

<b>01.2 ARP, Wireshark, Netsim</b>	<b>1</b>
ARP #1	1
Netsim #2	4
<b>01.3: Cloud Networking</b>	<b>5</b>
Scan targets for services	5
Navigating default networks	5
Creating Custom Networks	6

## 01.2 ARP, Wireshark, Netsim

### ARP #1

```

htran@DESKTOP-01BI236: ~$ 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: bond0: <BROADCAST,MULTICAST,MASTER> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 32:30:ab:b2:e2:bc brd ff:ff:ff:ff:ff:ff
3: dummy0: <BROADCAST,NOARP> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 46:ac:8b:0c:28:94 brd ff:ff:ff:ff:ff:ff
4: tunl0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN group default qlen 1000
    link/ipip 0.0.0.0 brd 0.0.0.0
5: sit0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN group default qlen 1000
    link/sit 0.0.0.0 brd 0.0.0.0
6: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:52:67:c1 brd ff:ff:ff:ff:ff:ff
    inet 172.29.58.175/20 brd 172.29.63.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::215:5dff:fe52:67c1/64 scope link
        valid_lft forever preferred_lft forever
htran@DESKTOP-01BI236:~$ netstat -rn
Kernel IP routing table
Destination        Gateway           Genmask          Flags  MSS  Window  irtt  Iface
0.0.0.0            172.29.48.1      0.0.0.0          UG     0    0        0     eth0
172.29.48.0        0.0.0.0          255.255.240.0    U      0    0        0     eth0
htran@DESKTOP-01BI236:~$ ping www.google.com
PING www.google.com (142.251.215.228) 56(84) bytes of data.
64 bytes from sea09s35-in-f4.1e100.net (142.251.215.228): icmp_seq=1 ttl=116 time=23.7 ms
64 bytes from sea09s35-in-f4.1e100.net (142.251.215.228): icmp_seq=2 ttl=116 time=10.4 ms
^C
--- www.google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 10.353/17.015/23.677/6.662 ms
htran@DESKTOP-01BI236:~$ arp
Address          HWtype  HWaddress      Flags Mask    Iface
172.29.48.0      ether   00:15:5d:ce:aa:8b  C          eth0
DESKTOP-01BI236.mshome. ether    00:15:5d:ce:aa:8b  C          eth0
htran@DESKTOP-01BI236:~$

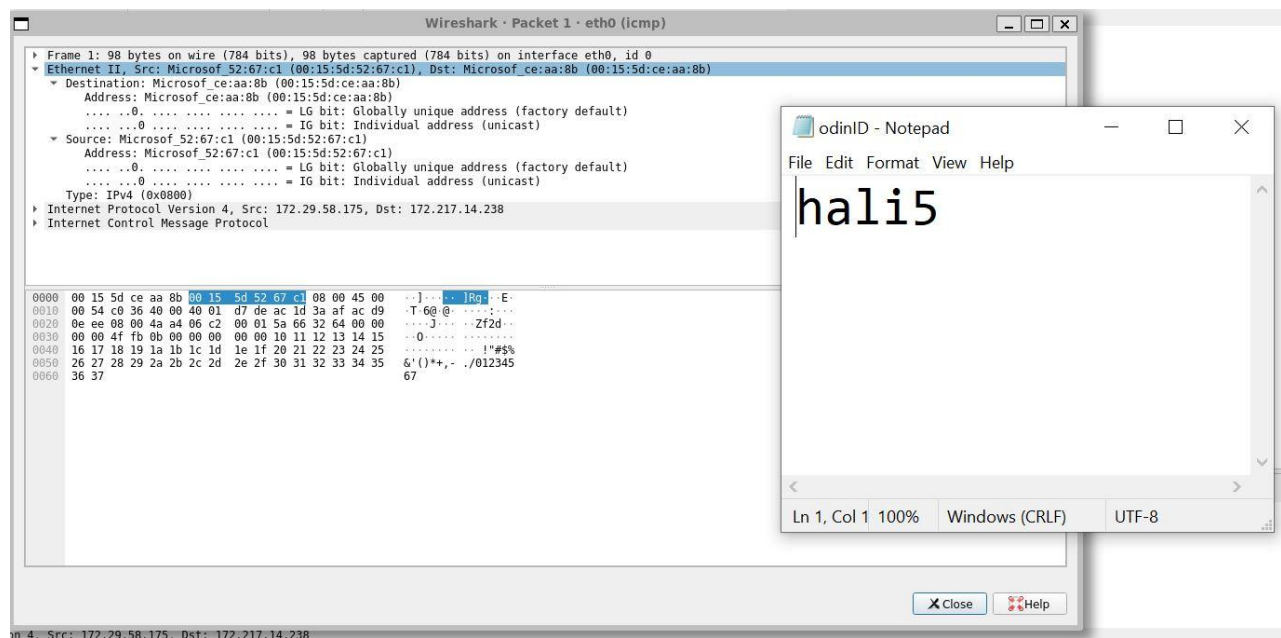
```

**Note:** Professor Wu-chang feng allowed me to ping [www.google.com](http://www.google.com) instead of my default router's IP address due to unresolved issues regarding netstat -rn and Ubuntu WSL

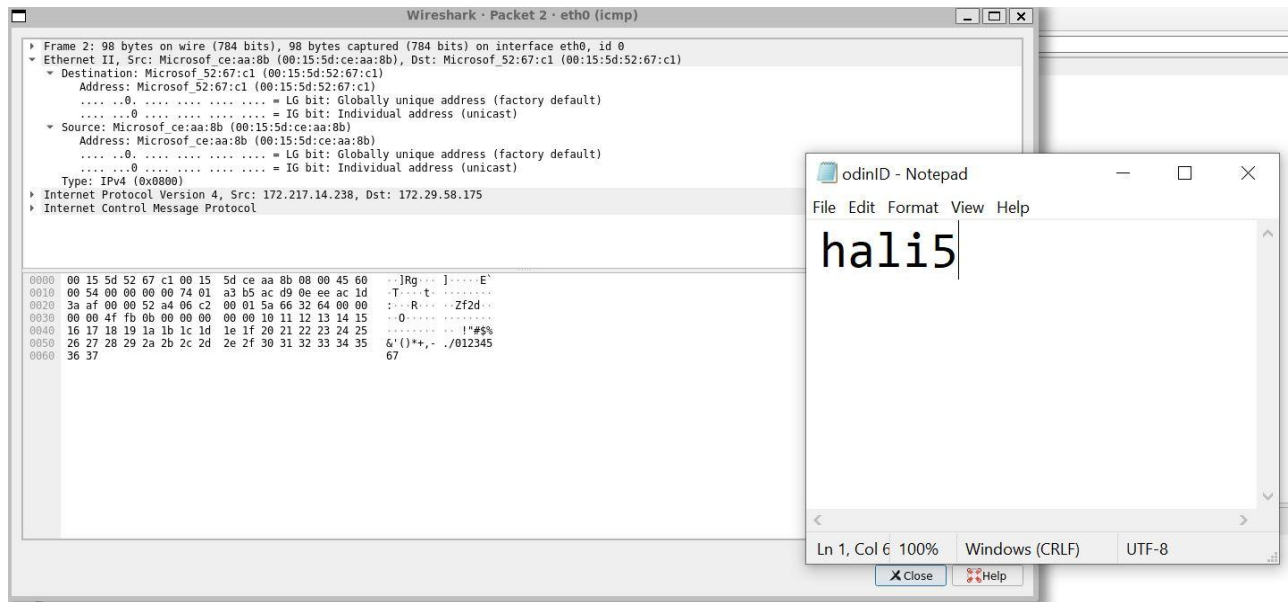
**Which hardware manufacturer does the destination hardware address of the packet indicate?**

The destination hardware address packet indicates that the hardware manufacturer is Microsoft.  
This is shown in the screenshots below under Destination → Address

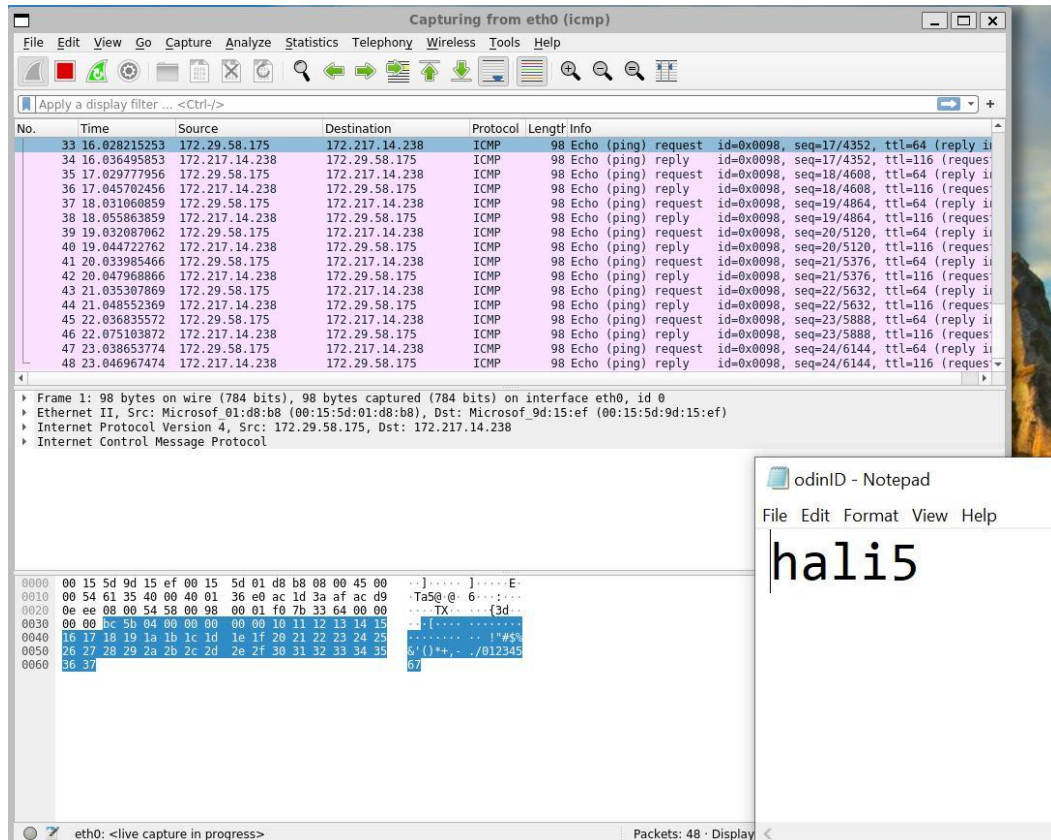
*Request packet window*



## Response packet window



## Screenshot of the bytes in the packet dump window



## Netsim #2

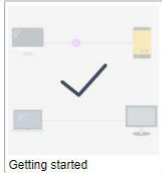
### Screenshot of the completed list of levels in Netsim.

### 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 [@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

odinID - Notepad

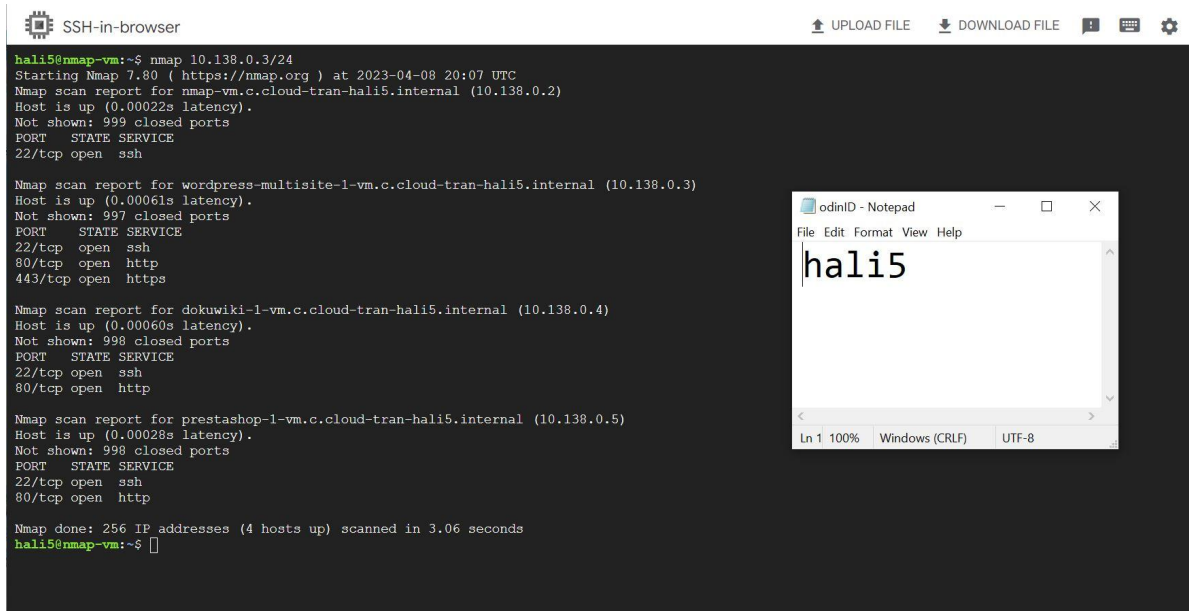
File Edit Format View Help

hali5

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

## 01.3: Cloud Networking

### Scan targets for services



```
SSH-in-browser
hali5@nmap-vm:~$ nmap 10.138.0.3/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-08 20:07 UTC
Nmap scan report for nmap-vm.c.cloud-tran-hali5.internal (10.138.0.2)
Host is up (0.00022s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap scan report for wordpress-multisite-1-vm.c.cloud-tran-hali5.internal (10.138.0.3)
Host is up (0.00061s 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-tran-hali5.internal (10.138.0.4)
Host is up (0.00060s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap scan report for prestashop-1-vm.c.cloud-tran-hali5.internal (10.138.0.5)
Host is up (0.00028s 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 3.06 seconds
hali5@nmap-vm:~$
```

### Navigating default networks

**How many subnetworks are created initially on the default network? How many regions does this correspond to?**

There are 38 subnetworks that are initially created on the default network, with 38 corresponding regions.

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

Each subnetwork supports 4096 hosts.

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

The CIDR subnetwork that these instances are brought up in are 10.150.0.2 for us-east4b and 10.182.0.2 for us-west-4b. Yes, they both correspond to the appropriate region based on the prior command.

```
hali5@cloudshell:~ (cloud-tran-hali5)$ 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: 34.86.247.112
STATUS: RUNNING

NAME: instance-2
ZONE: us-west4-b
MACHINE_TYPE: n1-standard-1
PREEMPTIBLE:
INTERNAL_IP: 10.182.0.2
EXTERNAL_IP: 34.125.50.29
STATUS: RUNNING
hali5@cloudshell:~ (cloud-tran-hali5)$
```

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

The Virtual Switch

### Creating Custom Networks

**Take a screenshot of the new subnets created in custom-network1 alongside the default subnetworks in those regions assigned to the default network**

```

hali5@cloudshell:~ (cloud-tran-hali5) $ gcloud compute networks subnets list --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:

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:

```

```

hali5@cloudshell:~ (cloud-tran-hali5) $ gcloud compute networks subnets list --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:

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:

```

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

Since instance-1 is within the same network as instance-2, it is able to perform the ping command and get a response back. However, instance-1 is not within the same network as instance-3 and instance-4 which is why an attempt to ping those VM's results in no response.



**Take screenshots of all 4 instances in the UI including the network they belong to.**




cloud-Tran-hali5

Search (/) for resources, docs, products, and more

Search



2



VM instances

[CREATE INSTANCE](#) [IMPORT VM](#) [REFRESH](#) [HELP ASSISTANT](#)

INSTANCES

OBSERVABILITY

INSTANCE SCHEDULES

VM instances

Filter

Enter property name or value



<input type="checkbox"/>	Status	Name ↑	Zone	Recommendations	In use by	Internal IP	External IP	Network	Connect
<input type="checkbox"/>	✓	<a href="#">instance-1</a>	us-east4-b			10.150.0.2 ( <a href="#">nic0</a> )	34.86.247.112 ( <a href="#">nic0</a> )	<a href="#">default</a>	SSH ▾
<input type="checkbox"/>	✓	<a href="#">instance-2</a>	us-west4-b			10.182.0.2 ( <a href="#">nic0</a> )	34.125.50.29 ( <a href="#">nic0</a> )	<a href="#">default</a>	SSH ▾
<input type="checkbox"/>	✓	<a href="#">instance-3</a>	us-central1-a			192.168.1.2 ( <a href="#">nic0</a> )	35.239.224.87 ( <a href="#">nic0</a> )	<a href="#">custom-network1</a>	SSH ▾
<input type="checkbox"/>	✓	<a href="#">instance-4</a>	europa-west1-d			192.168.5.2 ( <a href="#">nic0</a> )	104.155.87.213 ( <a href="#">nic0</a> )	<a href="#">custom-network1</a>	SSH ▾

Then visit "VPC Network" and take a screenshot of the subnetworks created.


cloud-Tran-hali5

Search (/) for resources, docs, products, and more

Search



2



VPC networks

[CREATE VPC NETWORK](#) [REFRESH](#) [HE](#)

NETWORKS IN CURRENT PROJECT

SUBNETS IN CURRENT PROJECT

Select the VPC networks for which you want to view subnets. If no networks are selected, the table shows the subnets in the current project.

VPC networks ▾

Subnets

Filter

Enter property name or value

Name	Region	VPC network ↑	Internal IP ranges	External IP ranges	Secondary IPv4 ranges	Gateways	Flow logs
<a href="#">subnet-europe-west-192</a>	europa-west1	<a href="#">custom-network1</a>	192.168.5.0/24	None	None	192.168.5.1	Off
<a href="#">subnet-us-central-192</a>	us-central1	<a href="#">custom-network1</a>	192.168.1.0/24	None	None	192.168.1.1	Off