1.2 ARP, Wireshark, Netsim

1.2.1 ARP (linux.cs.pdx.edu)

IPv4 Address

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
```

Hardware Address of local ethernet interface

```
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    altname enp0s3
    inet 131.252.208.103/24 metric 100 brd 131.252.208.255 scope global dynamic ens3
       valid_lft 9243sec preferred_lft 9243sec
```

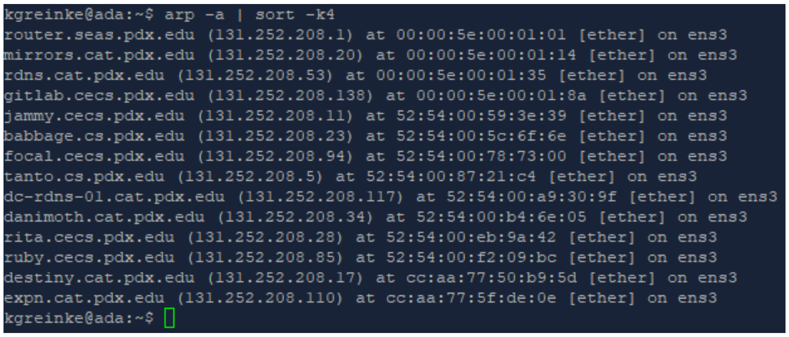
What is the default router's IP address (e.g. the gateway address for the default route 0.0.0.0/0)?
131.252.208.1

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?
14

List any IP addresses share the same hardware address
Actually none.

How many less hardware addresses are there than Ip addresses in the ARP table?
There is an equal amount of each.



```
kgreinke@ada:~$ arp -a | sort -k4
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
rdns.cat.pdx.edu (131.252.208.53) at 00:00:5e:00:01:35 [ether] on ens3
gitlab.cecs.pdx.edu (131.252.208.138) at 00:00:5e:00:01:8a [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
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
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
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
kgreinke@ada:~$ 
```

Include the command in your lab notebook

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

What network prefix do most of the IP addresses in the ARP table share?
Shared Prefix: 131

1.2.3 ARP (Cloud)

IP Address and Hardware Address of the local ethernet card interface:

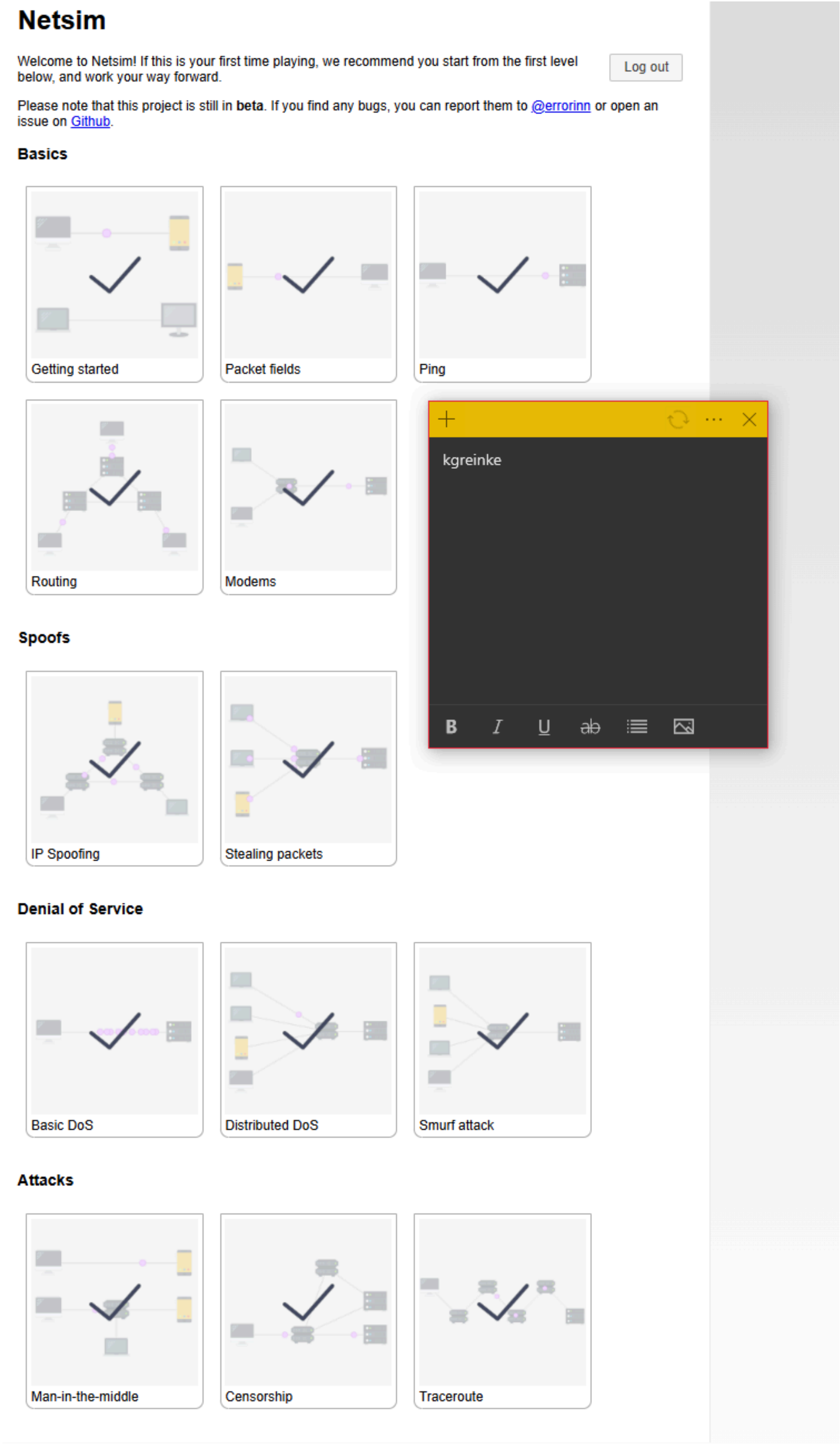
```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1460 qdisc mq state UP group
default qlen 1000
    link/ether 42:01:0a:8a:00:04 brd ff:ff:ff:ff:ff:ff
    inet 10.138.0.4/32 metric 100 scope global dynamic ens4
       valid_lft 86014sec preferred_lft 86014sec
    inet6 fe80::4001:aff:fe8a:4/64 scope link
       valid_lft forever preferred_lft forever
```

What is the default router's IP address?
10.138.0.1

```
arp 10.138.0.1
```

What is the default router's hardware address?
42:01:0a:8a:00:01

1.2.4 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

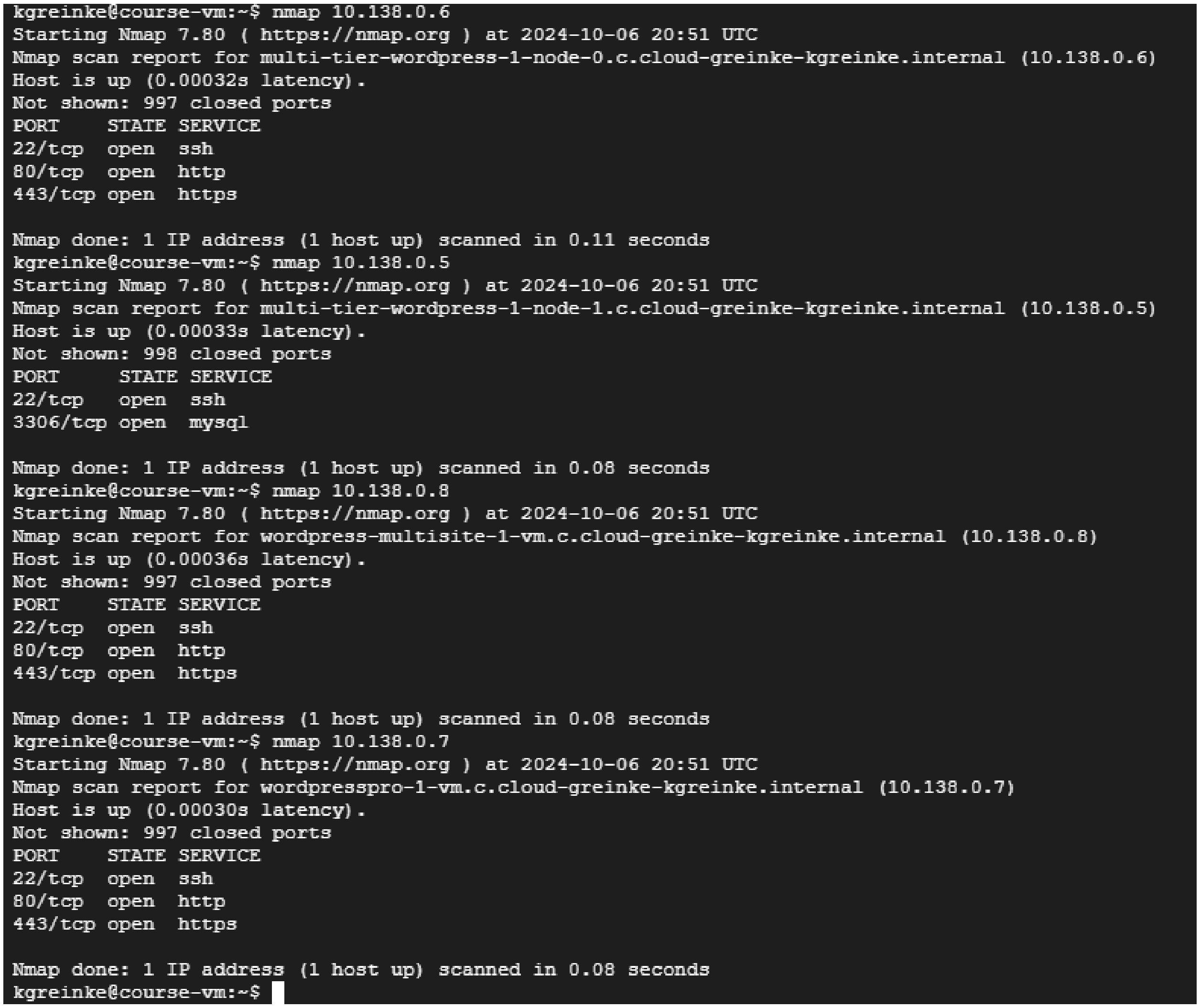
- Basic DoS ✓
- Distributed DoS ✓
- Smurf attack ✓

Attacks

- Man-in-the-middle ✓
- Censorship ✓
- Traceroute ✓

kgreinke

1.3 Cloud Networking



```
kgreinke@course-vm:~$ nmap 10.138.0.6
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-06 20:51 UTC
Nmap scan report for multi-tier-wordpress-1-node-0.c.cloud-greinke-kgreinke.internal (10.138.0.6)
Host is up (0.00032s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
kgreinke@course-vm:~$ nmap 10.138.0.5
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-06 20:51 UTC
Nmap scan report for multi-tier-wordpress-1-node-1.c.cloud-greinke-kgreinke.internal (10.138.0.5)
Host is up (0.00033s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
kgreinke@course-vm:~$ nmap 10.138.0.8
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-06 20:51 UTC
Nmap scan report for wordpress-multisite-1-vm.c.cloud-greinke-kgreinke.internal (10.138.0.8)
Host is up (0.00036s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
kgreinke@course-vm:~$ nmap 10.138.0.7
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-06 20:51 UTC
Nmap scan report for wordpresspro-1-vm.c.cloud-greinke-kgreinke.internal (10.138.0.7)
Host is up (0.00030s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
kgreinke@course-vm:~$
```

1.3.5 Navigating Default Networks

Answer the following questions in your lab notebook:

> How many subnetworks are created initially on the default network? How many regions does this correspond to?
> 84
> 42
>
> Given the CIDR prefix associated with each subnetwork, how many hosts does each subnetwork support?
> 20

Which CIDR subnetworks are these instances brought up in? Do they correspond to the appropriate region based on the prior commands?
Instance-1:

> us-central1-a
> 10.128.0.2

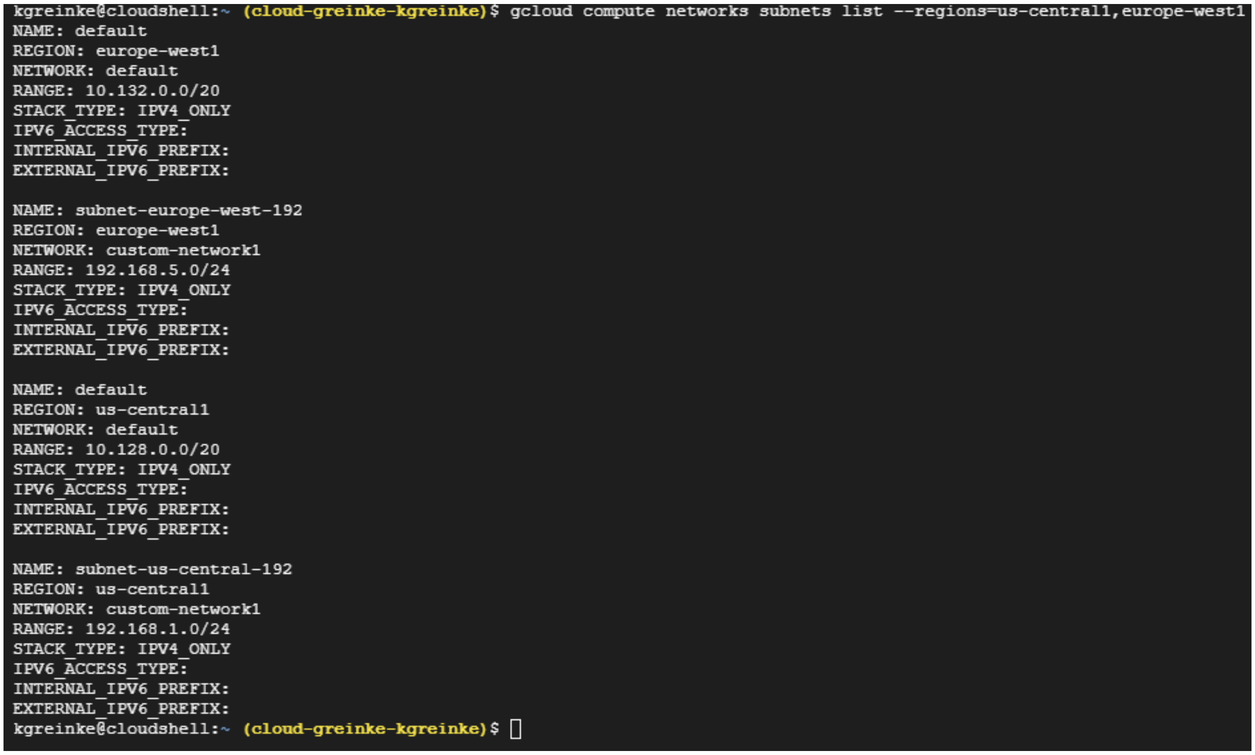
Instance-2:

> us-east1-c
> 10.142.0.2

They do match up.

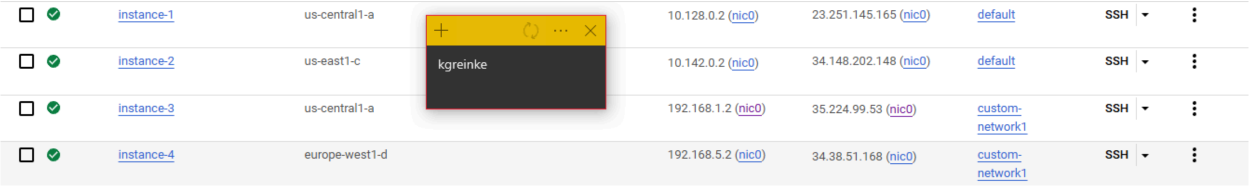
From the figure in the previous step. What facilitates this connectivity: the virtual switch or the VPN Gateway?
Virtual Switch

1.3.6 Creating Custom Networks

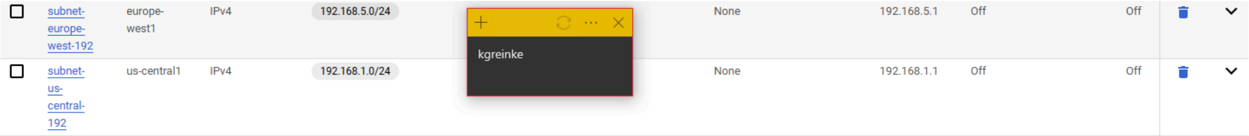


```
kgreinke@cloudshell:~ (cloud-greinke-kgreinke)$ gcloud compute networks subnets list --regions=us-central1,europe-west1
NAME: default
REGION: europe-west1
NETWORK: default
RANGE: 10.132.0.0/20
STACK_TYPE: IPV4_ONLY
IPV6_ACCESS_TYPE:
INTERNAL_IPV6_PREFIX:
EXTERNAL_IPV6_PREFIX:

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:
kgreinke@cloudshell:~ (cloud-greinke-kgreinke)$ 
```

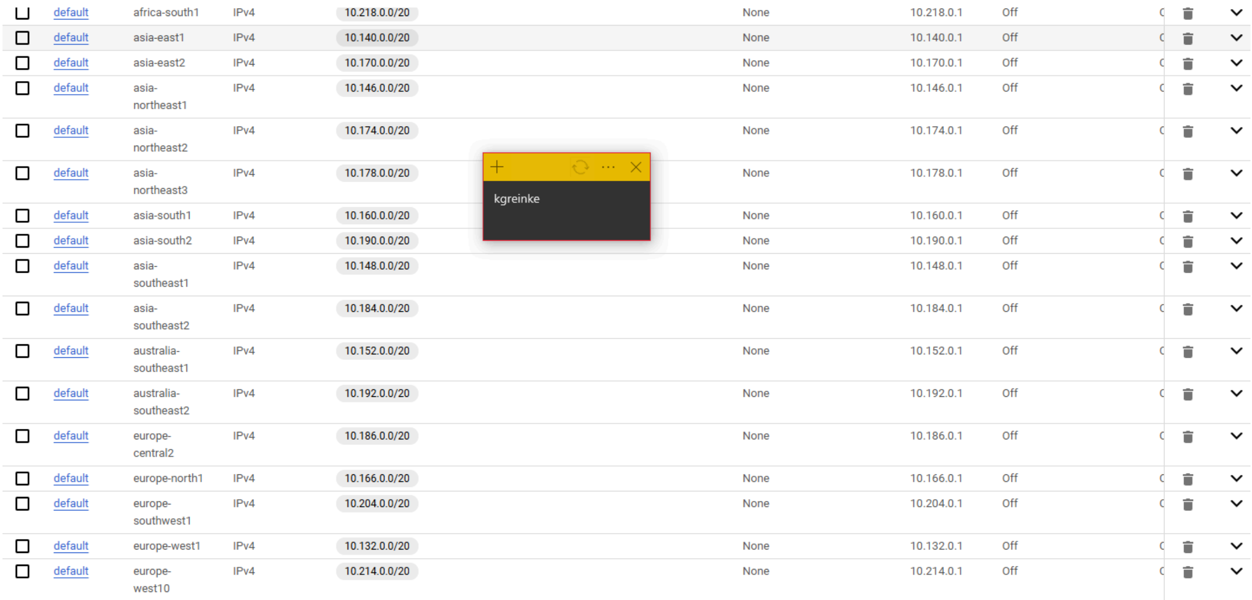
Explain why the result of this ping is different from when you performed the ping to instance-2.
Not sure. Maybe it is because they are a subnet??



☐	✓	instance-1	us-central1-a	10.128.0.2 (nic0)	23.251.145.165 (nic0)	default	SSH ▾	⋮
☐	✓	instance-2	us-east1-c	10.142.0.2 (nic0)	34.148.202.148 (nic0)	default	SSH ▾	⋮
☐	✓	instance-3	us-central1-a	192.168.1.2 (nic0)	35.224.99.53 (nic0)	custom-network1	SSH ▾	⋮
☐	✓	instance-4	europe-west1-d	192.168.5.2 (nic0)	34.38.51.168 (nic0)	custom-network1	SSH ▾	⋮



☐	subnet-europe-west-192	europe-west1	IPv4	192.168.5.0/24	None	192.168.5.1	Off	Off	🗑 ⌄
☐	subnet-us-central-192	us-central1	IPv4	192.168.1.0/24	None	192.168.1.1	Off	Off	🗑 ⌄



☐	default	africa-south1	IPv4	10.218.0.0/20	None	10.218.0.1	Off	C
☐	default	asia-east1	IPv4	10.140.0.0/20	None	10.140.0.1	Off	C
☐	default	asia-east2	IPv4	10.170.0.0/20	None	10.170.0.1	Off	C
☐	default	asia-northeast1	IPv4	10.146.0.0/20	None	10.146.0.1	Off	C
☐	default	asia-northeast2	IPv4	10.174.0.0/20	None	10.174.0.1	Off	C
☐	default	asia-northeast3	IPv4	10.178.0.0/20	None	10.178.0.1	Off	C
☐	default	asia-south1	IPv4	10.160.0.0/20	None	10.160.0.1	Off	C
☐	default	asia-south2	IPv4	10.190.0.0/20	None	10.190.0.1	Off	C
☐	default	asia-southeast1	IPv4	10.148.0.0/20	None	10.148.0.1	Off	C
☐	default	asia-southeast2	IPv4	10.184.0.0/20	None	10.184.0.1	Off	C
☐	default	australia-southeast1	IPv4	10.152.0.0/20	None	10.152.0.1	Off	C
☐	default	australia-southeast2	IPv4	10.192.0.0/20	None	10.192.0.1	Off	C
☐	default	europe-central2	IPv4	10.186.0.0/20	None	10.186.0.1	Off	C
☐	default	europe-north1	IPv4	10.166.0.0/20	None	10.166.0.1	Off	C
☐	default	europe-southwest1	IPv4	10.204.0.0/20	None	10.204.0.1	Off	C
☐	default	europe-west1	IPv4	10.132.0.0/20	None	10.132.0.1	Off	C
☐	default	europe-west10	IPv4	10.214.0.0/20	None	10.214.0.1	Off	C

kgreinke