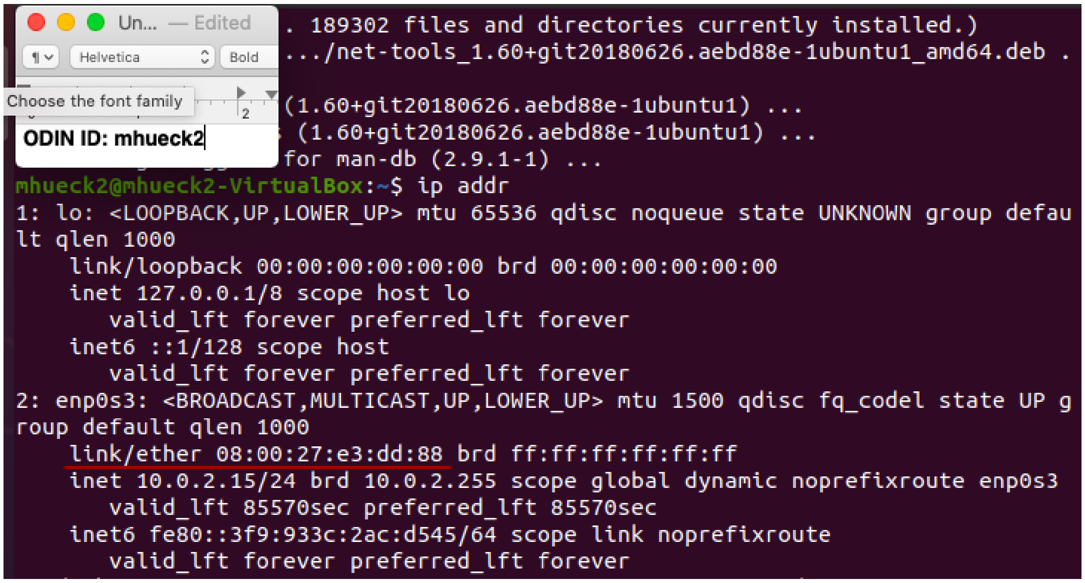
Max Huecksteadt, CS 530
Week 1, Lab 1.2

1. Use the ip command to find the IP address and hardware address of the local virtual ethernet card interface.



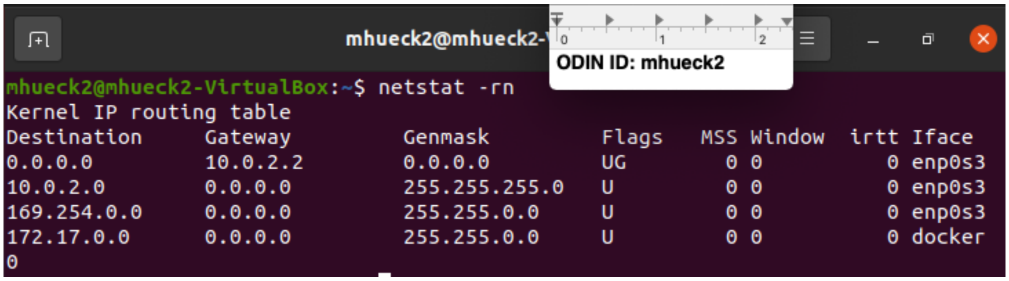
ODIN ID: mhueck2

```
. 189302 files and directories currently installed.)
.../net-tools_1.60+git20180626.aebd88e-1ubuntu1_amd64.deb .

(1.60+git20180626.aebd88e-1ubuntu1) ...
 (1.60+git20180626.aebd88e-1ubuntu1) ...
for man-db (2.9.1-1) ...
mhueck2@mhueck2-VirtualBox:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defau
lt 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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:e3:dd:88 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 85570sec preferred_lft 85570sec
    inet6 fe80::3f9:933c:2ac:d545/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

From this screenshot we can see that it is: link/ether 08:00:27:e3:dd:88

2. Perform a netstat -rn to find default router's IP address:

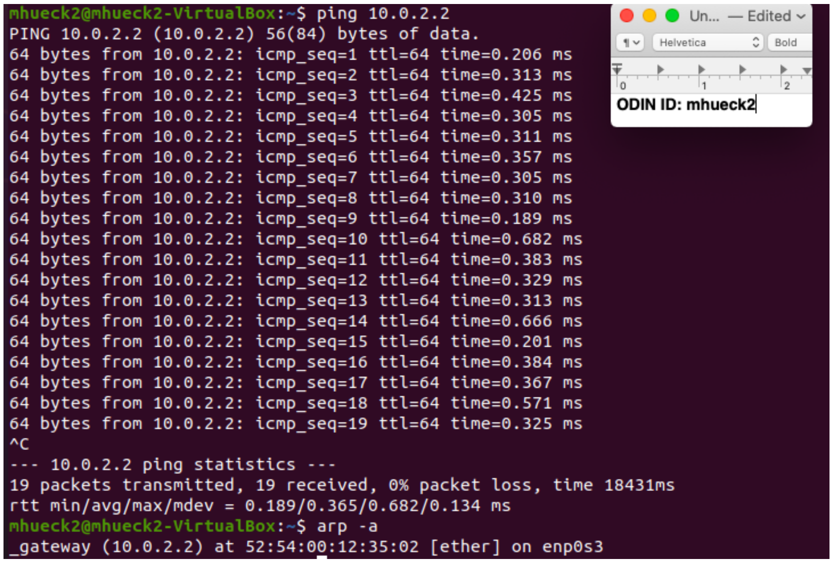


ODIN ID: mhueck2

```
mhueck2@mhueck2-VirtualBox:~$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         10.0.2.2        0.0.0.0         UG        0 0          0 enp0s3
10.0.2.0        0.0.0.0         255.255.255.0   U         0 0          0 enp0s3
169.254.0.0     0.0.0.0         255.255.0.0     U         0 0          0 enp0s3
172.17.0.0      0.0.0.0         255.255.0.0     U         0 0          0 docker
0
```

The default router's IP address is: 10.0.2.2.

3. Ping the default router and use arp to find its hardware address:



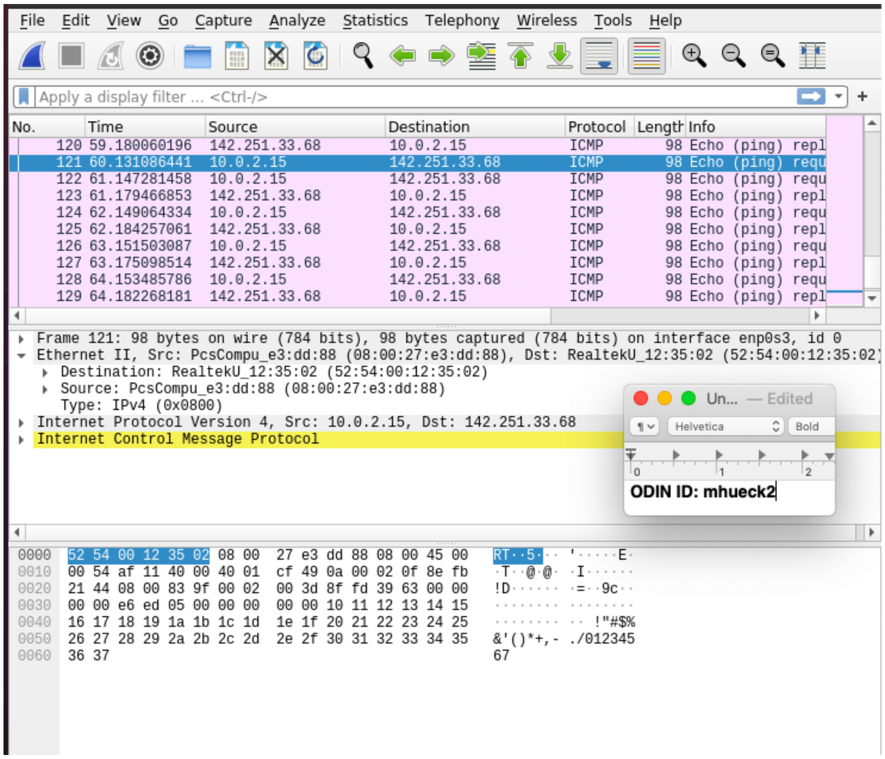
```
mhueck2@mhueck2-VirtualBox:~$ ping 10.0.2.2
PING 10.0.2.2 (10.0.2.2) 56(84) bytes of data.
64 bytes from 10.0.2.2: icmp_seq=1 ttl=64 time=0.206 ms
64 bytes from 10.0.2.2: icmp_seq=2 ttl=64 time=0.313 ms
64 bytes from 10.0.2.2: icmp_seq=3 ttl=64 time=0.425 ms
64 bytes from 10.0.2.2: icmp_seq=4 ttl=64 time=0.305 ms
64 bytes from 10.0.2.2: icmp_seq=5 ttl=64 time=0.311 ms
64 bytes from 10.0.2.2: icmp_seq=6 ttl=64 time=0.357 ms
64 bytes from 10.0.2.2: icmp_seq=7 ttl=64 time=0.305 ms
64 bytes from 10.0.2.2: icmp_seq=8 ttl=64 time=0.310 ms
64 bytes from 10.0.2.2: icmp_seq=9 ttl=64 time=0.189 ms
64 bytes from 10.0.2.2: icmp_seq=10 ttl=64 time=0.682 ms
64 bytes from 10.0.2.2: icmp_seq=11 ttl=64 time=0.383 ms
64 bytes from 10.0.2.2: icmp_seq=12 ttl=64 time=0.329 ms
64 bytes from 10.0.2.2: icmp_seq=13 ttl=64 time=0.313 ms
64 bytes from 10.0.2.2: icmp_seq=14 ttl=64 time=0.666 ms
64 bytes from 10.0.2.2: icmp_seq=15 ttl=64 time=0.201 ms
64 bytes from 10.0.2.2: icmp_seq=16 ttl=64 time=0.384 ms
64 bytes from 10.0.2.2: icmp_seq=17 ttl=64 time=0.367 ms
64 bytes from 10.0.2.2: icmp_seq=18 ttl=64 time=0.571 ms
64 bytes from 10.0.2.2: icmp_seq=19 ttl=64 time=0.325 ms
^C
--- 10.0.2.2 ping statistics ---
19 packets transmitted, 19 received, 0% packet loss, time 18431ms
rtt min/avg/max/mdev = 0.189/0.365/0.682/0.134 ms
mhueck2@mhueck2-VirtualBox:~$ arp -a
_gateway (10.0.2.2) at 52:54:00:12:35:02 [ether] on enp0s3
```

ODIN ID: mhueck2

The default router hardware address is: 52:54:00:12:35:02.

4. Which hardware manufacturer does the destination hardware address of the packet indicate? Realtek.

Request packet dump:


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

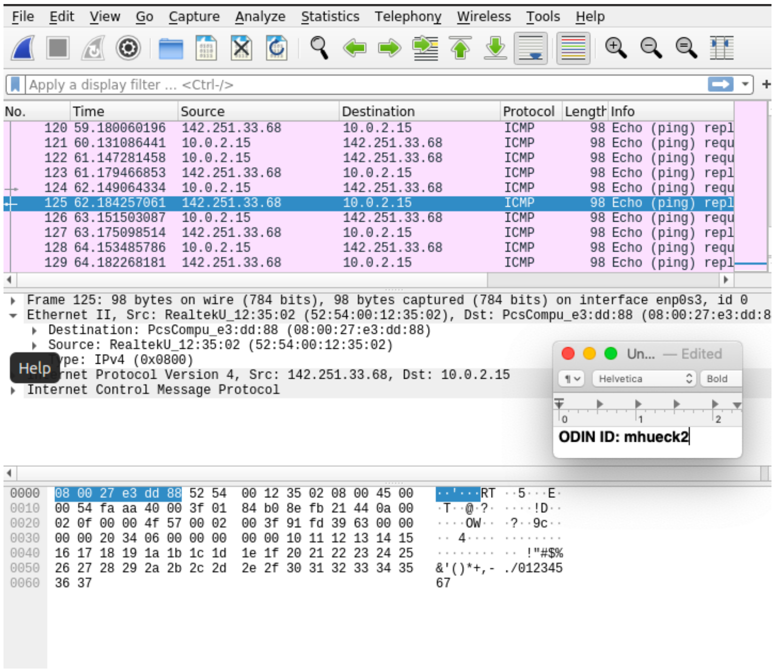
```
No.   Time          Source          Destination     Protocol Length Info
  120 59.180060196  142.251.33.68   10.0.2.15       ICMP        98 Echo (ping) repl
  121 60.131086441  10.0.2.15       142.251.33.68   ICMP        98 Echo (ping) requ
  122 61.147281458  10.0.2.15       142.251.33.68   ICMP        98 Echo (ping) requ
  123 61.179466853  142.251.33.68   10.0.2.15       ICMP        98 Echo (ping) repl
  124 62.149064334  10.0.2.15       142.251.33.68   ICMP        98 Echo (ping) requ
  125 62.184257061  142.251.33.68   10.0.2.15       ICMP        98 Echo (ping) repl
  126 63.151503087  10.0.2.15       142.251.33.68   ICMP        98 Echo (ping) requ
  127 63.175098514  142.251.33.68   10.0.2.15       ICMP        98 Echo (ping) repl
  128 64.153485786  10.0.2.15       142.251.33.68   ICMP        98 Echo (ping) requ
  129 64.182268181  142.251.33.68   10.0.2.15       ICMP        98 Echo (ping) repl
```

```
Frame 121: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface enp0s3, id 0
Ethernet II, Src: PcsCompu_e3:dd:88 (08:00:27:e3:dd:88), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
  Destination: RealtekU_12:35:02 (52:54:00:12:35:02)
  Source: PcsCompu_e3:dd:88 (08:00:27:e3:dd:88)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 142.251.33.68
Internet Control Message Protocol
```

ODIN ID: mhueck2

```
0000  52 54 00 12 35 02 08 00  27 e3 dd 88 08 00 45 00   RT··5··· '·····E·
0010  00 54 af 11 40 00 40 01  cf 49 0a 00 02 0f 8e fb   ·T··@·@· ·I······
0020  21 44 08 00 83 9f 00 02  00 3d 8f fd 39 63 00 00   !D······ ·=··9c··
0030  00 00 e6 ed 05 00 00 00  00 00 10 11 12 13 14 15   ········ ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

Reply packet dump:


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Help
Un... — Edited
¶
Helvetica
Bold
0
1
2

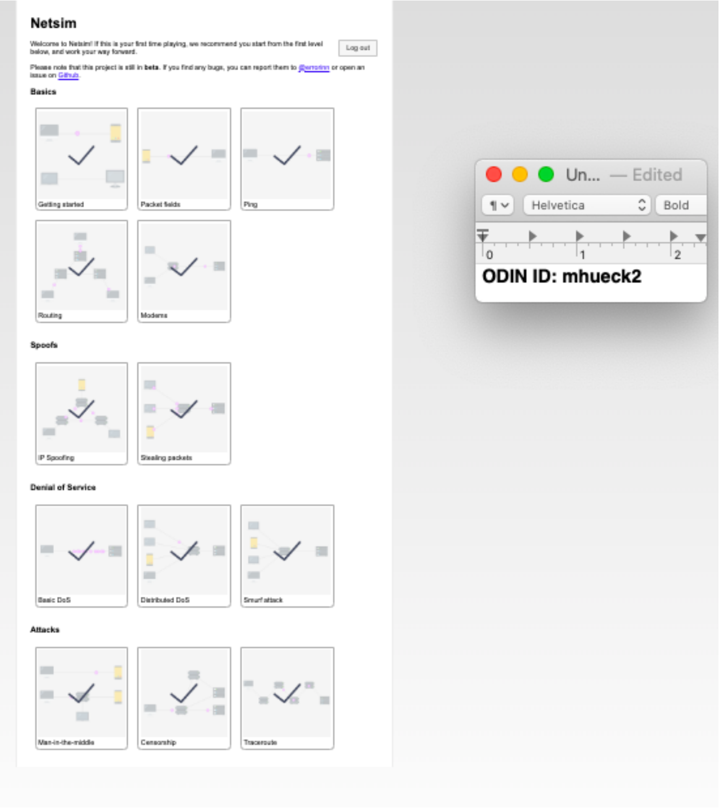
```
No.  Time           Source          Destination     Protocol Length Info
 120 59.180060196  142.251.33.68   10.0.2.15        ICMP       98 Echo (ping) repl
 121 60.131086441  10.0.2.15       142.251.33.68    ICMP       98 Echo (ping) requ
 122 61.147281458  10.0.2.15       142.251.33.68    ICMP       98 Echo (ping) requ
 123 61.179466853  142.251.33.68   10.0.2.15        ICMP       98 Echo (ping) repl
 124 62.149064334  10.0.2.15       142.251.33.68    ICMP       98 Echo (ping) requ
 125 62.184257061  142.251.33.68   10.0.2.15        ICMP       98 Echo (ping) repl
 126 63.151503087  10.0.2.15       142.251.33.68    ICMP       98 Echo (ping) requ
 127 63.175098514  142.251.33.68   10.0.2.15        ICMP       98 Echo (ping) repl
 128 64.153485786  10.0.2.15       142.251.33.68    ICMP       98 Echo (ping) requ
 129 64.182268181  142.251.33.68   10.0.2.15        ICMP       98 Echo (ping) repl
```

```
Frame 125: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface enp0s3, id 0
Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_e3:dd:88 (08:00:27:e3:dd:8
  Destination: PcsCompu_e3:dd:88 (08:00:27:e3:dd:88)
  Source: RealtekU_12:35:02 (52:54:00:12:35:02)
  Type: IPv4 (0x0800)
rnet Protocol Version 4, Src: 142.251.33.68, Dst: 10.0.2.15
Internet Control Message Protocol
```

ODIN ID: mhueck2

```
0000  08 00 27 e3 dd 88 52 54  00 12 35 02 08 00 45 00   ··'···RT ··5···E·
0010  00 54 fa aa 40 00 3f 01  84 b0 8e fb 21 44 0a 00   ·T··@·?· ····!D··
0020  02 0f 00 00 4f 57 00 02  00 3f 91 fd 39 63 00 00   ····OW·· ·?··9c··
0030  00 00 20 34 06 00 00 00  00 00 10 11 12 13 14 15   ·· 4···· ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

Netsim:



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.

Basics

Getting started

Packet fields

Ping

Routing

Modems

Spoofs

IP Spoofing

Stealing packets

Denial of Service

Basic DoS

Distributed DoS

Smurf attack

Attacks

Man-in-the-middle

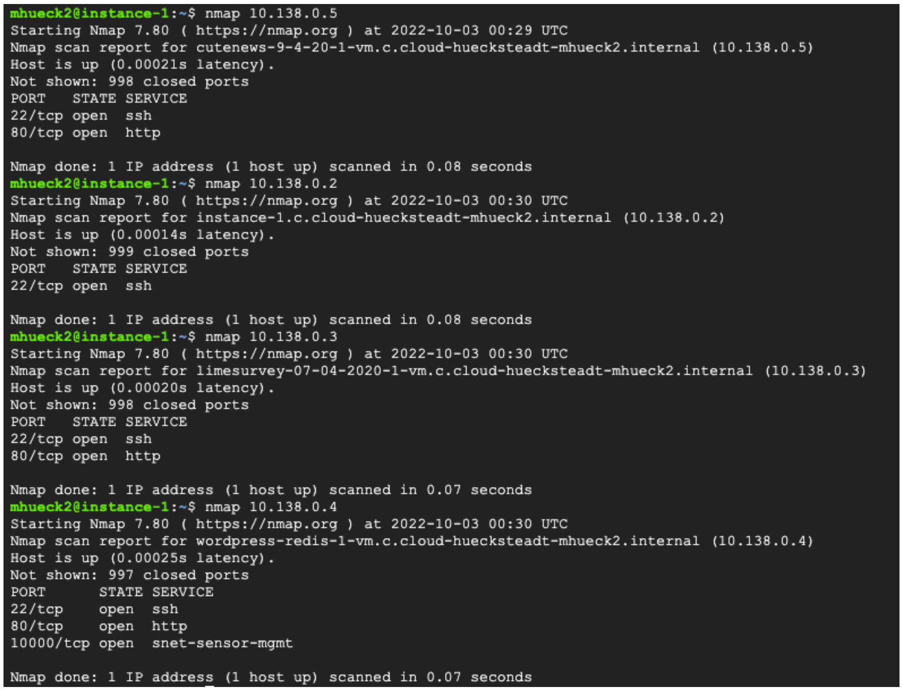
Censorship

Traceroute

ODIN ID: mhueck2

Lab 1.3:

Nmap scan:



```
mhueck2@instance-1:~$ nmap 10.138.0.5
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-03 00:29 UTC
Nmap scan report for cutenews-9-4-20-1-vm.c.cloud-huecksteadt-mhueck2.internal (10.138.0.5)
Host is up (0.00021s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
mhueck2@instance-1:~$ nmap 10.138.0.2
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-03 00:30 UTC
Nmap scan report for instance-1.c.cloud-huecksteadt-mhueck2.internal (10.138.0.2)
Host is up (0.00014s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
mhueck2@instance-1:~$ nmap 10.138.0.3
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-03 00:30 UTC
Nmap scan report for limesurvey-07-04-2020-1-vm.c.cloud-huecksteadt-mhueck2.internal (10.138.0.3)
Host is up (0.00020s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
mhueck2@instance-1:~$ nmap 10.138.0.4
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-03 00:30 UTC
Nmap scan report for wordpress-redis-1-vm.c.cloud-huecksteadt-mhueck2.internal (10.138.0.4)
Host is up (0.00025s 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: 1 IP address (1 host up) scanned in 0.07 seconds
```

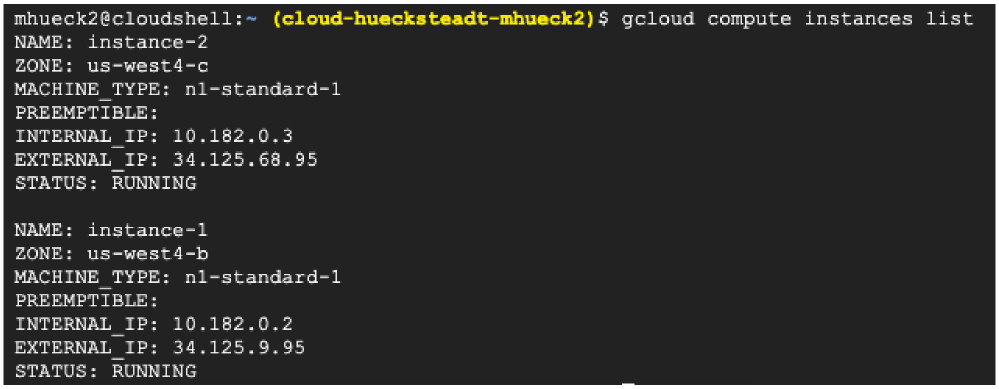
- How many subnetworks are created initially on the default network? How many regions does this correspond to? (Use a pipe to pass output to grep in order to return specific lines of output and then another to pass output to wc to count them: | grep default | wc -l)

  35 subnets, and 35 regions.

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

  4096 (prefix is 20 bits, 32 bit IP - 20 = 12, 2^12 = 4096)

Both instances in gcloud



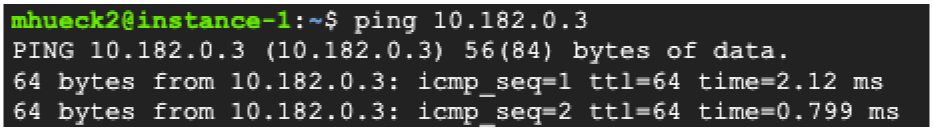
```
mhueck2@cloudshell:~ (cloud-huecksteadt-mhueck2)$ gcloud compute instances list
NAME: instance-2
ZONE: us-west4-c
MACHINE_TYPE: n1-standard-1
PREEMPTIBLE:
INTERNAL_IP: 10.182.0.3
EXTERNAL_IP: 34.125.68.95
STATUS: RUNNING

NAME: instance-1
ZONE: us-west4-b
MACHINE_TYPE: n1-standard-1
PREEMPTIBLE:
INTERNAL_IP: 10.182.0.2
EXTERNAL_IP: 34.125.9.95
STATUS: RUNNING
```

- Which CIDR subnetworks are these instances brought up in? Do they correspond to the appropriate region based on the prior commands? They are both brought up in the US-west subnet, at 10.182.0.2 and 10.182.0.3 respectively. The subnet is listed below for reference:

  NAME: default
  REGION: us-west4
  NETWORK: default
  RANGE: 10.182.0.0/20
  STACK_TYPE: IPV4_ONLY
  IPV6_ACCESS_TYPE:
  INTERNAL_IPV6_PREFIX:
  EXTERNAL_IPV6_PREFIX:

  Ping from instance 1 to instance 2:

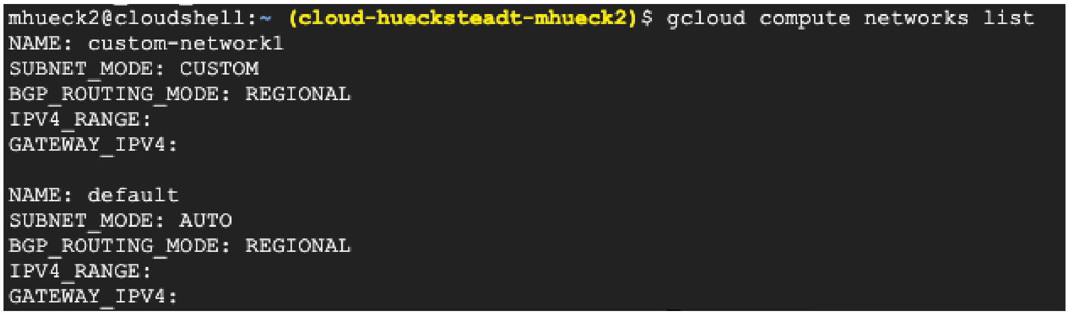


```
mhueck2@instance-1:~$ ping 10.182.0.3
PING 10.182.0.3 (10.182.0.3) 56(84) bytes of data.
64 bytes from 10.182.0.3: icmp_seq=1 ttl=64 time=2.12 ms
64 bytes from 10.182.0.3: icmp_seq=2 ttl=64 time=0.799 ms
```

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

  The virtual switch enables connectivity between the subnetworks, the VPN would enable traffic between an external destination and the gcp infrastructure. Because we are just pinging, or sending packets back and forth between subnets, the virtual switch is used.

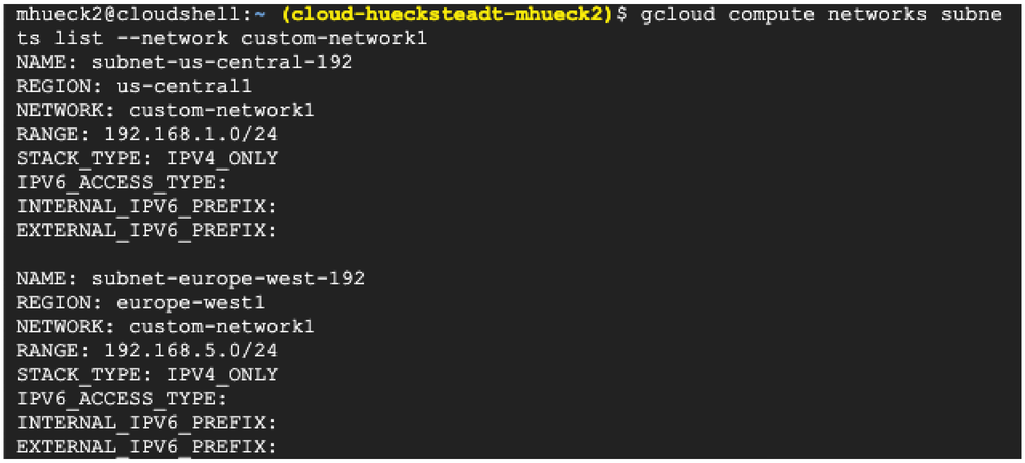
Custom and default network screenshot:



```
mhueck2@cloudshell:~ (cloud-huecksteadt-mhueck2)$ 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:
```

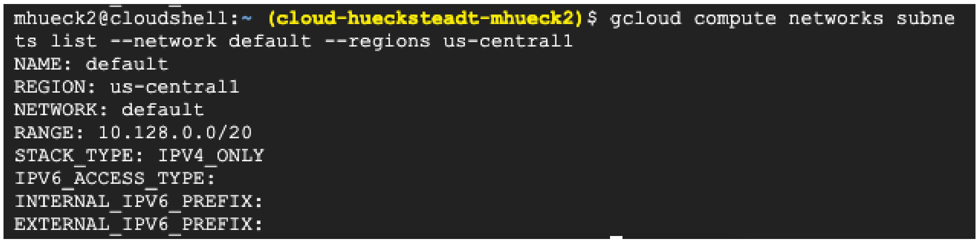
Custom network 1 Subnets:



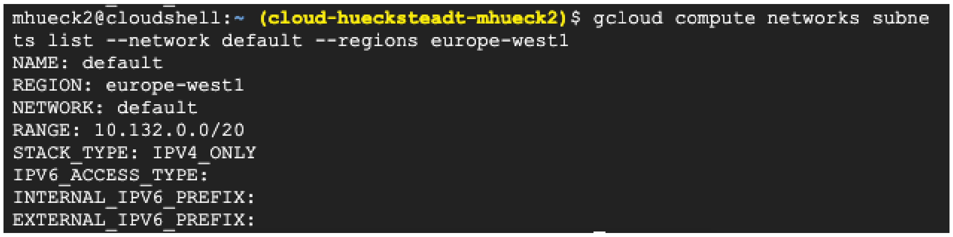
```
mhueck2@cloudshell:~ (cloud-huecksteadt-mhueck2)$ gcloud compute networks subne
ts list --network custom-network1
NAME: subnet-us-central-192
REGION: us-central1
NETWORK: custom-network1
RANGE: 192.168.1.0/24
STACK_TYPE: IPV4_ONLY
IPV6_ACCESS_TYPE:
INTERNAL_IPV6_PREFIX:
EXTERNAL_IPV6_PREFIX:

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:
```

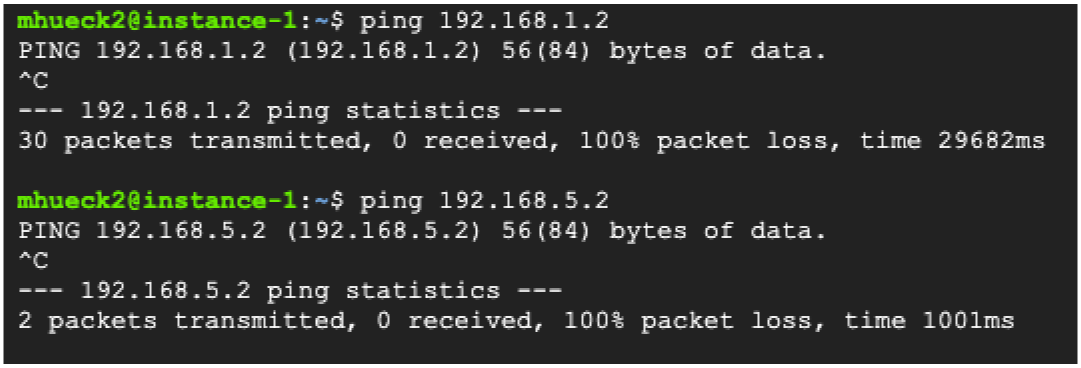
Default subnets in same regions as custom subnets:



```
mhueck2@cloudshell:~ (cloud-huecksteadt-mhueck2)$ gcloud compute networks subne
ts list --network default --regions us-central1
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:
```



```
mhueck2@cloudshell:~ (cloud-huecksteadt-mhueck2)$ gcloud compute networks subne
ts list --network default --regions 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:
```



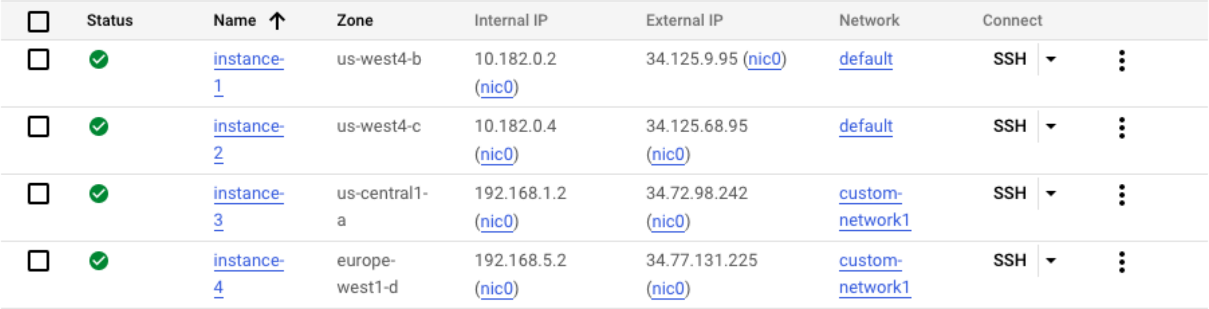
```
mhueck2@instance-1:~$ ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
^C
--- 192.168.1.2 ping statistics ---
30 packets transmitted, 0 received, 100% packet loss, time 29682ms

mhueck2@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 ---
2 packets transmitted, 0 received, 100% packet loss, time 1001ms
```

- Explain why the result is different from instance-2.

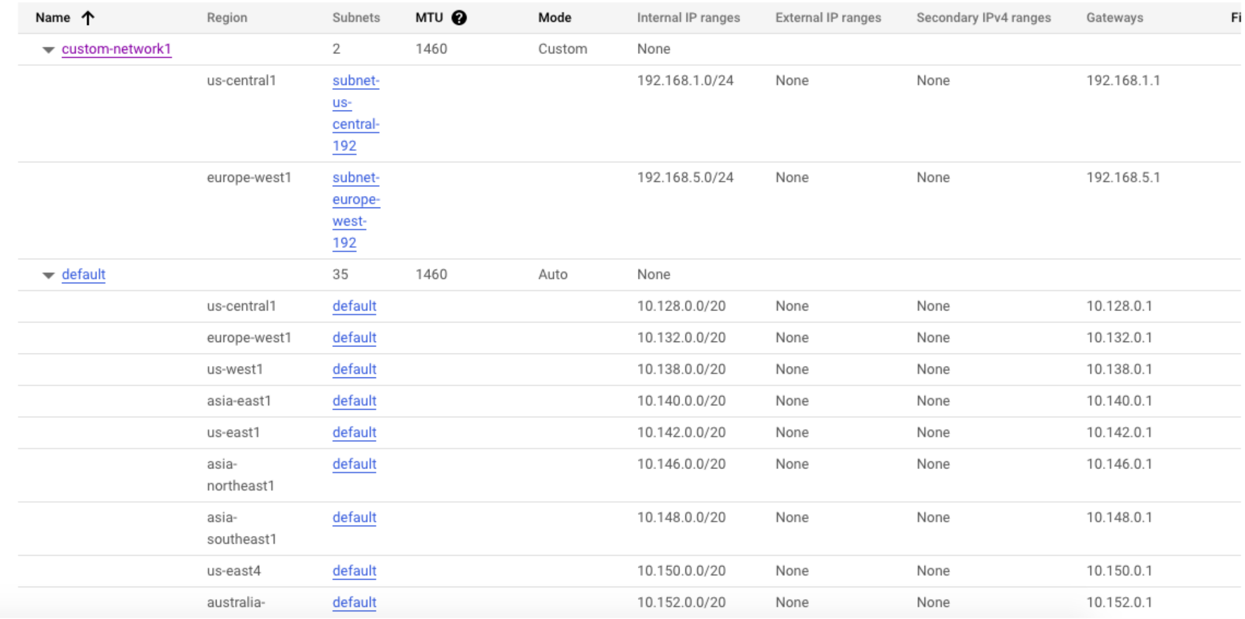
  We are trying to communicate with two separate networks, across the networks, not within them. We haven't enabled or configured anything to do this yet.

  GCP instances:



☐	Status	Name ↑	Zone	Internal IP	External IP	Network	Connect	
☐	✓	instance-1	us-west4-b	10.182.0.2 (nic0)	34.125.9.95 (nic0)	default	SSH ▾	⋮
☐	✓	instance-2	us-west4-c	10.182.0.4 (nic0)	34.125.68.95 (nic0)	default	SSH ▾	⋮
☐	✓	instance-3	us-central1-a	192.168.1.2 (nic0)	34.72.98.242 (nic0)	custom-network1	SSH ▾	⋮
☐	✓	instance-4	europe-west1-d	192.168.5.2 (nic0)	34.77.131.225 (nic0)	custom-network1	SSH ▾	⋮

Subnets:



Name ↑	Region	Subnets	MTU ?	Mode	Internal IP ranges	External IP ranges	Secondary IPv4 ranges	Gateways	Fi
▾ custom-network1		2	1460	Custom	None				
	us-central1	subnet-us-central-192			192.168.1.0/24	None	None	192.168.1.1	
	europe-west1	subnet-europe-west-192			192.168.5.0/24	None	None	192.168.5.1	
▾ default		35	1460	Auto	None				
	us-central1	default			10.128.0.0/20	None	None	10.128.0.1	
	europe-west1	default			10.132.0.0/20	None	None	10.132.0.1	
	us-west1	default			10.138.0.0/20	None	None	10.138.0.1	
	asia-east1	default			10.140.0.0/20	None	None	10.140.0.1	
	us-east1	default			10.142.0.0/20	None	None	10.142.0.1	
	asia-northeast1	default			10.146.0.0/20	None	None	10.146.0.1	
	asia-southeast1	default			10.148.0.0/20	None	None	10.148.0.1	
	us-east4	default			10.150.0.0/20	None	None	10.150.0.1	
	australia-	default			10.152.0.0/20	None	None	10.152.0.1	