Week 1 Lab

Robin Su
robisu@pdx.edu

1. ARP

IP and Hardware Addresses

IP Address of local virtual ethernet card: 10.0.2.15
Hardware Address: 08:00:27:e4:f8:5c

```
robisu@robisu:~$ ifconfig -v
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:59:65:31:2f  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::57ee:f0d0:f85a:4f6f  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:e4:f8:5c  txqueuelen 1000  (Ethernet)
        RX packets 95099  bytes 120790263 (120.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 26615  bytes 4202725 (4.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1273  bytes 133507 (133.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1273  bytes 133507 (133.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Default Router IP: 10.0.2.2

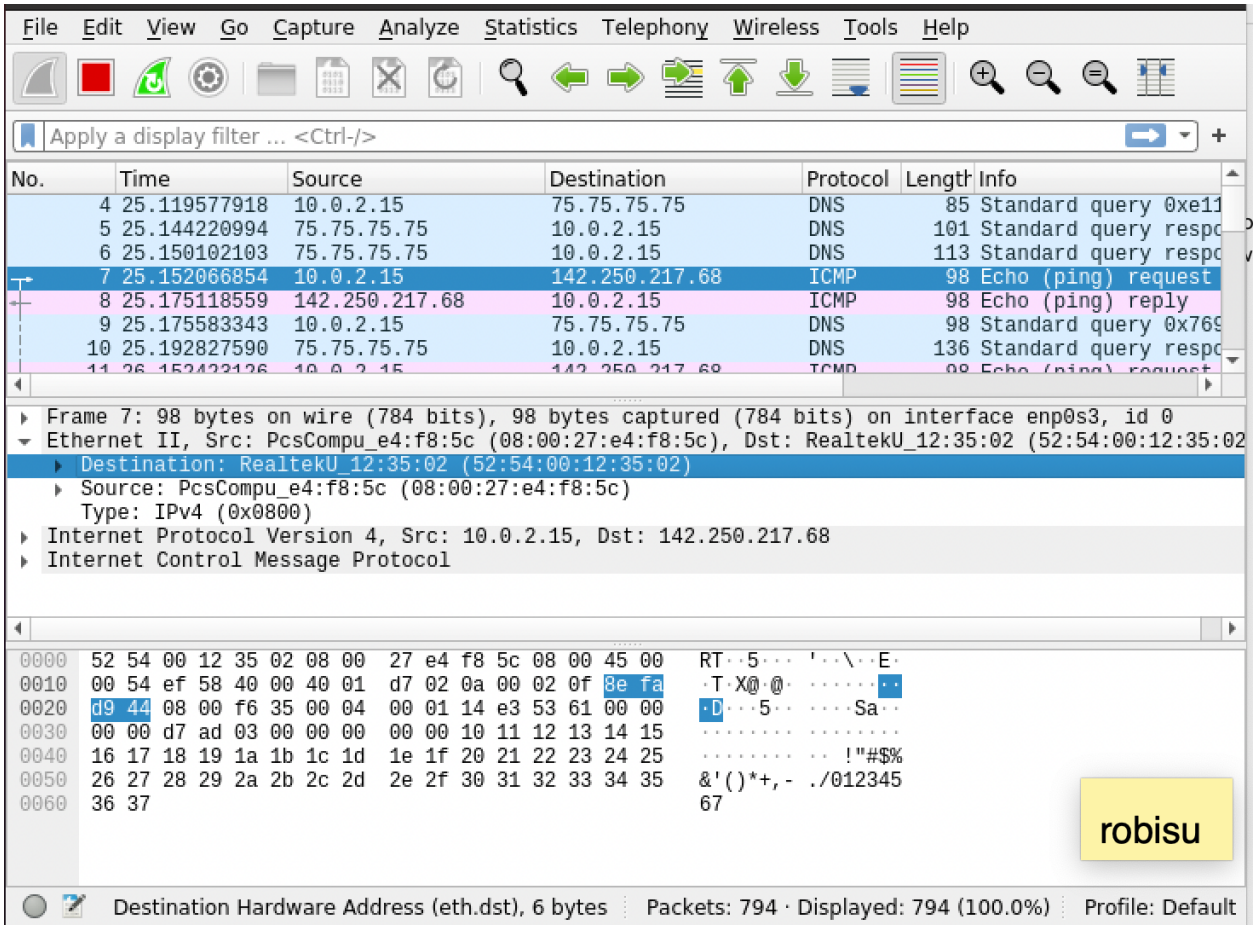
```
robisu@robisu:~$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         10.0.2.2        0.0.0.0         UG        0 0          0 enp0s3
10.0.2.0        0.0.0.0         255.255.255.0   U         0 0          0 enp0s3
169.254.0.0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

Hardware Address: 52:54:00:12:35:02

```
robisu@robisu:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Ifac
e
_gateway                 ether   52:54:00:12:35:02   C                     enp0
s3
```

Wireshark Questions

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



- *Which hardware manufacturer does the destination hardware address of the response packet indicate?* **PCS Computer Systems**

No.	Time	Source	Destination	Protocol	Length	Info
4	25.119577918	10.0.2.15	75.75.75.75	DNS	85	Standard query 0xe11
5	25.144220994	75.75.75.75	10.0.2.15	DNS	101	Standard query respo
6	25.150102103	75.75.75.75	10.0.2.15	DNS	113	Standard query respo
7	25.152066854	10.0.2.15	142.250.217.68	ICMP	98	Echo (ping) request
8	25.175118559	142.250.217.68	10.0.2.15	ICMP	98	Echo (ping) reply
9	25.175583343	10.0.2.15	75.75.75.75	DNS	98	Standard query 0x769
10	25.192827590	75.75.75.75	10.0.2.15	DNS	136	Standard query respo
11	26.152423126	10.0.2.15	142.250.217.68	ICMP	98	Echo (ping) request

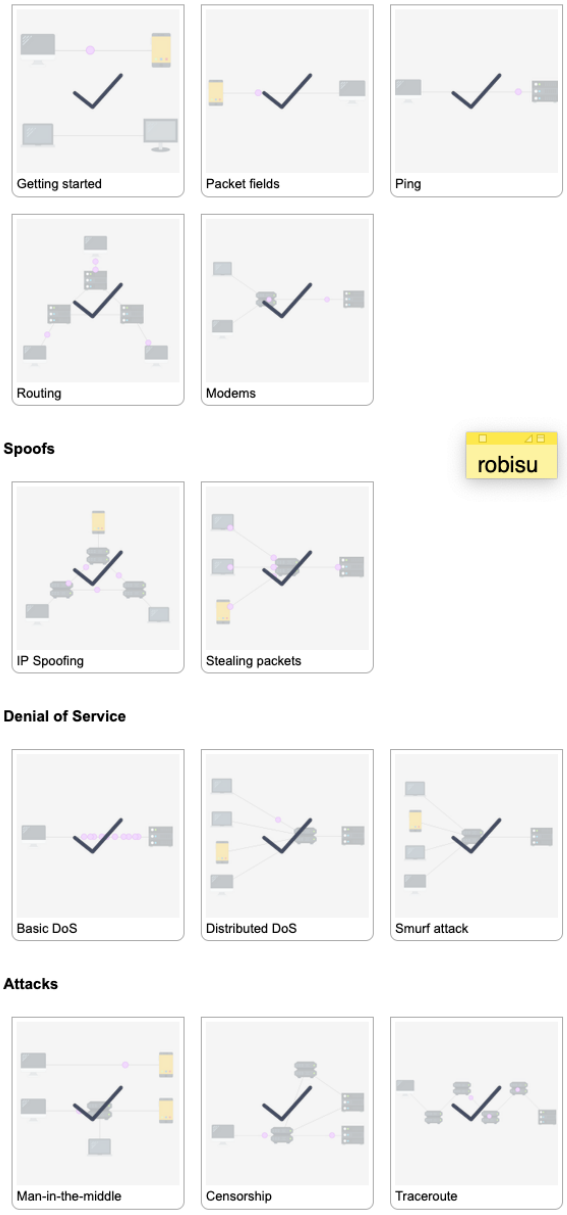
```
▸ Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface enp0s3, id 0
▾ Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_e4:f8:5c (08:00:27:e4:f8:5c
  ▸ Destination: PcsCompu_e4:f8:5c (08:00:27:e4:f8:5c)
  ▸ Source: RealtekU_12:35:02 (52:54:00:12:35:02)
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 142.250.217.68, Dst: 10.0.2.15
▸ Internet Control Message Protocol
```

```
0000  08 00 27 e4 f8 5c 52 54  00 12 35 02 08 00 45 00   ··'··\RT ··5···E·
0010  00 54 cc a6 40 00 3f 01  fa b4 8e fa d9 44 0a 00   ·T··@·?· ·····D··
0020  02 0f 00 00 fe 35 00 04  00 01 14 e3 53 61 00 00   ·····5·· ····Sa··
0030  00 00 d7 ad 03 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
```

robisu

Destination Hardware Address (eth.dst), 6 bytes | Packets: 866 · Displayed: 866 (100.0%) | Profile: Default

2. Netsim


Getting started
Packet fields
Ping
Routing
Modems
Spoofs
robisu
IP Spoofing
Stealing packets
Denial of Service
Basic DoS
Distributed DoS
Smurf attack
Attacks
Man-in-the-middle
Censorship
Traceroute

3. Cloud Networking

** Quick note about my commands below: I configured my home machine to ssh into the instances and use *gcloud compute* commands, so the commands in the screenshots are slightly different than what is in the lab instructions - I set an alias for “gcloud compute” as “gc”.**

Nmap for 3 deployed solutions

```
rsu@robisu-instance-1:~$ nmap 10.138.0.3

Starting Nmap 7.60 ( https://nmap.org ) at 2021-10-01 22:59 UTC
Nmap scan report for wordpress-1-vm.c.cloud-f21-robin-su-robisu.internal (10.138.0.3)
Host is up (0.00027s 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
rsu@robisu-instance-1:~$ nmap 10.138.0.5

Starting Nmap 7.60 ( https://nmap.org ) at 2021-10-01 23:00 UTC
Nmap scan report for wordpress-2-vm.c.cloud-f21-robin-su-robisu.internal (10.138.0.5)
Host is up (0.00022s 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
rsu@robisu-instance-1:~$ nmap 10.138.0.6

Starting Nmap 7.60 ( https://nmap.org ) at 2021-10-01 23:00 UTC
Nmap scan report for wordpress-3-vm.c.cloud-f21-robin-su-robisu.internal (10.138.0.6)
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 0.06 seconds
rsu@robisu-instance-1:~$
```

robisu

Subnetwork Questions

- *How many subnetworks are created initially on the default network? How many regions does this correspond to?* **There are 28 subnetworks, 28 regions**

```
➜  ~ source ~/.zshrc
➜  ~ gc networks subnets list
NAME     REGION                   NETWORK  RANGE          STACK_TYPE  IPV6_ACCESS_TYPE  IPV6_CIDR_RANGE  EXTERNAL_IPV6_CIDR_RANGE
default  us-central1              default  10.128.0.0/20  IPV4_ONLY
default  europe-west1             default  10.132.0.0/20  IPV4_ONLY
default  us-west1                 default  10.138.0.0/20  IPV4_ONLY
default  asia-east1               default  10.140.0.0/20  IPV4_ONLY
default  us-east1                 default  10.142.0.0/20  IPV4_ONLY
default  asia-northeast1          default  10.146.0.0/20  IPV4_ONLY
default  asia-southeast1          default  10.148.0.0/20  IPV4_ONLY
default  us-east4                 default  10.150.0.0/20  IPV4_ONLY
default  australia-southeast1     default  10.152.0.0/20  IPV4_ONLY
default  europe-west2             default  10.154.0.0/20  IPV4_ONLY
default  europe-west3             default  10.156.0.0/20  IPV4_ONLY
default  southamerica-east1       default  10.158.0.0/20  IPV4_ONLY
default  asia-south1              default  10.160.0.0/20  IPV4_ONLY
default  northamerica-northeast1  default  10.162.0.0/20  IPV4_ONLY
default  europe-west4             default  10.164.0.0/20  IPV4_ONLY
default  europe-north1            default  10.166.0.0/20  IPV4_ONLY
default  us-west2                 default  10.168.0.0/20  IPV4_ONLY
default  asia-east2               default  10.170.0.0/20  IPV4_ONLY
default  europe-west6             default  10.172.0.0/20  IPV4_ONLY
default  asia-northeast2          default  10.174.0.0/20  IPV4_ONLY
default  asia-northeast3          default  10.178.0.0/20  IPV4_ONLY
default  us-west3                 default  10.180.0.0/20  IPV4_ONLY
default  us-west4                 default  10.182.0.0/20  IPV4_ONLY
default  asia-southeast2          default  10.184.0.0/20  IPV4_ONLY
default  europe-central2          default  10.186.0.0/20  IPV4_ONLY
default  northamerica-northeast2  default  10.188.0.0/20  IPV4_ONLY
default  asia-south2              default  10.190.0.0/20  IPV4_ONLY
default  australia-southeast2     default  10.192.0.0/20  IPV4_ONLY
➜  ~ gc networks subnets list | grep default | wc -l
      28
➜  ~
```

- *Given the CIDR prefix associated with each subnetwork, how many hosts does each subnetwork support?* **2^12, or 4096 hosts per subnetwork**

Two new instances, instance-1 and instance-2

```
➜  ~ gc instances list
NAME        ZONE           MACHINE_TYPE   PREEMPTIBLE  INTERNAL_IP  EXTERNAL_IP   STATUS
instance-2  asia-south1-b  n1-standard-1               10.160.0.3   34.93.79.178  RUNNING
instance-1  asia-south1-a  n1-standard-1               10.160.0.2   35.244.11.68  RUNNING
➜  ~ gc networks subnets list | grep asia-south1
default  asia-south1              default  10.160.0.0/20  IPV4_ONLY
➜  ~
```

robisu

- *Which CIDR subnetworks are these instances brought up in? Do they correspond to the appropriate region based on the prior commands?* **Both are on the asia-south1 region, as they share a network address (10.160.0.*), which does correspond to the region in which they were instructed to be created in.**

Ping instance-2 from instance-1:

```
permitted by applicable law.
rsu@instance-1:~$ ping 10.160.0.3
PING 10.160.0.3 (10.160.0.3) 56(84) bytes of data.
64 bytes from 10.160.0.3: icmp_seq=1 ttl=64 time=1.18 ms
64 bytes from 10.160.0.3: icmp_seq=2 ttl=64 time=0.192 ms
64 bytes from 10.160.0.3: icmp_seq=3 ttl=64 time=0.208 ms
64 bytes from 10.160.0.3: icmp_seq=4 ttl=64 time=0.197 ms
64 bytes from 10.160.0.3: icmp_seq=5 ttl=64 time=0.215 ms
64 bytes from 10.160.0.3: icmp_seq=6 ttl=64 time=0.199 ms
64 bytes from 10.160.0.3: icmp_seq=7 ttl=64 time=0.208 ms
64 bytes from 10.160.0.3: icmp_seq=8 ttl=64 time=0.200 ms
^C
--- 10.160.0.3 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 160ms
rtt min/avg/max/mdev = 0.192/0.324/1.175/0.321 ms
rsu@instance-1:~$
```

robisu

- *From the figure in the previous step. What facilitates this connectivity: the virtual switch or the VPN Gateway?* **Since both instances are in the same region AND zone, it would appear that the <u>virtual switch</u> can connect one to the other**

New custom-network-1 created alongside the default network

```
➜  ~ gc networks list
NAME            SUBNET_MODE  BGP_ROUTING_MODE  IPV4_RANGE  GATEWAY_IPV4
custom-network1 CUSTOM       REGIONAL
default         AUTO         REGIONAL
➜  ~
```

robisu

New subnetworks created in custom-network-1

```
→  ~ gc networks subnets list
NAME                    REGION                  NETWORK          RANGE           STACK_TYPE  IPV6_ACCESS_TYPE  IPV6_CIDR_RANGE  EXTERNAL_IPV6_CIDR
_RANGE
default                 us-central1             default          10.128.0.0/20   IPV4_ONLY
subnet-us-central-192   us-central1             custom-network1  192.168.1.0/24  IPV4_ONLY
default                 europe-west1            default          10.132.0.0/20   IPV4_ONLY
subnet-europe-west-192  europe-west1            custom-network1  192.168.5.0/24  IPV4_ONLY
default                 us-west1                default          10.138.0.0/20   IPV4_ONLY
default                 asia-east1              default          10.140.0.0/20   IPV4_ONLY
default                 us-east1                default          10.142.0.0/20   IPV4_ONLY
default                 asia-northeast1         default          10.146.0.0/20   IPV4_ONLY
default                 asia-southeast1         default          10.148.0.0/20   IPV4_ONLY
default                 us-east4                default          10.150.0.0/20   IPV4_ONLY
default                 australia-southeast1    default          10.152.0.0/20   IPV4_ONLY
default                 europe-west2            default          10.154.0.0/20   IPV4_ONLY
default                 europe-west3            default          10.156.0.0/20   IPV4_ONLY
default                 southamerica-east1      default          10.158.0.0/20   IPV4_ONLY
default                 asia-south1             default          10.160.0.0/20   IPV4_ONLY
default                 northamerica-northeast1 default          10.162.0.0/20   IPV4_ONLY
default                 europe-west4            default          10.164.0.0/20   IPV4_ONLY
default                 europe-north1           default          10.166.0.0/20   IPV4_ONLY
default                 us-west2                default          10.168.0.0/20   IPV4_ONLY
default                 asia-east2              default          10.170.0.0/20   IPV4_ONLY
default                 europe-west6            default          10.172.0.0/20   IPV4_ONLY
default                 asia-northeast2         default          10.174.0.0/20   IPV4_ONLY
default                 asia-northeast3         default          10.178.0.0/20   IPV4_ONLY
default                 us-west3                default          10.180.0.0/20   IPV4_ONLY
default                 us-west4                default          10.182.0.0/20   IPV4_ONLY
default                 asia-southeast2         default          10.184.0.0/20   IPV4_ONLY
default                 europe-central2         default          10.186.0.0/20   IPV4_ONLY
default                 northamerica-northeast2 default          10.188.0.0/20   IPV4_ONLY
default                 asia-south2             default          10.190.0.0/20   IPV4_ONLY
default                 australia-southeast2    default          10.192.0.0/20   IPV4_ONLY
→  ~
```

robisu

Ping from instance-1 to instance-3 and instance-4

```
rsu@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 ---
14 packets transmitted, 0 received, 100% packet loss, time 324ms

rsu@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 ---
11 packets transmitted, 0 received, 100% packet loss, time 257ms
```

robisu

- *Explain why the result is different from instance-2.* **The two instances are not within the same network as instance-1, let alone zone or region, so they are not directly connected. Thus, though the packets are being sent, we see that there has been 100% packet loss in both pings, instead of 0%. The two networks have completely different IP ranges.**

Instances in the GCP UI

Filter Enter property name or value

Status	Name	Zone	Recommendations	In use by	Internal IP	External IP	Network	Connect
	instance-1	asia-south1-a			10.160.0.2 (nic0)	35.244.11.68	default	SSH
	instance-2	asia-south1-b			10.160.0.3 (nic0)	34.93.79.178	default	SSH
	instance-3	us-central1-a			192.168.1.2 (nic0)	104.154.129.178	custom-network1	SSH
	instance-4	europe-west1-d			192.168.5.2 (nic0)	34.79.169.78	custom-network1	SSH

Related actions

robisu

Networks in the GCP UI

Name	Region	Subnets	MTU	Mode	IP address ranges	Gateways	Firewall Rules	Global dynamic routing	Flow
custom-network1		2	1460	Custom			0	Off	
	us-central1	subnet-us-central-192			192.168.1.0/24	192.168.1.1			Off
	europe-west1	subnet-europe-west-192			192.168.5.0/24	192.168.5.1			Off

robisu