

Lab notebook Week 1

Submitted by: Vishrut Sharma (OdinID: vishrut)

Table of Contents

01.2: ARP, Wireshark, Netsim

1. ARP #1

2. Netsim #2

01.3: Cloud networking

4. Scan targets for services

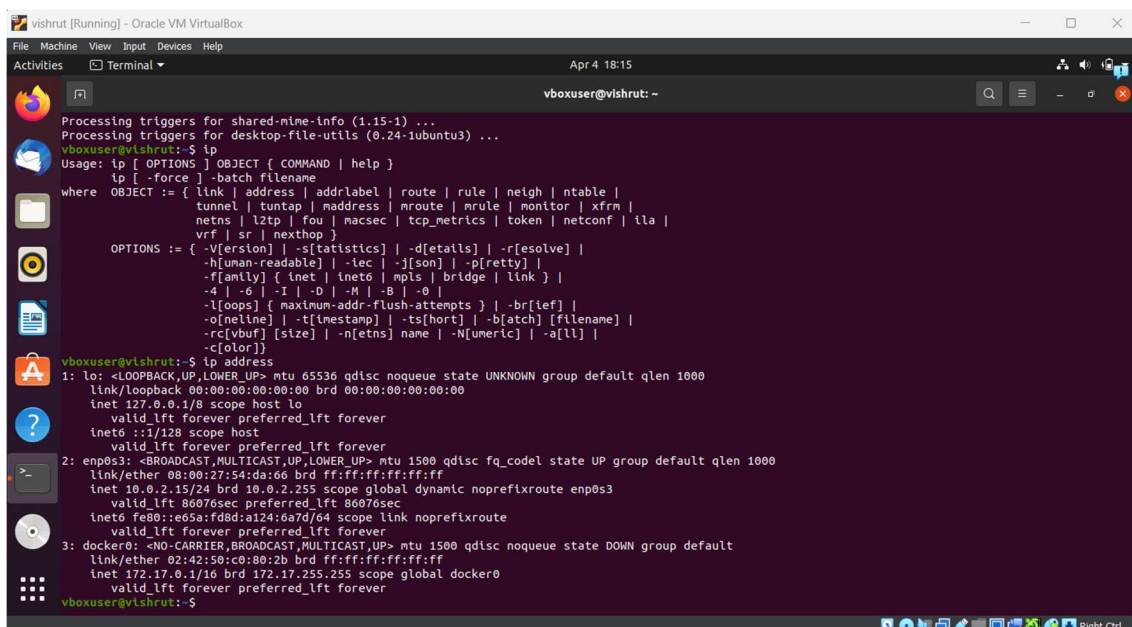
6. Navigating default networks

7. Creating custom networks

01.2: ARP, Wireshark, Netsim

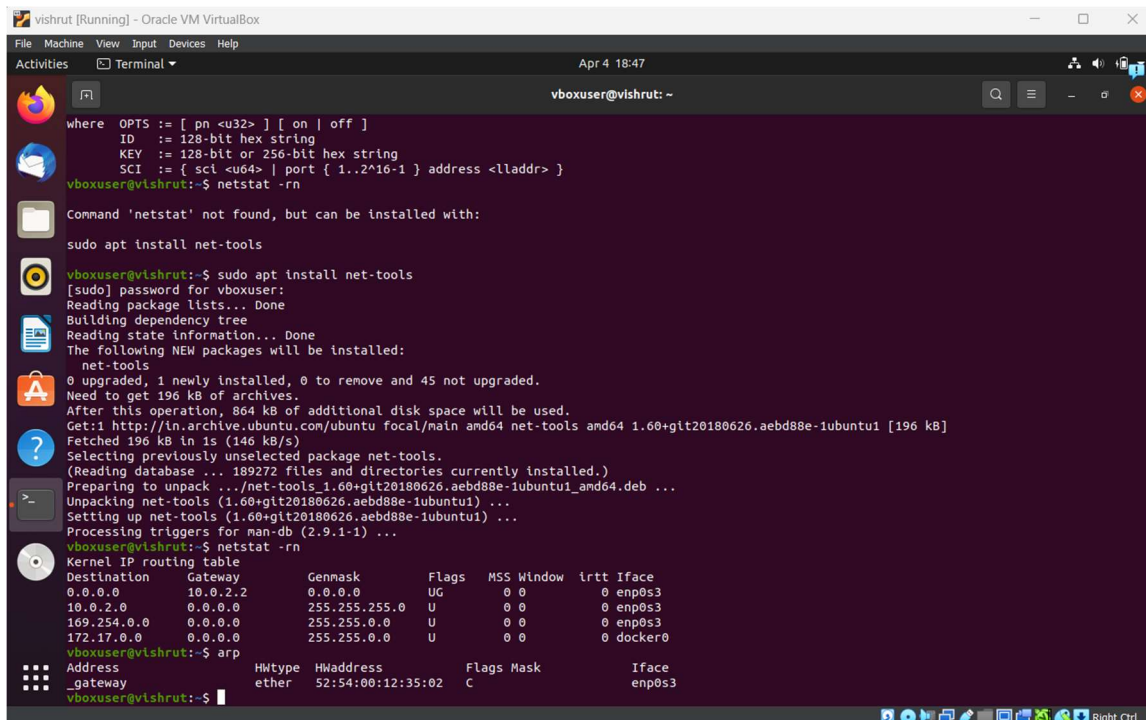
1. ARP #1

1) The screenshot below contains the results from the ip command.



```
vishrut [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Apr 4 18:15
vboxuser@vishrut: ~
Processing triggers for shared-mime-info (1.15-1) ...
Processing triggers for desktop-file-utils (0.24-1ubuntu3) ...
vboxuser@vishrut:~$ ip
Usage: ip [ OPTIONS ] OBJECT { COMMAND | help }
       ip [ -force ] -batch filename
where OBJECT := { link | address | addrlabel | route | rule | neigh | ntable |
                  tunnel | tuntap | maddress | mroute | mrule | monitor | xfrm |
                  netns | l2tp | fou | macsec | tcp_metrics | token | netconf | ila |
                  vrf | sr | nexthop }
OPTIONS := { -V[ersion] | -s[tatistics] | -d[etails] | -r[esolve] |
              -h[uman-readable] | -t[ec] | -j[son] | -p[retty] |
              -f[amily] { inet | inet6 | npls | bridge | link } |
              -4 | -6 | -I | -O | -M | -B | -O |
              -l[oops] { maxnum-addr-flush-attempts } | -b[rief] |
              -o[neline] | -t[imestamp] | -ts[hort] | -b[atch] [filename] |
              -rc[vbuf] [size] | -n[etns] name | -N[umeric] | -a[ll] |
              -c[olor]}
vboxuser@vishrut:~$ 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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 08:00:27:54:da:66 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 86076sec preferred_lft 86076sec
   inet6 fe80::e08a:fd0d:a124:6a7d/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
   link/ether 02:42:50:c0:80:2b 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
vboxuser@vishrut:~$
```

The screenshot below contains the results from the following commands: netstat -rn, arp.

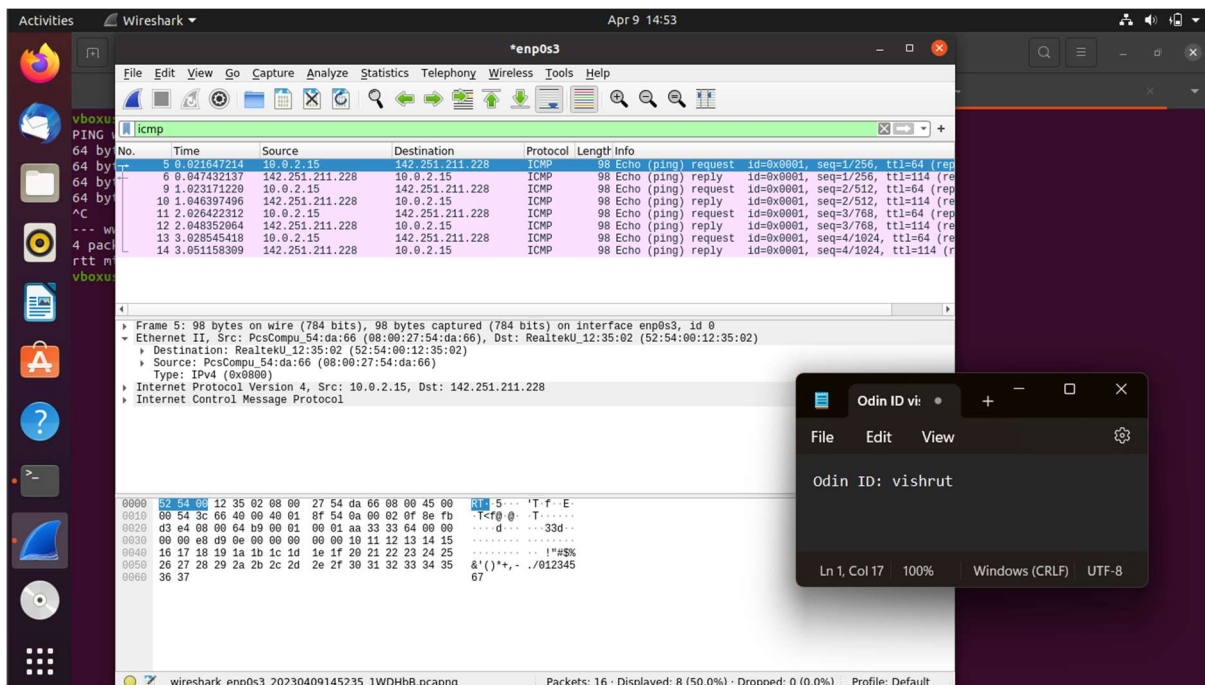


The screenshot shows a terminal window titled "vishrut [Running] - Oracle VM VirtualBox". The user is logged in as "vboxuser@vishrut: ~". The terminal output shows the following commands and their results:

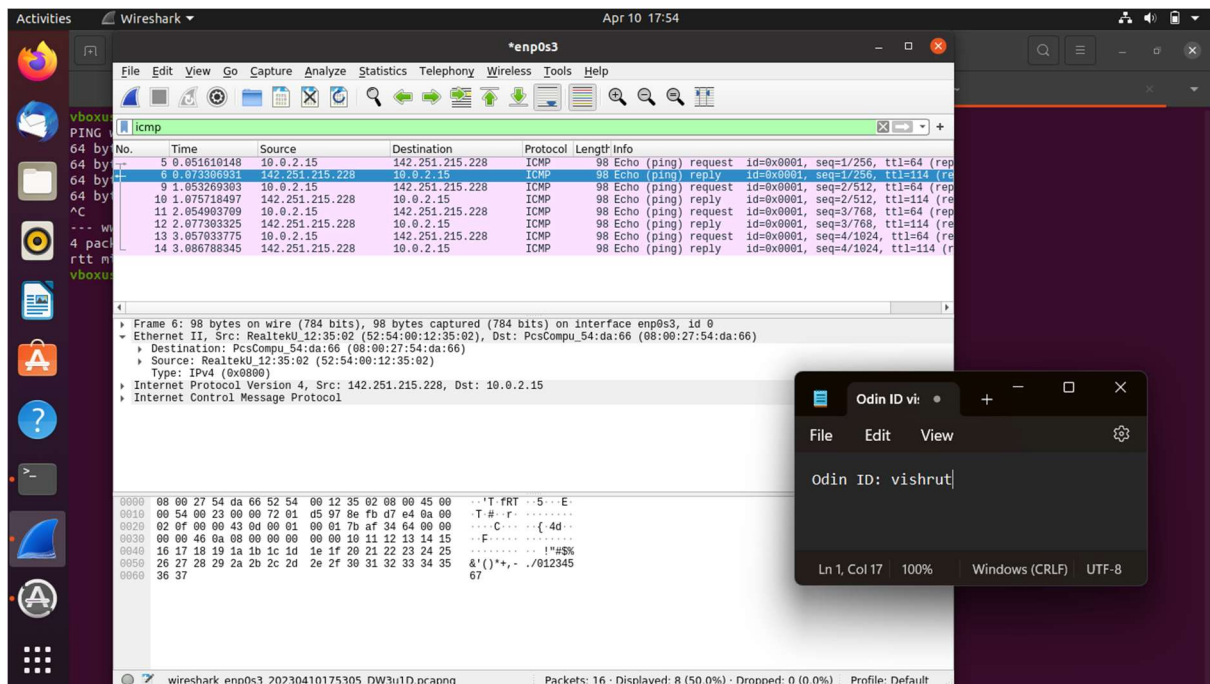
```
where OPTS := [ pn <u32> ] [ on | off ]
ID := 128-bit hex string
KEY := 128-bit or 256-bit hex string
SCI := { scl <u64> | port { 1..2^16-1 } address <lladdr> }
vboxuser@vishrut:~$ netstat -rn
Command 'netstat' not found, but can be installed with:
sudo apt install net-tools
vboxuser@vishrut:~$ sudo apt install net-tools
[sudo] password for vboxuser:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
net-tools
0 upgraded, 1 newly installed, 0 to remove and 45 not upgraded.
Need to get 196 kB of archives.
After this operation, 864 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu focal/main amd64 net-tools amd64 1.60+git20180626.aebd88e-1ubuntu1 [196 kB]
Fetched 196 kB in 1s (146 kB/s)
Selecting previously unselected package net-tools.
(Reading database ... 189272 files and directories currently installed.)
Preparing to unpack .../net-tools 1.60+git20180626.aebd88e-1ubuntu1_amd64.deb ...
Unpacking net-tools (1.60+git20180626.aebd88e-1ubuntu1) ...
Setting up net-tools (1.60+git20180626.aebd88e-1ubuntu1) ...
Processing triggers for man-db (2.9.1-1) ...
vboxuser@vishrut:~$ 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 docker0

vboxuser@vishrut:~$ arp
Address          HWtype  HWaddress      Flags Mask    Iface
_gateway        ether    52:54:00:12:35:02  C          enp0s3
vboxuser@vishrut:~$
```

2) The hardware manufacturer indicated by the destination hardware address of the packet is RealtekU as seen in the screenshot below. The packet dump section is also shown in the screenshot below. This is for the request packet.



The screenshot below is for the response packet.



2. Netsim #2

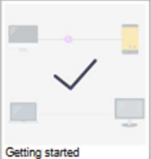
The screenshot below contains the completed list of levels of netsim.

Netsim

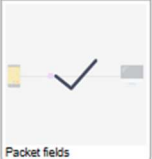
Welcome to Netsim! If this is your first time playing, we recommend you start from the first level below, and work your way forward. [Log out](#)

Please note that this project is still in **beta**. If you find any bugs, you can report them to [@errorim](#) or open an issue on [Github](#).


Basics




Getting started



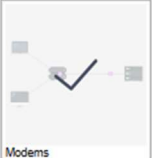
Packet fields



Ping

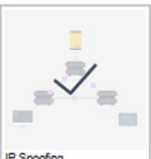


Routing

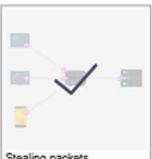


Modems

Spoofs




IP Spoofing




Stealing packets


Denial of Service



Basic DoS




Distributed DoS




Smurf attack


Attacks



Man-in-the-middle



Censorship



Traceroute

Odin ID vi: • + - □ ×

File Edit View ⚙

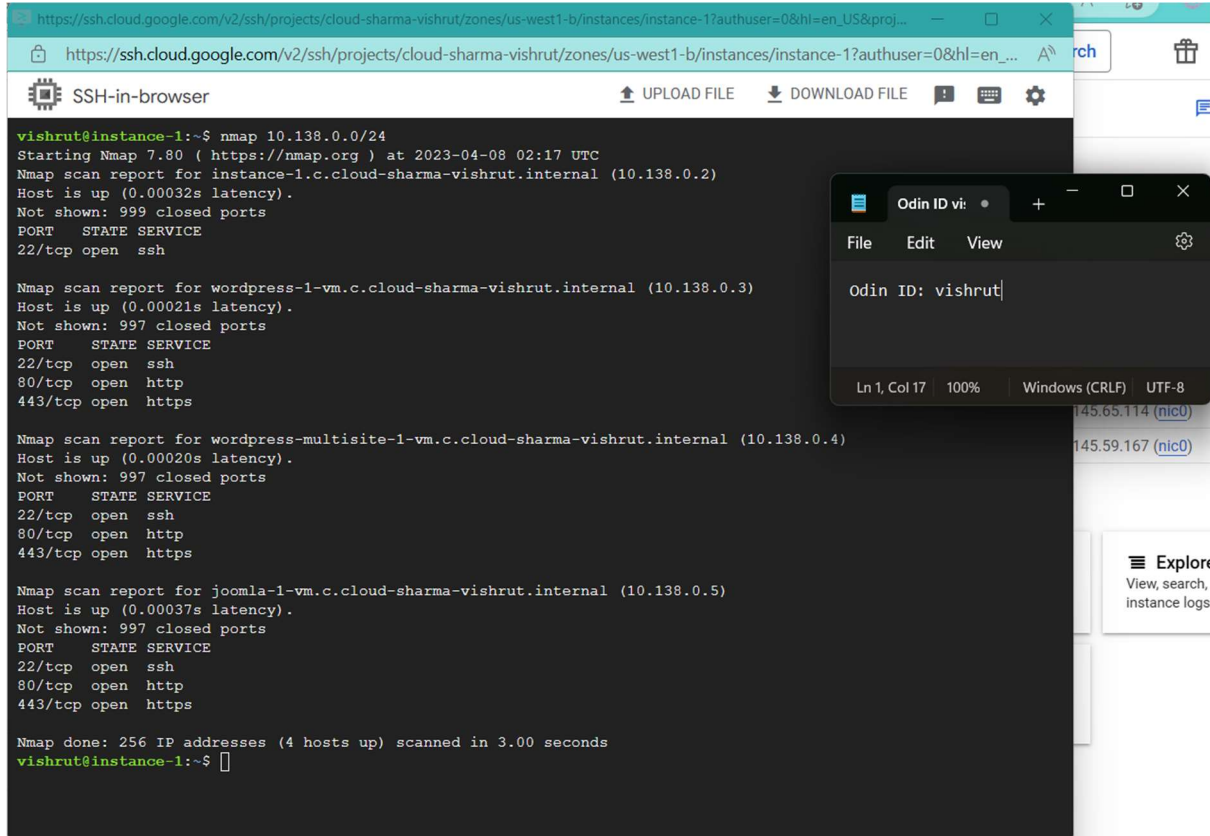
Odin ID: vishrut

Ln 1, Col 10 | 100% | Windows (CRLF) | UTF-8

01.3: Cloud networking

4. Scan targets for services

The screenshot below contains the output from the nmap command.



```
vishrut@instance-1:~$ nmap 10.138.0.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-08 02:17 UTC
Nmap scan report for instance-1.c.cloud-sharma-vishrut.internal (10.138.0.2)
Host is up (0.00032s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap scan report for wordpress-1-vm.c.cloud-sharma-vishrut.internal (10.138.0.3)
Host is up (0.00021s 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 wordpress-multisite-1-vm.c.cloud-sharma-vishrut.internal (10.138.0.4)
Host is up (0.00020s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https

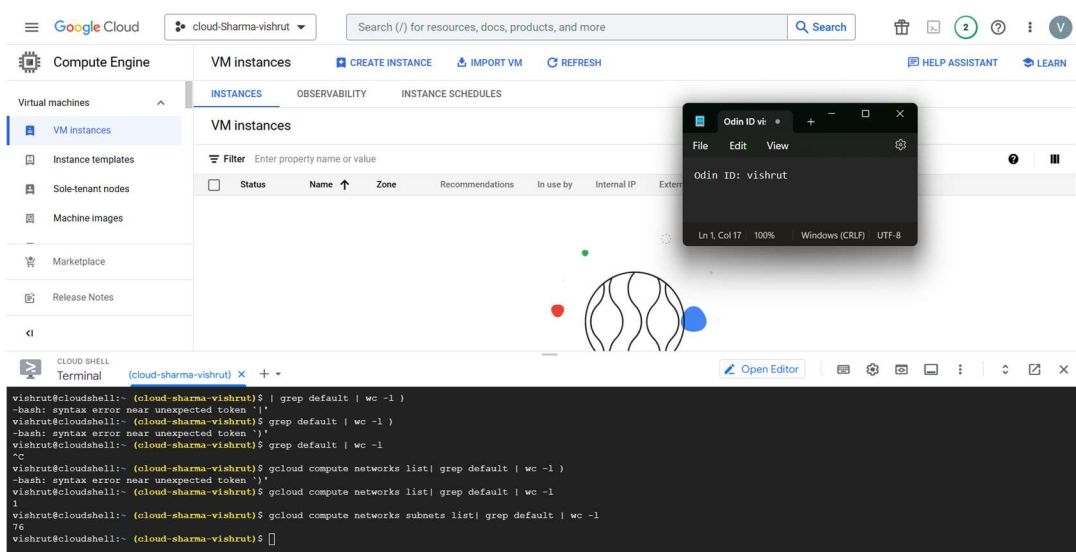
Nmap scan report for joomla-1-vm.c.cloud-sharma-vishrut.internal (10.138.0.5)
Host is up (0.00037s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https

Nmap done: 256 IP addresses (4 hosts up) scanned in 3.00 seconds
vishrut@instance-1:~$
```

Odin ID vishrut

6. Navigating default networks

1) The screenshot below shows the number of subnetworks. As seen in the image below 76 subnets were created and they correspond to 76 regions.



```
vishrut@cloudshell:~ (cloud-sharma-vishrut) $ gcloud compute networks list | grep default | wc -l
1
vishrut@cloudshell:~ (cloud-sharma-vishrut) $ gcloud compute networks subnets list | grep default | wc -l
76
vishrut@cloudshell:~ (cloud-sharma-vishrut) $
```

Odin ID vishrut

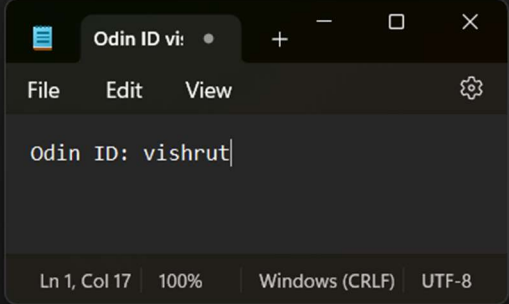
2) Given the CIDR prefix, each subnetwork supports 4094 hosts.

$$2^{(32 - 20)} - 2 = 4094 \text{ hosts}$$

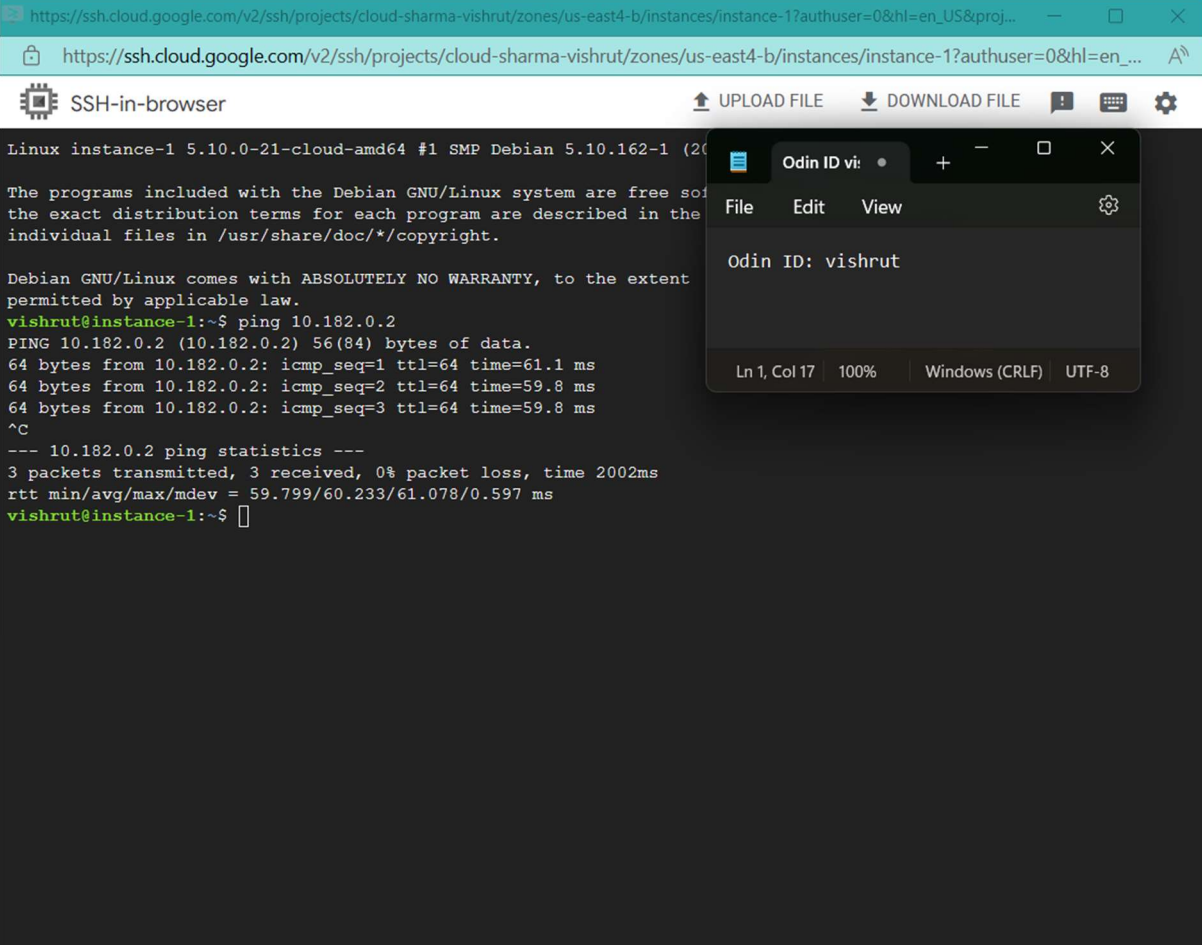
3) The newly created instances are brought up in 10.182.0.0/20. And, yes it corresponds to the appropriate region based on the prior commands.

```
vishrut@cloudshell:~ (cloud-sharma-vishrut)$ gcloud compute instances list
NAME: instance-1
ZONE: us-east4-b
MACHINE_TYPE: n1-standard-1
PREEMPTIBLE:
INTERNAL_IP: 10.150.0.2
EXTERNAL_IP: 34.86.68.178
STATUS: RUNNING

NAME: instance-2
ZONE: us-west4-b
MACHINE_TYPE: n1-standard-1
PREEMPTIBLE:
INTERNAL_IP: 10.182.0.2
EXTERNAL_IP: 34.118.243.233
STATUS: RUNNING
vishrut@cloudshell:~ (cloud-sharma-vishrut)$
```



4) Virtual switch facilitates this connectivity.



7. Creating custom networks

1) The screenshot below shows the new subnets created in **custom-network1** alongside the default subnetworks in those regions assigned to the **default** network.

```
vishrut@cloudshell:~ (cloud-sharma-vishrut)$ 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:
```

2) The result differs from instance-2 because we cannot view the ping. This is because the connectivity to instance 3 and instance 4 is being facilitated by a VPN gateway.

```
https://ssh.cloud.google.com/v2/ssh/projects/cloud-sharma-vishrut/zones/us-east4-b/instances/instance-1?authuser=0&hl=en_US&proj...
https://ssh.cloud.google.com/v2/ssh/projects/cloud-sharma-vishrut/zones/us-east4-b/instances/instance-1?authuser=0&hl=en_... A

SSH-in-browser  UPLOAD FILE  DOWNLOAD FILE  ?  ?  ?

Linux instance-1 5.10.0-21-cloud-amd64 #1 SMP Debian 5.10.162-1 (2023-01-21) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
vishrut@instance-1:~$ ping 10.128.0.2
PING 10.128.0.2 (10.128.0.2) 56(84) bytes of data.
64 bytes from 10.128.0.2: icmp_seq=1 ttl=64 time=61.1 ms
64 bytes from 10.128.0.2: icmp_seq=2 ttl=64 time=59.8 ms
64 bytes from 10.128.0.2: icmp_seq=3 ttl=64 time=59.8 ms
^C
--- 10.128.0.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 59.799/60.233/61.078/0.597 ms
vishrut@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 ---
18 packets transmitted, 0 received, 100% packet loss, time 17391ms

vishrut@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 ---
5 packets transmitted, 0 received, 100% packet loss, time 4097ms

vishrut@instance-1:~$
```

3) Screenshot of all 4 instances in the UI including the network they belong to.

The screenshot shows the Google Cloud console for the project 'cloud-sharma-vishrut'. The 'VM instances' page is active, displaying a table of 4 instances. Each instance is associated with a specific network. A terminal window is open in the foreground, showing the command 'odin ID: vishrut'.

Status	Name	Zone	Internal IP	External IP	Network	Connect
Running	instance-1	us-east4-b	10.150.0.2 (nic0)	34.86.68.178 (nic0)	default	SSH
Running	instance-2	us-west4-b	10.182.0.2 (nic0)	34.118.243.233 (nic0)	default	SSH
Running	instance-3	us-central1-a	192.168.1.2 (nic0)	35.188.138.243 (nic0)	custom-network1	SSH
Running	instance-4	europa-west1-d	192.168.5.2 (nic0)	34.140.156.83 (nic0)	custom-network1	SSH

4) Screenshot of the subnetworks created.

The screenshot shows the Google Cloud console for the project 'cloud-sharma-vishrut'. The 'VPC network' page is active, displaying a table of subnetworks. A terminal window is open in the foreground, showing the command 'odin ID: vishrut'.

Name	Subnets	MTU	Mode	Internal IP ranges	Gateways	Firewall rules	Global dynamic routing
custom-network1	2	1460	Custom			0	Off
default	38	1460	Auto			4	Off

Google Cloud

cloud-sharma-vishrut

vpc network

Search

2

?

V

VPC network

VPC networks

IP addresses

Bring your own IP

Firewall

Routes

VPC network peering

Shared VPC

Serverless VPC access

Packet mirroring

VPC network details

EDIT

DELETE VPC NETWORK

HELP ASSISTANT

HIDE INFO PANEL

Maximum transmission unit

1460

SUBNETS

STATIC INTERNAL IP ADDRESSES

FIREWALLS

ROUTES

VPC NETWORK PEERING

ADD SUBNET

FLOW LOGS

Filter

Enter property name or value

?

III

☐

Name

↑

Region

Stack Type

Internal IP ranges

External IP ranges

Secondary I

☐

subnet-europe-west-192

europa-west1

IPv4

192.168.5.0/24

None

None

☐

subnet-us-central-192

us-central1

IPv4

192.168.1.0/24

None

None

Reserved proxy-only subnets for load balancing

☐

Name

Region

↑

IP address ranges

Gateway

Role

Purpose

No rows to display

SELECT A SUBNET

Please select at least one resource.

Odin ID vishrut

File Edit View

odin ID: vishrut

Ln 1, Col 17 100% Windows (CRLF) UTF-8

CLOUD SHELL

Terminal

cloud-sharma-vishrut

Open Editor

Google Cloud

cloud-sharma-vishrut

vpc network

Search

2

?

V

VPC network

VPC networks

IP addresses

Bring your own IP

Firewall

Routes

VPC network peering

Shared VPC

Serverless VPC access

Packet mirroring

VPC network details

EDIT

DELETE VPC NETWORK

HELP ASSISTANT

HIDE INFO PANEL

SUBNETS

STATIC INTERNAL IP ADDRESSES

FIREWALLS

ROUTES

VPC NETWORK PEERING

ADD SUBNET

FLOW LOGS

Filter

Enter property name or value

?

III

☐

Name

↑

Region

Stack Type

Internal IP ranges

External IP ranges

Secondary I

☐

default

us-central1

IPv4

10.128.0.0/20

None

None

☐

default

europa-west1

IPv4

10.132.0.0/20

None

None

☐

default

us-west1

IPv4

10.138.0.0/20

None

None

☐

default

asia-east1

IPv4

10.140.0.0/20

None

None

☐

default

us-east1

IPv4

10.142.0.0/20

None

None

☐

default

asia-northeast1

IPv4

10.146.0.0/20

None

None

☐

default

asia-southeast1

IPv4

10.148.0.0/20

None

None

☐

default

us-east4

IPv4

10.150.0.0/20

None

None

☐

default

australia-southeast1

IPv4

10.152.0.0/20

None

None

☐

default

europa-west2

IPv4

10.154.0.0/20

None

None

☐

default

europa-west3

IPv4

10.156.0.0/20

None

None

☐

default

southamerica-east1

IPv4

10.158.0.0/20

None

None

☐

default

asia-south1

IPv4

10.160.0.0/20

None

None

SELECT A SUBNET

Please select at least one resource.

Odin ID vishrut

File Edit View

odin ID: vishrut

Ln 1, Col 17 100% Windows (CRLF) UTF-8

CLOUD SHELL

Terminal

cloud-sharma-vishrut

Open Editor