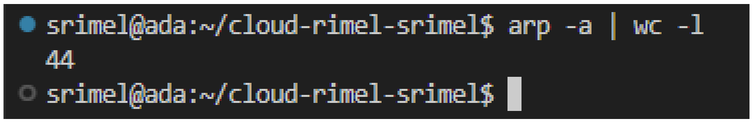
```
srimel@ada:~/cloud-rimel-srimel$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
rocket-01.cat.pdx.edu    ether   cc:aa:77:2e:16:a0   C                     ens3
jammy.cecs.pdx.edu       ether   52:54:00:59:3e:39   C                     ens3
gitlab-01.cecs.pdx.edu   ether   52:54:00:c2:05:63   C                     ens3
169.254.169.254          ether   30:e4:db:f9:26:37   C                     ens3
dc-rdns-01.cat.pdx.edu   ether   52:54:00:a9:30:9f   C                     ens3
quizor6.cs.pdx.edu       ether   52:54:00:a3:46:7f   C                     ens3
simirror.cat.pdx.edu     ether   52:54:00:5f:45:5f   C                     ens3
quizor4.cs.pdx.edu       ether   52:54:00:cf:4c:1b   C                     ens3
aarl-web.mme.pdx.edu     ether   52:54:00:93:91:b9   C                     ens3
mirrors.cat.pdx.edu      ether   52:54:00:5f:45:5f   C                     ens3
ruby.cecs.pdx.edu        ether   52:54:00:f2:09:bc   C                     ens3
cs162lab.cs.pdx.edu      ether   00:00:5e:00:01:51   C                     ens3
rita.cecs.pdx.edu        ether   52:54:00:eb:9a:42   C                     ens3
silverfish.cat.pdx.edu   ether   cc:aa:77:0b:76:be   C                     ens3
gitlab.cecs.pdx.edu      ether   00:00:5e:00:01:8a   C                     ens3
concertina.cat.pdx.edu   ether   cc:aa:77:91:be:3f   C                     ens3
rdns.cat.pdx.edu         ether   00:00:5e:00:01:35   C                     ens3
omr-rdns-01.cat.pdx.edu  ether   52:54:00:30:e3:f2   C                     ens3
vhost-therest.cat.pdx.e          (incomplete)                              ens3
expn.cat.pdx.edu         ether   cc:aa:77:5f:de:0e   C                     ens3
quizor1.cs.pdx.edu       ether   cc:aa:77:07:f2:7a   C                     ens3
radiant.seas.pdx.edu     ether   30:e4:db:f9:26:37   C                     ens3
destiny.cat.pdx.edu      ether   cc:aa:77:50:b9:5d   C                     ens3
focal.cecs.pdx.edu       ether   52:54:00:78:73:00   C                     ens3
tanto.cs.pdx.edu         ether   52:54:00:87:21:c4   C                     ens3
router.seas.pdx.edu      ether   00:00:5e:00:01:01   C                     ens3
termite.cat.pdx.edu      ether   cc:aa:77:5a:ee:d5   C                     ens3
quizor3.cs.pdx.edu       ether   52:54:00:68:7f:45   C                     ens3
mircle.cat.pdx.edu       ether   52:54:00:f6:f8:54   C                     ens3
web-therest-ataru.cat.p  ether   cc:aa:77:e0:d5:93   C                     ens3
quizor2.cs.pdx.edu       ether   cc:aa:77:06:98:2b   C                     ens3
cs302lab.cs.pdx.edu      ether   00:00:5e:00:01:53   C                     ens3
quizor5.cs.pdx.edu       ether   52:54:00:58:b5:8e   C                     ens3
mirapo.cat.pdx.edu       ether   cc:aa:77:f1:d3:21   C                     ens3
quizortest.cs.pdx.edu    ether   cc:aa:77:2f:fa:de   C                     ens3
vhost-users.cat.pdx.edu  ether   00:00:5e:00:01:3b   C                     ens3
131.252.208.250          ether   e0:89:9d:a8:0a:dd   C                     ens3
web-therest-lum.cat.pdx  ether   cc:aa:77:8f:61:cb   C                     ens3
web-users-lum.cat.pdx.e  ether   cc:aa:77:5b:a1:c8   C                     ens3
stargate.cat.pdx.edu     ether   cc:aa:77:ed:72:3e   C                     ens3
babbage.cs.pdx.edu       ether   52:54:00:5c:6f:6e   C                     ens3
cs163lab.cs.pdx.edu      ether   00:00:5e:00:01:54   C                     ens3
rocket.cat.pdx.edu       ether   cc:aa:77:2e:16:a0   C                     ens3
shodan.seas.pdx.edu      ether   f4:cc:55:0c:71:00   C                     ens3
srimel@ada:~/cloud-rimel-srimel$ arp | grep "01:01"
router.seas.pdx.edu      ether   00:00:5e:00:01:01   C                     ens3
srimel@ada:~/cloud-rimel-srimel$
```

Running command “arp -a” shows both the DNS name and ip address of the full table.



```
srimel@ada:~/cloud-rimel-srimel$ arp -a
rocket-01.cat.pdx.edu (131.252.208.15) at cc:aa:77:2e:16:a0 [ether] on ens3
jammy.cecs.pdx.edu (131.252.208.11) at 52:54:00:59:3e:39 [ether] on ens3
gitlab-01.cecs.pdx.edu (131.252.208.137) at 52:54:00:c2:05:63 [ether] on ens3
? (169.254.169.254) at 30:e4:db:f9:26:37 [ether] on ens3
dc-rdns-01.cat.pdx.edu (131.252.208.117) at 52:54:00:a9:30:9f [ether] on ens3
quizor6.cs.pdx.edu (131.252.208.60) at 52:54:00:a3:46:7f [ether] on ens3
simirror.cat.pdx.edu (131.252.208.121) at 52:54:00:5f:45:5f [ether] on ens3
quizor4.cs.pdx.edu (131.252.208.36) at 52:54:00:cf:4c:1b [ether] on ens3
aarl-web.mme.pdx.edu (131.252.208.105) at 52:54:00:93:91:b9 [ether] on ens3
mirrors.cat.pdx.edu (131.252.208.20) at 52:54:00:5f:45:5f [ether] on ens3
ruby.cecs.pdx.edu (131.252.208.85) at 52:54:00:f2:09:bc [ether] on ens3
cs162lab.cs.pdx.edu (131.252.208.81) at cc:aa:77:07:f2:7a [ether] on ens3
rita.cecs.pdx.edu (131.252.208.28) at 52:54:00:eb:9a:42 [ether] on ens3
silverfish.cat.pdx.edu (131.252.208.77) at cc:aa:77:0b:76:be [ether] on ens3
gitlab.cecs.pdx.edu (131.252.208.138) at 00:00:5e:00:01:8a [ether] on ens3
concertina.cat.pdx.edu (131.252.208.73) at cc:aa:77:91:be:3f [ether] on ens3
rdns.cat.pdx.edu (131.252.208.53) at 00:00:5e:00:01:35 [ether] on ens3
omr-rdns-01.cat.pdx.edu (131.252.208.118) at 52:54:00:30:e3:f2 [ether] on ens3
vhost-therest.cat.pdx.edu (131.252.208.114) at <incomplete> on ens3
expn.cat.pdx.edu (131.252.208.110) at cc:aa:77:5f:de:0e [ether] on ens3
quizor1.cs.pdx.edu (131.252.208.171) at cc:aa:77:07:f2:7a [ether] on ens3
radiant.seas.pdx.edu (131.252.208.212) at 30:e4:db:f9:26:37 [ether] on ens3
destiny.cat.pdx.edu (131.252.208.17) at cc:aa:77:50:b9:5d [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
router.seas.pdx.edu (131.252.208.1) at 00:00:5e:00:01:01 [ether] on ens3
termite.cat.pdx.edu (131.252.208.78) at cc:aa:77:5a:ee:d5 [ether] on ens3
quizor3.cs.pdx.edu (131.252.208.13) at 52:54:00:68:7f:45 [ether] on ens3
mircle.cat.pdx.edu (131.252.208.54) at 52:54:00:f6:f8:54 [ether] on ens3
web-therest-ataru.cat.pdx.edu (131.252.208.99) at cc:aa:77:e0:d5:93 [ether] on ens3
quizor2.cs.pdx.edu (131.252.208.172) at cc:aa:77:06:98:2b [ether] on ens3
cs302lab.cs.pdx.edu (131.252.208.83) at 00:00:5e:00:01:53 [ether] on ens3
quizor5.cs.pdx.edu (131.252.208.55) at 52:54:00:58:b5:8e [ether] on ens3
mirapo.cat.pdx.edu (131.252.208.63) at cc:aa:77:f1:d3:21 [ether] on ens3
quizortest.cs.pdx.edu (131.252.208.124) at cc:aa:77:2f:fa:de [ether] on ens3
vhost-users.cat.pdx.edu (131.252.208.59) at 00:00:5e:00:01:3b [ether] on ens3
? (131.252.208.250) at e0:89:9d:a8:0a:dd [ether] on ens3
web-therest-lum.cat.pdx.edu (131.252.208.100) at cc:aa:77:8f:61:cb [ether] on ens3
web-users-lum.cat.pdx.edu (131.252.208.96) at cc:aa:77:5b:a1:c8 [ether] on ens3
stargate.cat.pdx.edu (131.252.208.43) at cc:aa:77:ed:72:3e [ether] on ens3
babbage.cs.pdx.edu (131.252.208.23) at 52:54:00:5c:6f:6e [ether] on ens3
cs163lab.cs.pdx.edu (131.252.208.84) at 00:00:5e:00:01:54 [ether] on ens3
rocket.cat.pdx.edu (131.252.208.7) at cc:aa:77:2e:16:a0 [ether] on ens3
shodan.seas.pdx.edu (131.252.208.3) at f4:cc:55:0c:71:00 [ether] on ens3
srimel@ada:~/cloud-rimel-srimel$
```

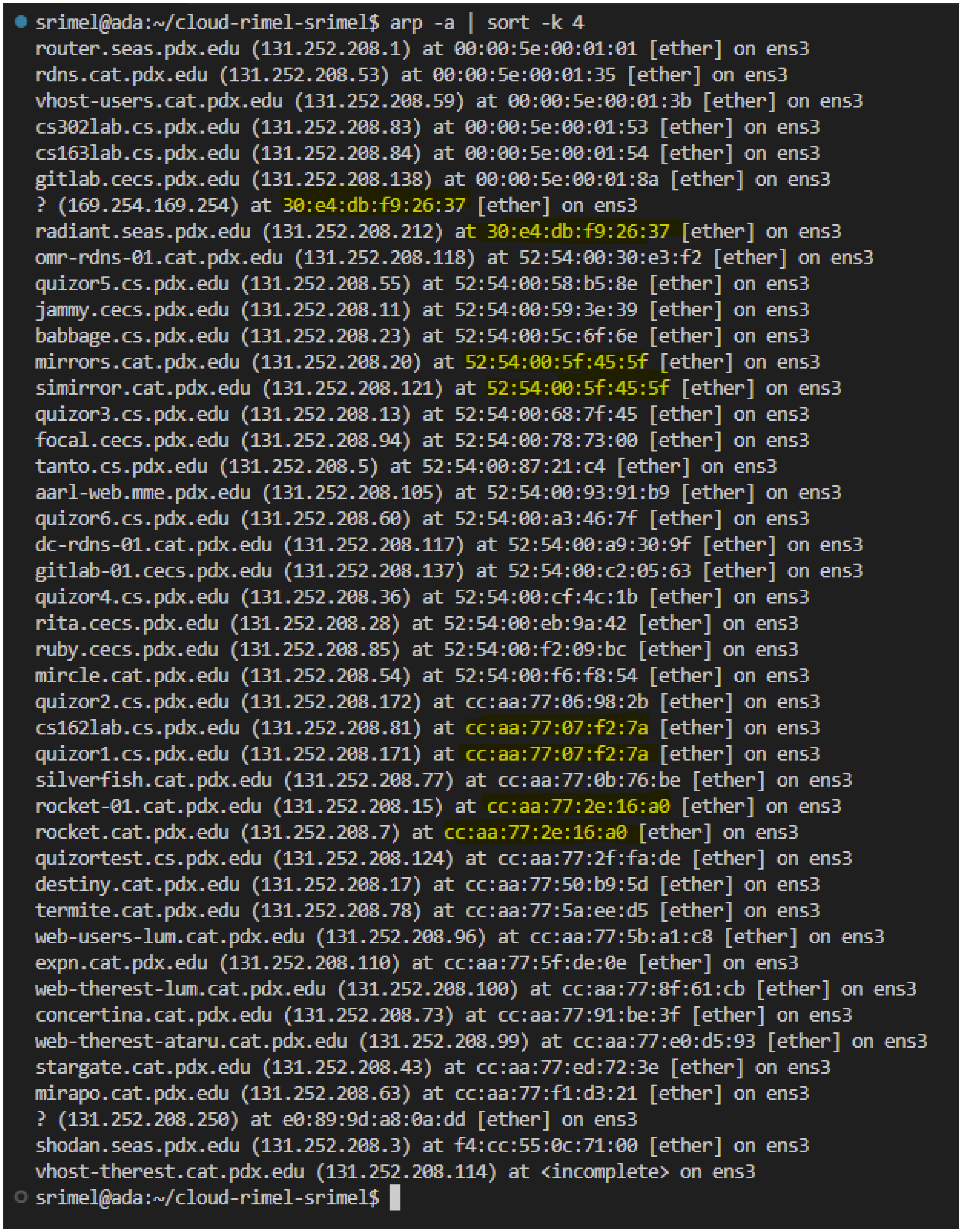
Running command “arp -a | wc -l” results in a count of 44 entries in the arp table.



```
srimel@ada:~/cloud-rimel-srimel$ arp -a | wc -l
44
srimel@ada:~/cloud-rimel-srimel$
```

1.2.2: -

Running command “arp -a | sort -k 4” will sort by MAC address:



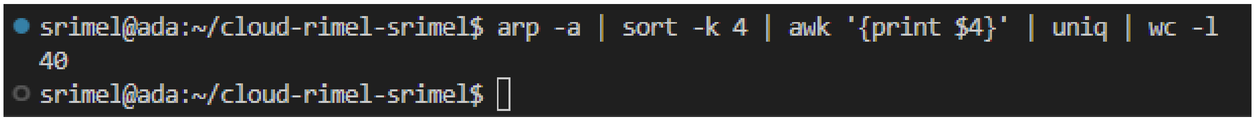
```
srimel@ada:~/cloud-rimel-srimel$ arp -a | sort -k 4
router.seas.pdx.edu (131.252.208.1) at 00:00:5e:00:01:01 [ether] on ens3
rdns.cat.pdx.edu (131.252.208.53) at 00:00:5e:00:01:35 [ether] on ens3
vhost-users.cat.pdx.edu (131.252.208.59) at 00:00:5e:00:01:3b [ether] on ens3
cs302lab.cs.pdx.edu (131.252.208.83) 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
? (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
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
cs162lab.cs.pdx.edu (131.252.208.81) at cc:aa:77:07:f2:7a [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
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
vhost-therest.cat.pdx.edu (131.252.208.114) at <incomplete> on ens3
srimel@ada:~/cloud-rimel-srimel$
```

IPs that share same hardware address:

- 169.254.169.254, 131.252.208.212 = 30:e4:db:f9:26:37
- 131.252.208.81, 131.252.208.171 = cc:aa:77:07:f2:7a
- 131.252.208.15, 131.252.208.7 = cc:aa:77:2e:16:a0
- 131.252.208.20, 131.252.208.121 = 52:54:00:5f:45:5f

Manually counting the duplication hardware addresses gives a result of 4.

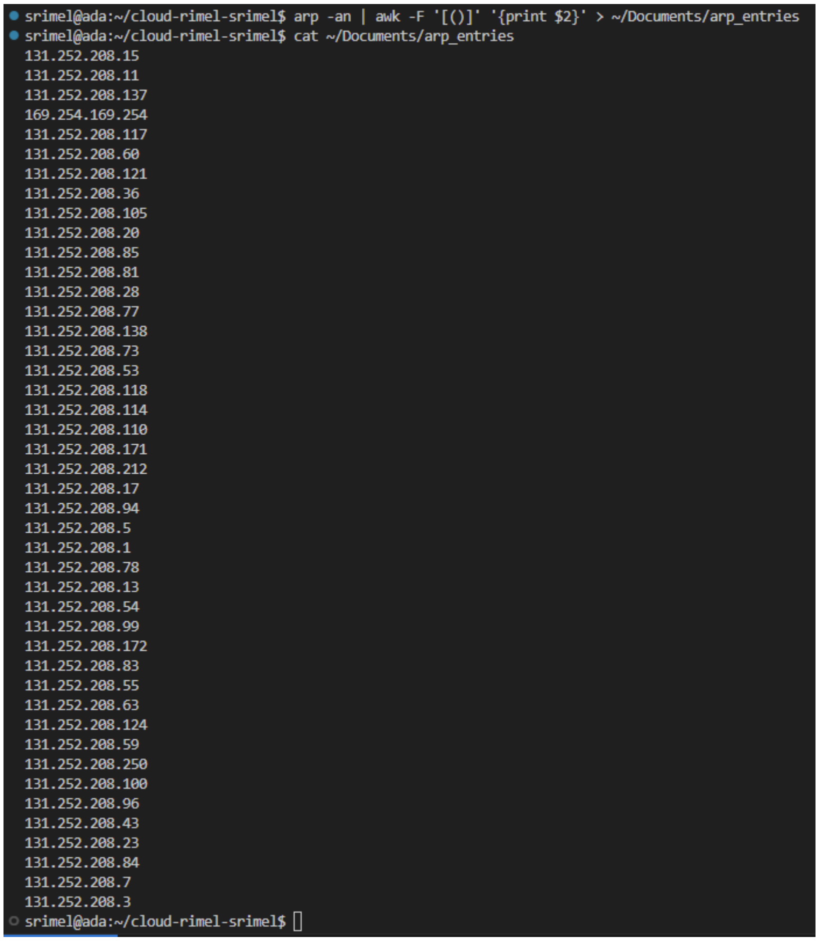
Running command “arp -a | sort -k 4 | awk '{print $4}' | uniq | wc -l” gives the result of: 40



```
● srimel@ada:~/cloud-rimel-srimel$ arp -a | sort -k 4 | awk '{print $4}' | uniq | wc -l
  40
○ srimel@ada:~/cloud-rimel-srimel$ ▯
```

The difference gives us 4 duplicated hardware addresses which confirms the manual count.

Command to generate arp entries for arp table:
“arp -an | awk -F '[()]' '{print $2}' > ~/Documents/arp_entries”

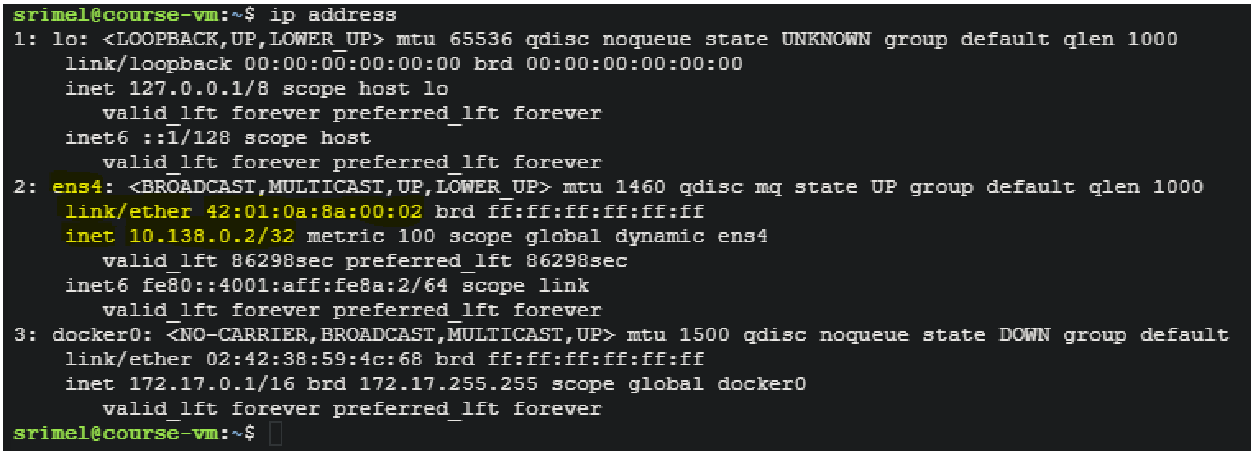


```
● srimel@ada:~/cloud-rimel-srimel$ arp -an | awk -F '[()]' '{print $2}' > ~/Documents/arp_entries
● srimel@ada:~/cloud-rimel-srimel$ cat ~/Documents/arp_entries
  131.252.208.15
  131.252.208.11
  131.252.208.137
  169.254.169.254
  131.252.208.117
  131.252.208.60
  131.252.208.121
  131.252.208.36
  131.252.208.105
  131.252.208.20
  131.252.208.85
  131.252.208.81
  131.252.208.28
  131.252.208.77
  131.252.208.138
  131.252.208.73
  131.252.208.53
  131.252.208.118
  131.252.208.114
  131.252.208.110
  131.252.208.171
  131.252.208.212
  131.252.208.17
  131.252.208.94
  131.252.208.5
  131.252.208.1
  131.252.208.78
  131.252.208.13
  131.252.208.54
  131.252.208.99
  131.252.208.172
  131.252.208.83
  131.252.208.55
  131.252.208.63
  131.252.208.124
  131.252.208.59
  131.252.208.250
  131.252.208.100
  131.252.208.96
  131.252.208.43
  131.252.208.23
  131.252.208.84
  131.252.208.7
  131.252.208.3
○ srimel@ada:~/cloud-rimel-srimel$ ▯
```

The common network prefix is within the arp table is: 131.252.208

1.2.3: ARP (Cloud)

Ran command “ip address” and found the following local ethernet card interface:

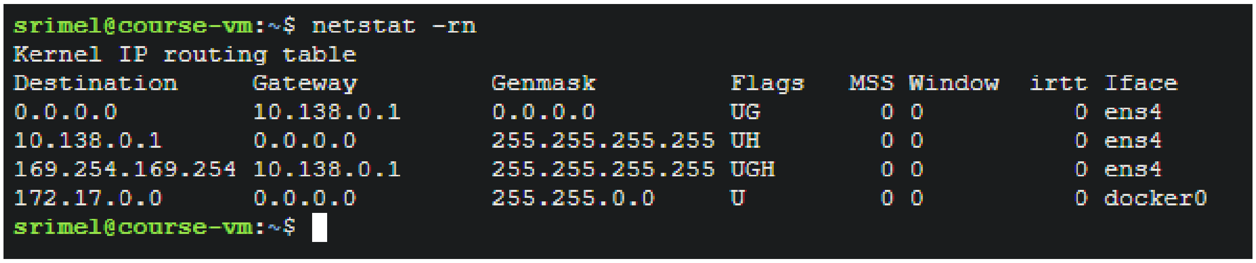


```
srimel@course-vm:~$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       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 86298sec preferred_lft 86298sec
    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 02:42:38:59:4c:68 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
srimel@course-vm:~$
```

ens4:

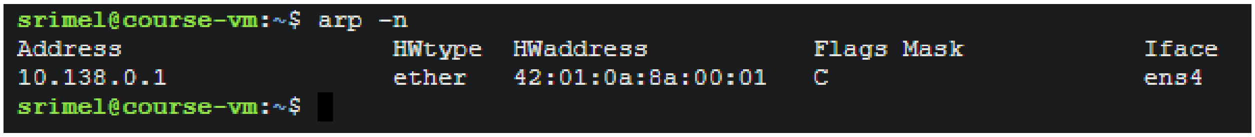
- IPv4: 10.138.0.2
- Hardware: 42:01:0a:8a:00:02

Result of “netstat -rn”:



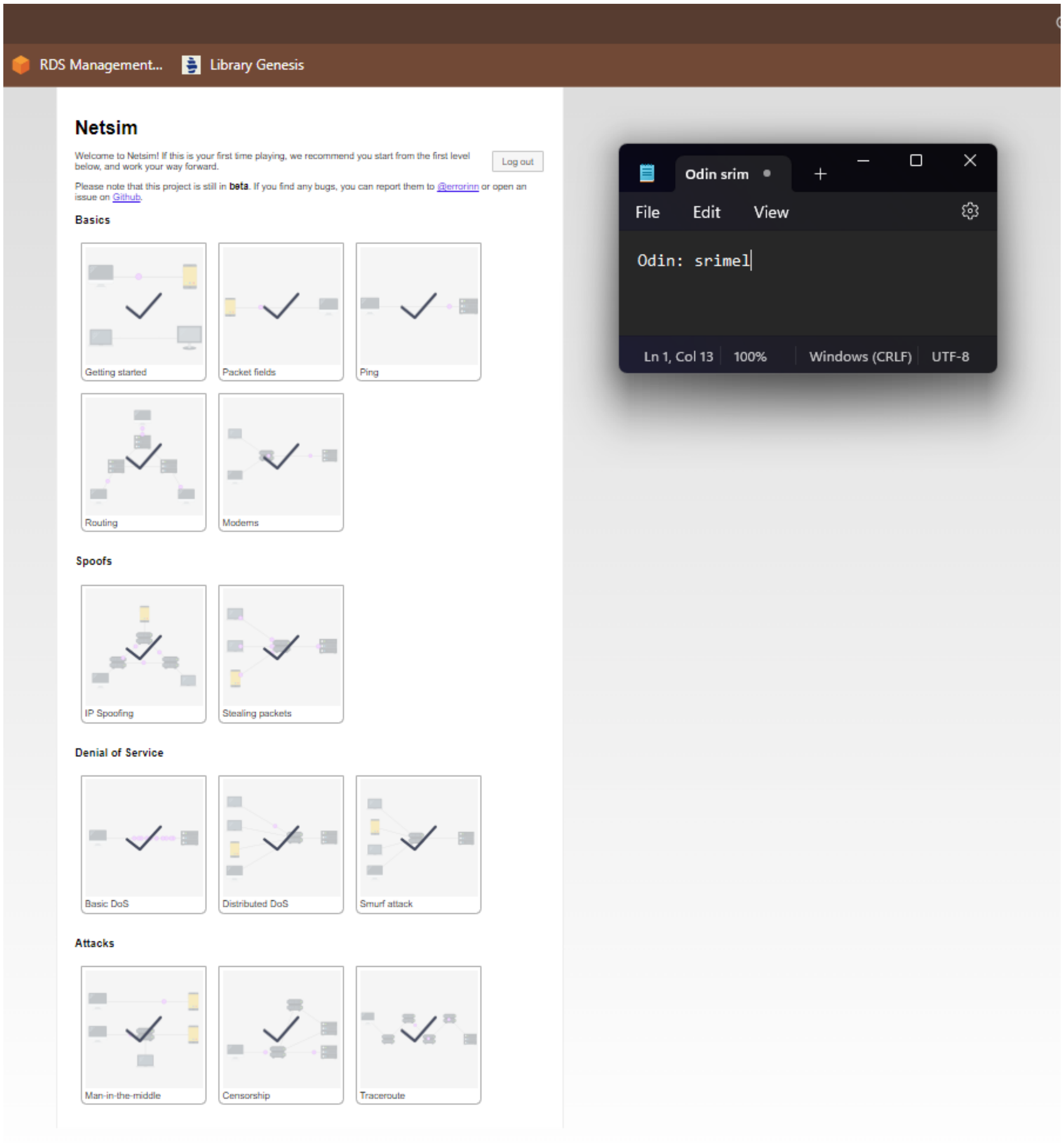
```
srimel@course-vm:~$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         10.138.0.1      0.0.0.0         UG        0 0          0 ens4
10.138.0.1      0.0.0.0         255.255.255.255 UH        0 0          0 ens4
169.254.169.254 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
srimel@course-vm:~$
```

Router IP: 10.1387.0.1
Router MAC: 42:01:0a:8a:00:01



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

1.2.4: Netsim Levels



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.

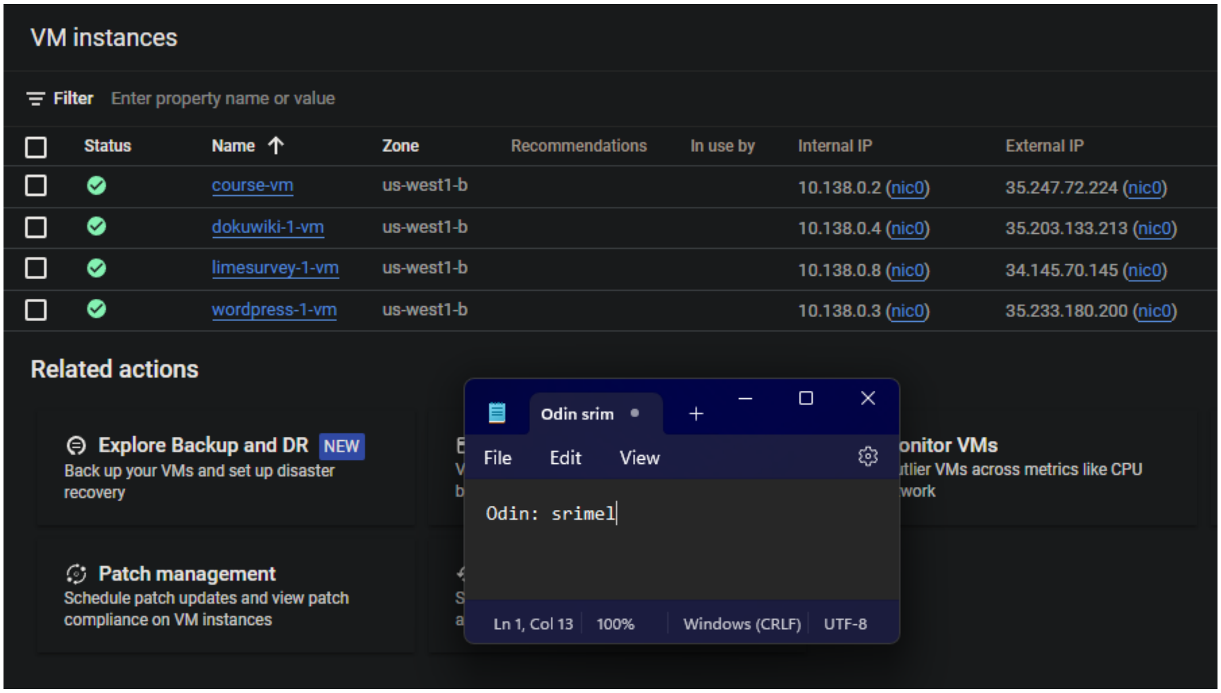
```
Odin: srimel
```

1.3: Cloud Networking

1.3.1-3: Network Scanning (nmap)

Launch Targets: I deployed 3 marketplace vms

- dokuwiki-1-vm
- limesurvey-1-vm
- Wordpress-1-vm



VM instances

Filter Enter property name or value

□	Status	Name ↑	Zone	Recommendations	In use by	Internal IP	External IP
□	✓	course-vm	us-west1-b			10.138.0.2 (nic0)	35.247.72.224 (nic0)
□	✓	dokuwiki-1-vm	us-west1-b			10.138.0.4 (nic0)	35.203.133.213 (nic0)
□	✓	limesurvey-1-vm	us-west1-b			10.138.0.8 (nic0)	34.145.70.145 (nic0)
□	✓	wordpress-1-vm	us-west1-b			10.138.0.3 (nic0)	35.233.180.200 (nic0)

Related actions

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

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

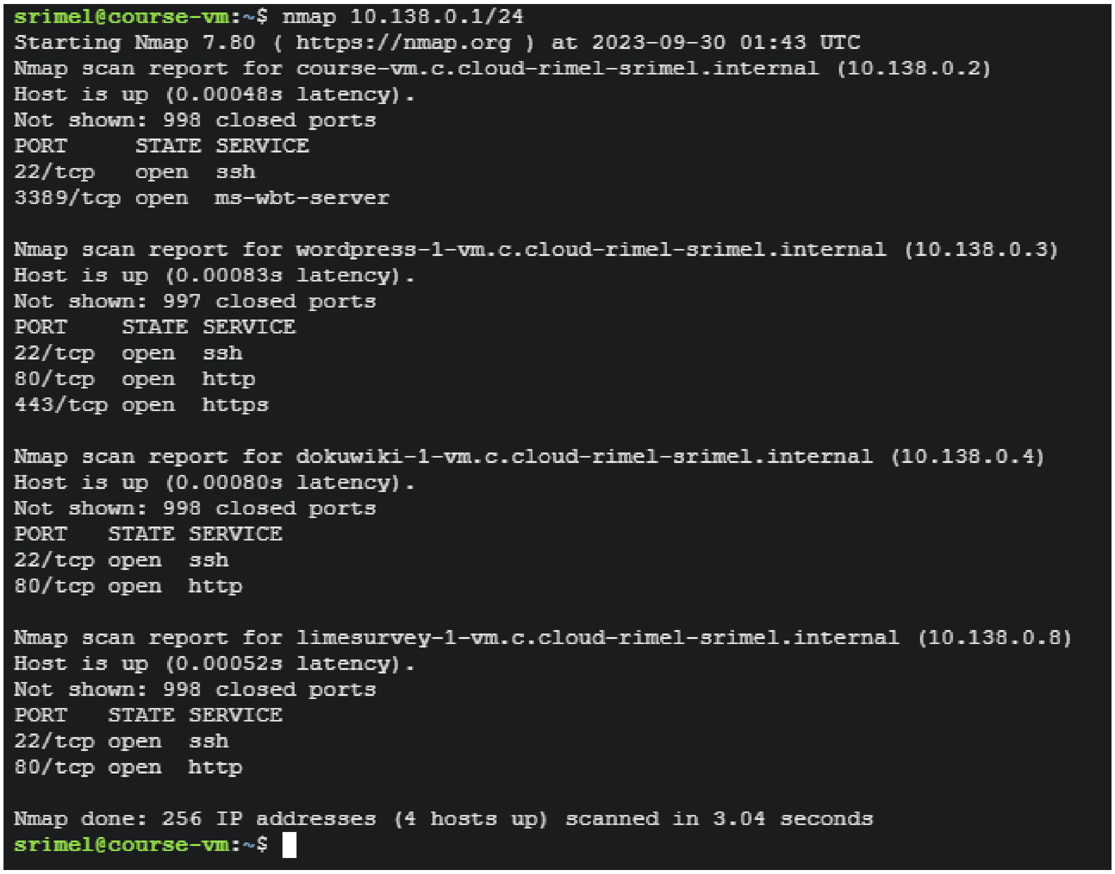
onitor VMs
utlier VMs across metrics like CPU
work

Odin srim

```
Odin: srimel
```

Ln 1, Col 13 | 100% | Windows (CRLF) | UTF-8

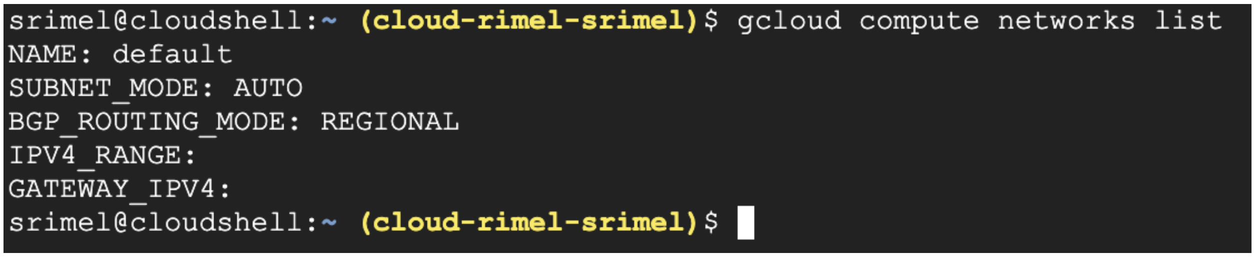
Result from running nmap on the internal subnet:



```
srimel@course-vm:~$ nmap 10.138.0.1/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-09-30 01:43 UTC
Nmap scan report for course-vm.c.cloud-rimel-srimel.internal (10.138.0.2)
Host is up (0.00048s 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-rimel-srimel.internal (10.138.0.3)
Host is up (0.00083s 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 dokuwiki-1-vm.c.cloud-rimel-srimel.internal (10.138.0.4)
Host is up (0.00080s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap scan report for limesurvey-1-vm.c.cloud-rimel-srimel.internal (10.138.0.8)
Host is up (0.00052s 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 3.04 seconds
srimel@course-vm:~$
```

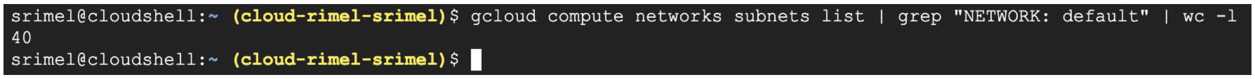
1.3.5: Navigating Default Networks

Default subnetwork for the project:



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

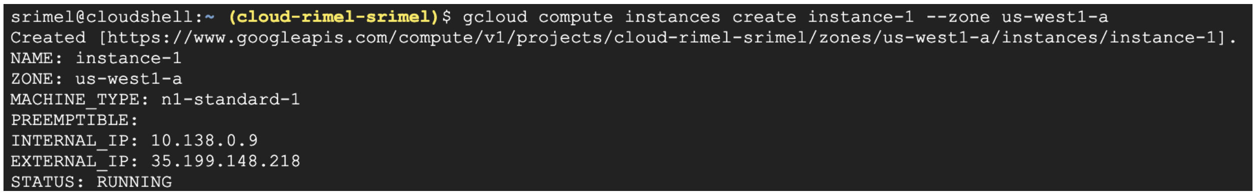
Number of subnets created initially on the default network: 40



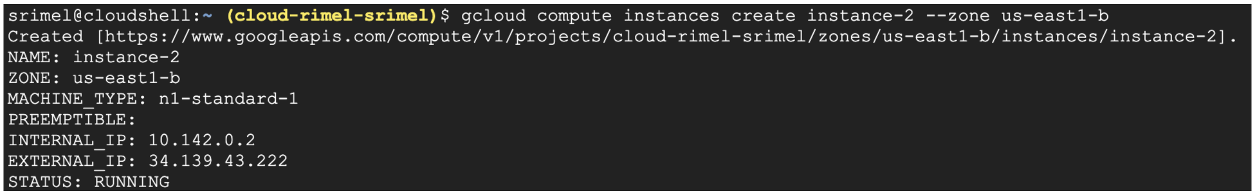
```
srimel@cloudshell:~ (cloud-rimel-srimel)$ gcloud compute networks subnets list | grep "NETWORK: default" | wc -l
40
srimel@cloudshell:~ (cloud-rimel-srimel)$
```

All subnet addresses have a subnet mask of “/20”, therefore the total number of hosts for each subnet would be $2^{12} - 2 = 4094$ hosts.

Create two instances in separate zone / regions:

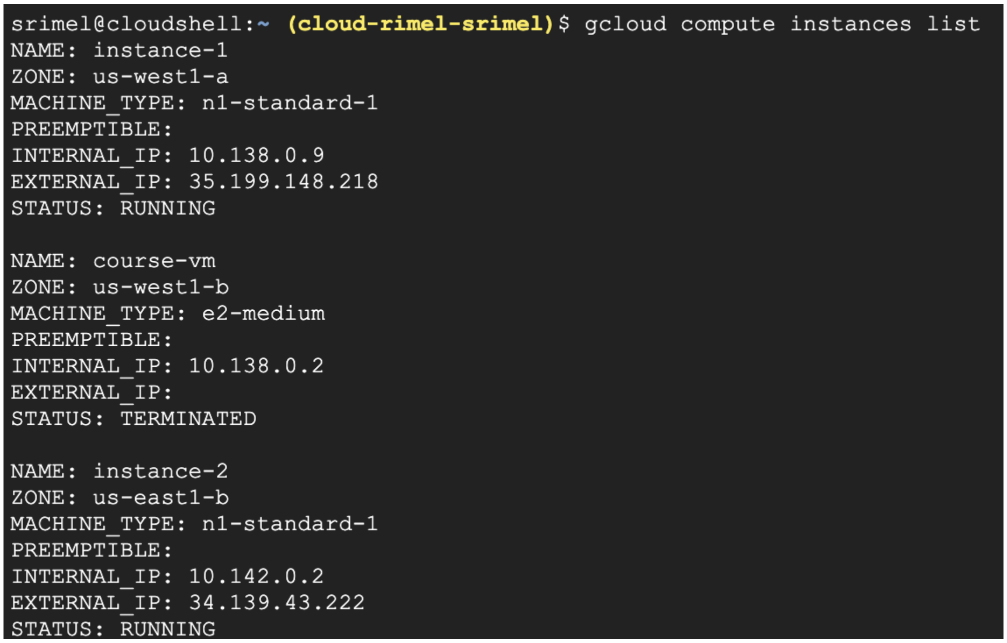


```
srimel@cloudshell:~ (cloud-rimel-srimel)$ gcloud compute instances create instance-1 --zone us-west1-a
Created [https://www.googleapis.com/compute/v1/projects/cloud-rimel-srimel/zones/us-west1-a/instances/instance-1].
NAME: instance-1
ZONE: us-west1-a
MACHINE_TYPE: n1-standard-1
PREEMPTIBLE:
INTERNAL_IP: 10.138.0.9
EXTERNAL_IP: 35.199.148.218
STATUS: RUNNING
```



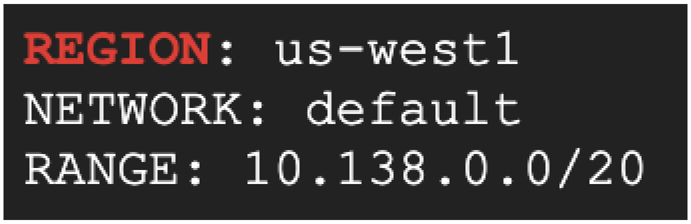
```
srimel@cloudshell:~ (cloud-rimel-srimel)$ gcloud compute instances create instance-2 --zone us-east1-b
Created [https://www.googleapis.com/compute/v1/projects/cloud-rimel-srimel/zones/us-east1-b/instances/instance-2].
NAME: instance-2
ZONE: us-east1-b
MACHINE_TYPE: n1-standard-1
PREEMPTIBLE:
INTERNAL_IP: 10.142.0.2
EXTERNAL_IP: 34.139.43.222
STATUS: RUNNING
```

Listing the instances created:

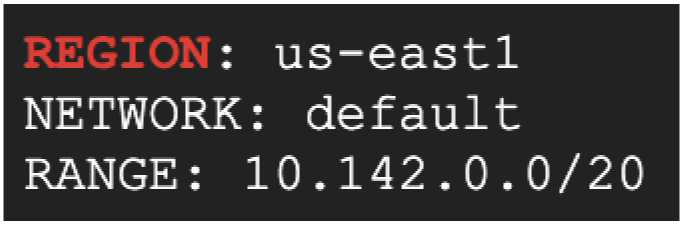


```
srimel@cloudshell:~ (cloud-rimel-srimel)$ gcloud compute instances list
NAME: instance-1
ZONE: us-west1-a
MACHINE_TYPE: n1-standard-1
PREEMPTIBLE:
INTERNAL_IP: 10.138.0.9
EXTERNAL_IP: 35.199.148.218
STATUS: RUNNING

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

NAME: instance-2
ZONE: us-east1-b
MACHINE_TYPE: n1-standard-1
PREEMPTIBLE:
INTERNAL_IP: 10.142.0.2
EXTERNAL_IP: 34.139.43.222
STATUS: RUNNING
```

Instance 1 is on 10.138.0.9, Instance 2 is on 10.142.0.2



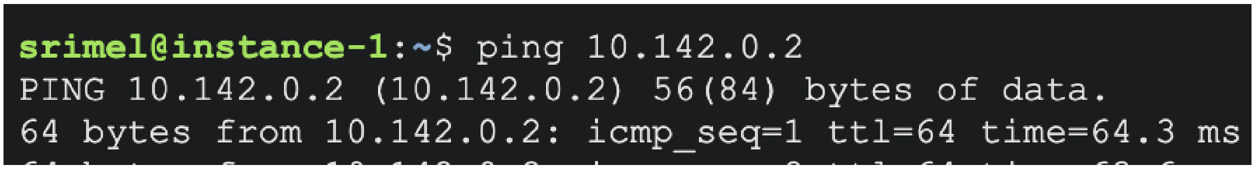
```
REGION: us-west1
NETWORK: default
RANGE: 10.138.0.0/20
```



```
REGION: us-east1
NETWORK: default
RANGE: 10.142.0.0/20
```

Yes, both instances have the appropriate ip prefix for their respective regions.

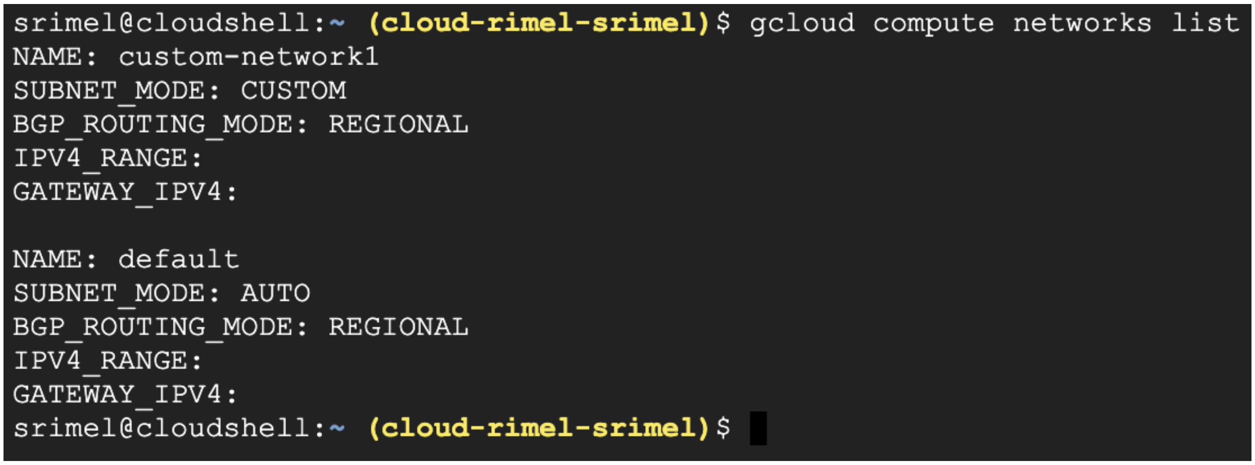
Pinging instance 2 from instance 1:



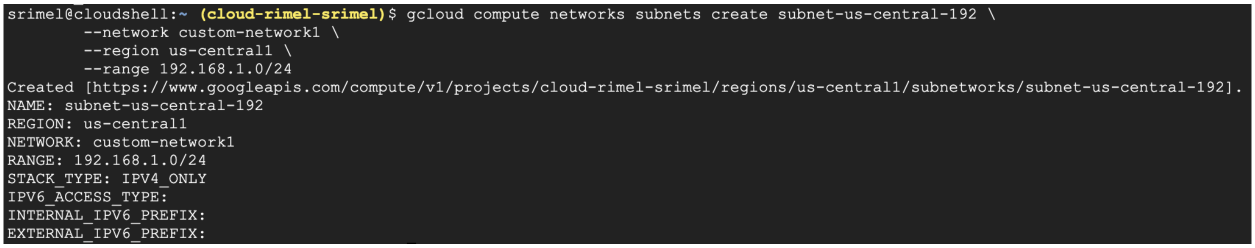
```
srimel@instance-1:~$ ping 10.142.0.2
PING 10.142.0.2 (10.142.0.2) 56(84) bytes of data.
64 bytes from 10.142.0.2: icmp_seq=1 ttl=64 time=64.3 ms
```

I think the virtual switch facilitates this connectivity between instance1 and instance2.

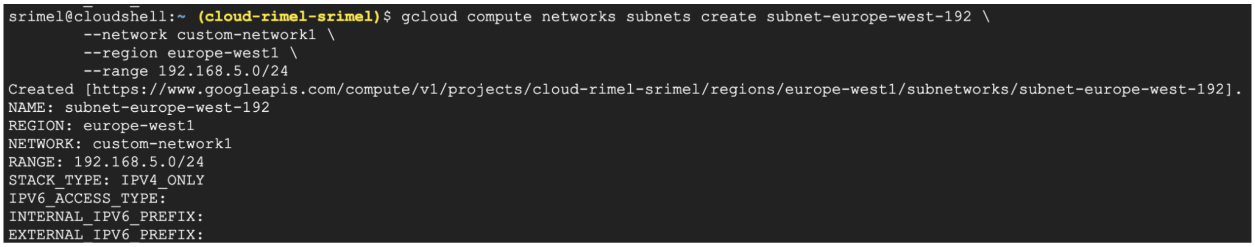
1.3.6: Creating Custom Networks



```
srimel@cloudshell:~ (cloud-rimel-srimel)$ gcloud compute networks list
NAME: custom-network1
SUBNET_MODE: CUSTOM
BGP_ROUTING_MODE: REGIONAL
IPV4_RANGE:
GATEWAY_IPV4:

NAME: default
SUBNET_MODE: AUTO
BGP_ROUTING_MODE: REGIONAL
IPV4_RANGE:
GATEWAY_IPV4:
srimel@cloudshell:~ (cloud-rimel-srimel)$
```

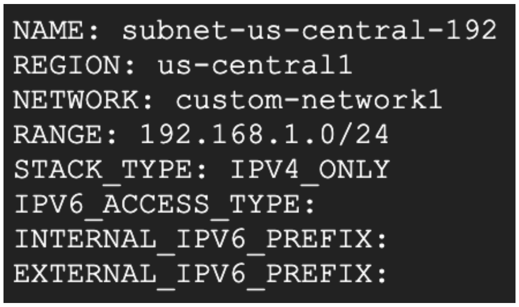


```
srimel@cloudshell:~ (cloud-rimel-srimel)$ gcloud compute networks subnets create subnet-us-central-192 \
        --network custom-network1 \
        --region us-central1 \
        --range 192.168.1.0/24
Created [https://www.googleapis.com/compute/v1/projects/cloud-rimel-srimel/regions/us-central1/subnetworks/subnet-us-central-192].
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:
```

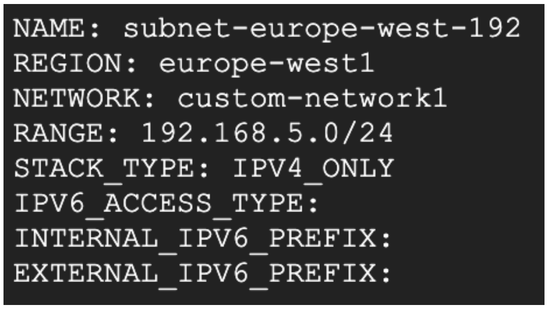


```
srimel@cloudshell:~ (cloud-rimel-srimel)$ gcloud compute networks subnets create subnet-europe-west-192 \
        --network custom-network1 \
        --region europe-west1 \
        --range 192.168.5.0/24
Created [https://www.googleapis.com/compute/v1/projects/cloud-rimel-srimel/regions/europe-west1/subnetworks/subnet-europe-west-192].
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:
```

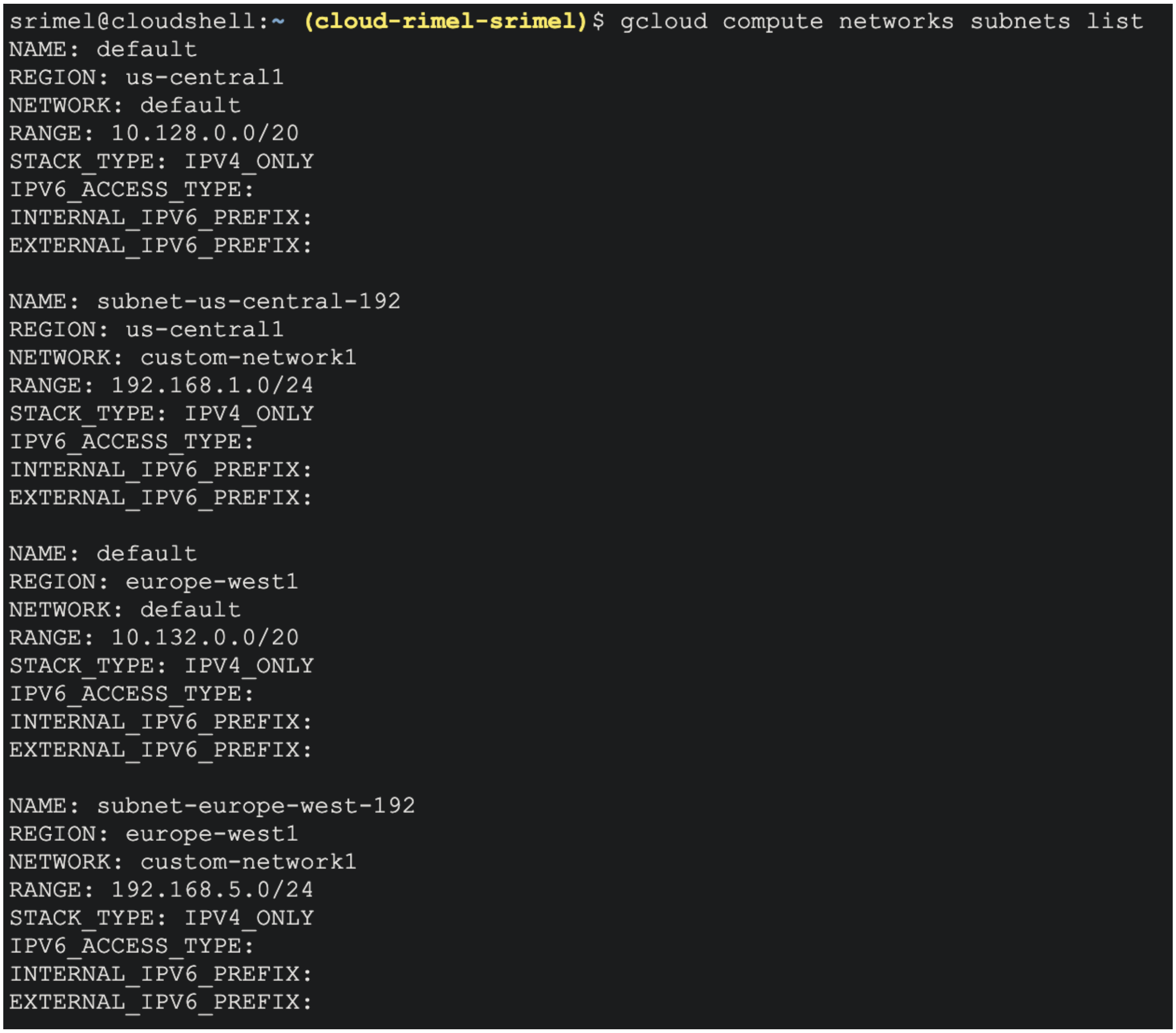
Running “gcloud compute networks subnets list”:



```
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:
```

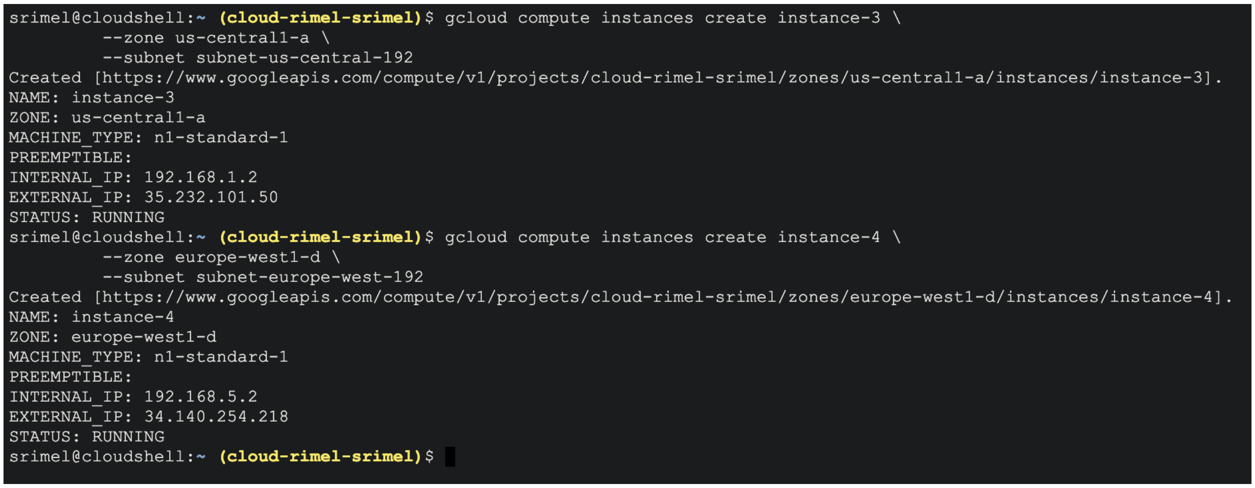


```
NAME: subnet-europe-west-192
REGION: europe-west1
NETWORK: custom-network1
RANGE: 192.168.5.0/24
STACK_TYPE: IPV4_ONLY
IPV6_ACCESS_TYPE:
INTERNAL_IPV6_PREFIX:
EXTERNAL_IPV6_PREFIX:
```



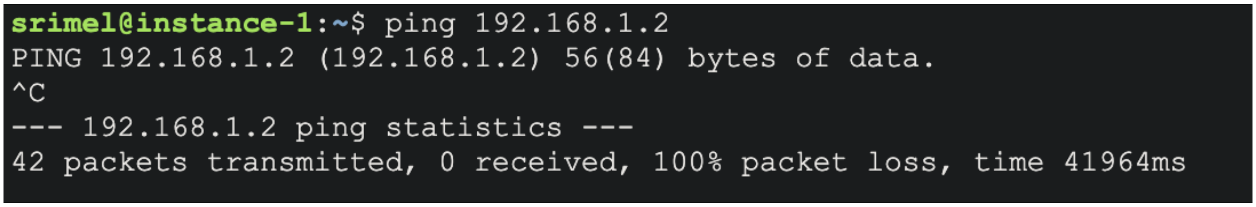
```
srimel@cloudshell:~ (cloud-rimel-srimel)$ gcloud compute networks subnets list
NAME: default
REGION: us-central1
NETWORK: default
RANGE: 10.128.0.0/20
STACK_TYPE: IPV4_ONLY
IPV6_ACCESS_TYPE:
INTERNAL_IPV6_PREFIX:
EXTERNAL_IPV6_PREFIX:

NAME: 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: 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:
```

Create two more instances on custom network:



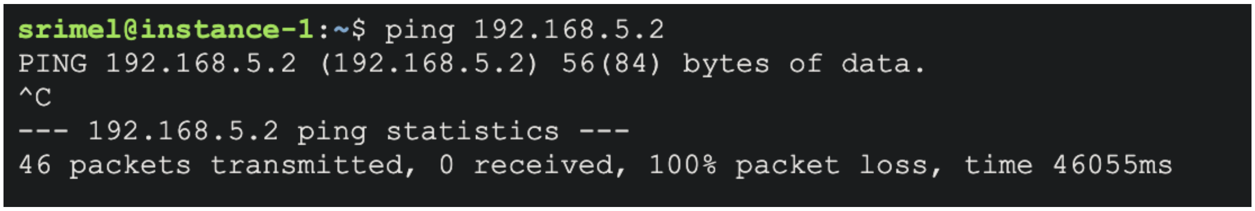
```
srimel@cloudshell:~ (cloud-rimel-srimel)$ gcloud compute instances create instance-3 \
         --zone us-central1-a \
         --subnet subnet-us-central-192
Created [https://www.googleapis.com/compute/v1/projects/cloud-rimel-srimel/zones/us-central1-a/instances/instance-3].
NAME: instance-3
ZONE: us-central1-a
MACHINE_TYPE: n1-standard-1
PREEMPTIBLE:
INTERNAL_IP: 192.168.1.2
EXTERNAL_IP: 35.232.101.50
STATUS: RUNNING
srimel@cloudshell:~ (cloud-rimel-srimel)$ gcloud compute instances create instance-4 \
         --zone europe-west1-d \
         --subnet subnet-europe-west-192
Created [https://www.googleapis.com/compute/v1/projects/cloud-rimel-srimel/zones/europe-west1-d/instances/instance-4].
NAME: instance-4
ZONE: europe-west1-d
MACHINE_TYPE: n1-standard-1
PREEMPTIBLE:
INTERNAL_IP: 192.168.5.2
EXTERNAL_IP: 34.140.254.218
STATUS: RUNNING
srimel@cloudshell:~ (cloud-rimel-srimel)$
```

Ping from instance1 to instance 3:



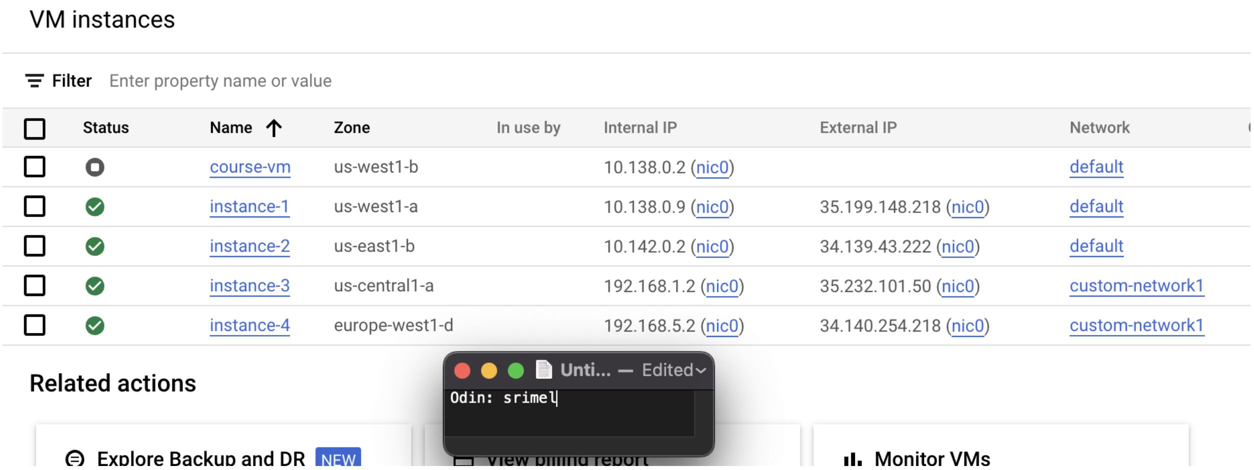
```
srimel@instance-1:~$ ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
^C
--- 192.168.1.2 ping statistics ---
42 packets transmitted, 0 received, 100% packet loss, time 41964ms
```

Ping from instance1 to instance 4:



```
srimel@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 ---
46 packets transmitted, 0 received, 100% packet loss, time 46055ms
```

The reason we can’t ping instance 3 and 4 is because they were created from a custom network and not the default one which is what instances 1 and 2 are on.



VM instances

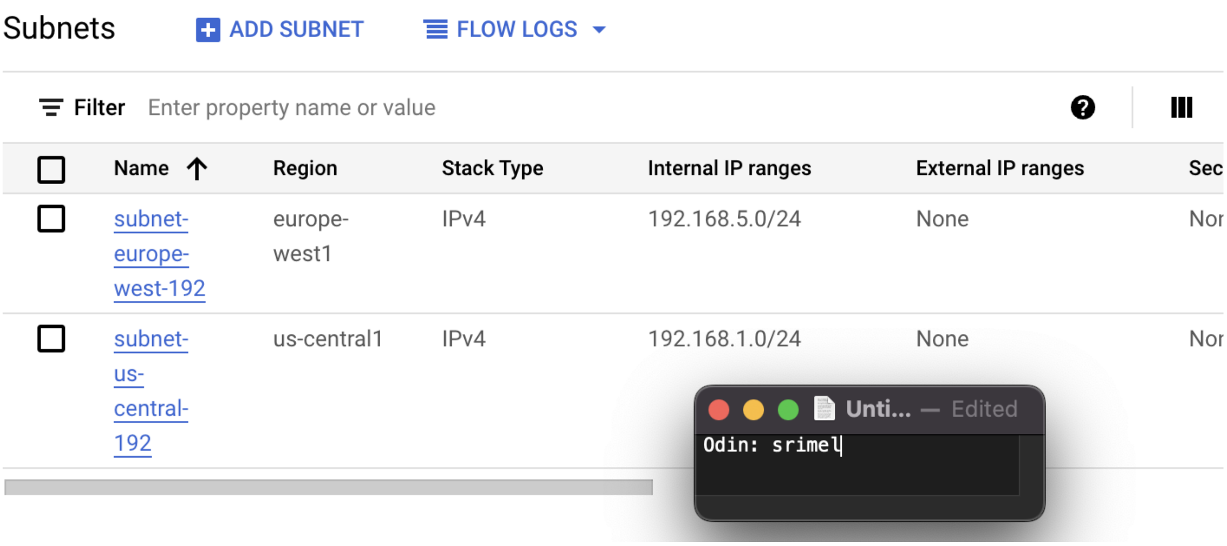
Filter Enter property name or value

□	Status	Name ↑	Zone	In use by	Internal IP	External IP	Network
□	●	course-vm	us-west1-b		10.138.0.2 (nic0)		default
□	✓	instance-1	us-west1-a		10.138.0.9 (nic0)	35.199.148.218 (nic0)	default
□	✓	instance-2	us-east1-b		10.142.0.2 (nic0)	34.139.43.222 (nic0)	default
□	✓	instance-3	us-central1-a		192.168.1.2 (nic0)	35.232.101.50 (nic0)	custom-network1
□	✓	instance-4	europe-west1-d		192.168.5.2 (nic0)	34.140.254.218 (nic0)	custom-network1

```
Odin: srimel
```

Related actions

Subnets for the custom network:



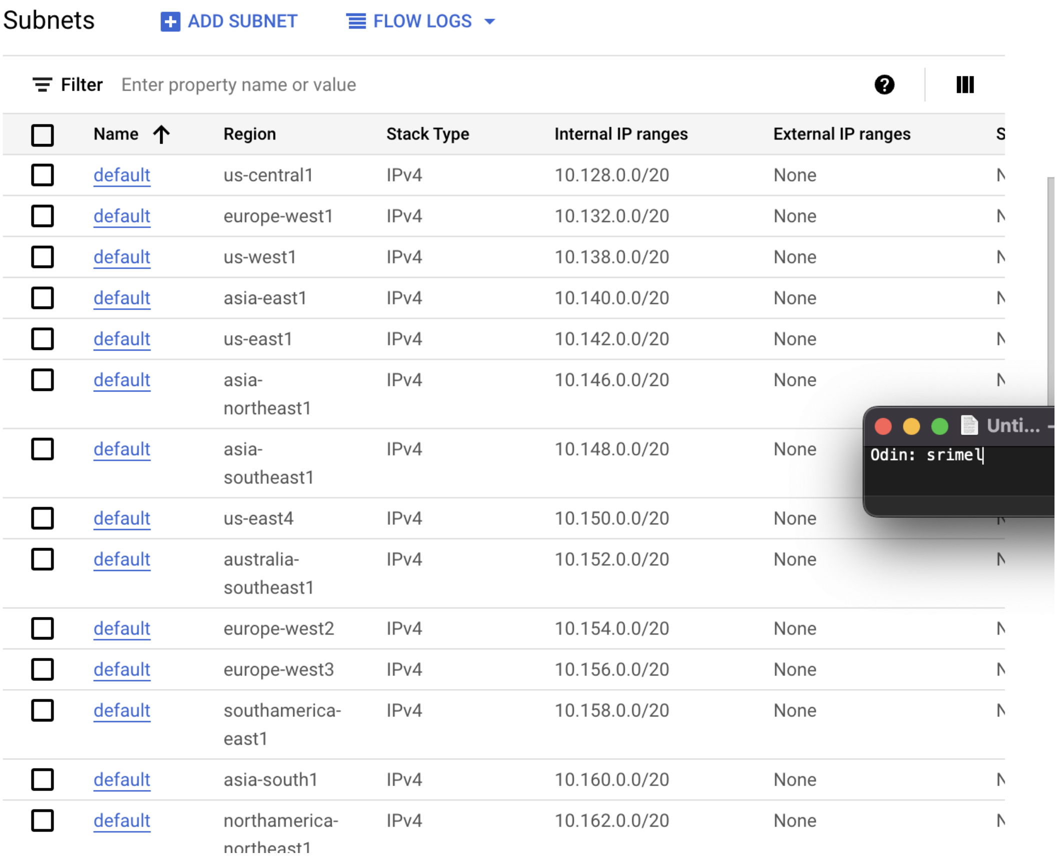
Subnets

Filter Enter property name or value

□	Name ↑	Region	Stack Type	Internal IP ranges	External IP ranges	Sec
□	subnet-europe-west-192	europe-west1	IPv4	192.168.5.0/24	None	Nor
□	subnet-us-central-192	us-central1	IPv4	192.168.1.0/24	None	Nor

```
Odin: srimel
```

Subnets for the default network:



☐	Name ↑	Region	Stack Type	Internal IP ranges	External IP ranges	S
☐	default	us-central1	IPv4	10.128.0.0/20	None	N
☐	default	europe-west1	IPv4	10.132.0.0/20	None	N
☐	default	us-west1	IPv4	10.138.0.0/20	None	N
☐	default	asia-east1	IPv4	10.140.0.0/20	None	N
☐	default	us-east1	IPv4	10.142.0.0/20	None	N
☐	default	asia-northeast1	IPv4	10.146.0.0/20	None	N
☐	default	asia-southeast1	IPv4	10.148.0.0/20	None	
☐	default	us-east4	IPv4	10.150.0.0/20	None	
☐	default	australia-southeast1	IPv4	10.152.0.0/20	None	N
☐	default	europe-west2	IPv4	10.154.0.0/20	None	N
☐	default	europe-west3	IPv4	10.156.0.0/20	None	N
☐	default	southamerica-east1	IPv4	10.158.0.0/20	None	N
☐	default	asia-south1	IPv4	10.160.0.0/20	None	N
☐	default	northamerica-northeast1	IPv4	10.162.0.0/20	None	N

```
Odin: srimel
```