

Week1

Lab1

Armant Touche

**Class/Instructor:** CS430P/ Dr. Wu-Chang  
**Date:** 9/30/22

# Table of Contents

## 1. Lab1, HW1

### 1.1. Homework #1

### 1.2. ARP, Wireshark, Netsim

### 1.3. Cloud networking

# Homework #1 ([Link](#))

1. Linux VM setup
  - ☐ Download Ubuntu 20.04 VM
    - i. Link: <https://releases.ubuntu.com/20.04/>
  - ☐ VirtualBox (VB)
    - i. Install
      1. Link: <https://www.virtualbox.org/wiki/Downloads>
2. Slack Account
  - ☐ Join
3. GitLab Account
  - ☐ Signup
  - ☐ Add `id_rsa.pub` key in Preferences -> SSH Keys
4. GitLab repo
  - ☐ Create Project
  - ☐ Invite Instructor and TA
  - ☐ Setup local git in VB, clone, and add README
5. Git
  - ☐ Init notebook
6. Docker Hub account
  - ☐ Add `dockerhub.txt` after signing up with `@pdx.edu` email
7. Google Cloud Platform account
  - ☐ Get Coupon
  - ☐ Create Project
8. AWS Academy
  - ☐ Wait for Canvas invite (NOTE: did not receive yet)
9. AWS via Vora
10. AWS CLI
  - ☐ Using Option **(1)**

## ARP, Wireshark, Netsim ([Link](#))

### 1. ARP #1

☐ Install Wireshark

☐ Perform tasks

i. Use `ip` cmd to find virtual `lo` interface address

```
atouche@atouche:~$ ip -br addr show
lo                UNKNOWN      127.0.0.1/8  ::1/128
enp0s3            UP          10.0.2.15/24 fe80::a4f3:d7aa:92d9:2e89/64
docker0           DOWN        172.17.0.1/16
```

1. enp0s3: 10.0.2.15

ii. Perform `netstat -rn` to find default router's IP address

```
atouche@atouche:~$ 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
```

1. gateway: 10.0.2.2

iii. ping default and use `arp` to find it's hardware address (MAC)

```
atouche@atouche:~$ 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=0.133 ms
64 bytes from 10.0.2.2: icmp_seq=2 ttl=64 time=0.241 ms
^C
--- 10.0.2.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1050ms
rtt min/avg/max/mdev = 0.133/0.187/0.241/0.054 ms
atouche@atouche:~$ arp -a 10.0.2.2
_gateway (10.0.2.2) at 52:54:00:12:35:02 [ether] on enp0s3
atouche@atouche:~$
```

1. MAC: 52:54:00:12:35:02

iv. Wireshark

1. Add icmp and ping [www.google.com](http://www.google.com)
2. Answer following questions for request:
  - a. Which hardware manufacturer does the destination hardware address of the packet indicate?

In the data-link layer (L2) packet or frame, the MAC address for destination is 52:54:00:12:35:02 which is the MAC address of the default gateway (10.0.0.2). L2 frame indicates source device is the VM and destination is the router/default gateway.

- b. Take a screenshot of the bytes in the packet dump window as shown below

Capturing from enp0s3 (icmp)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	142.251.33.68	ICMP	98	Echo (ping) request id=0x0003, seq=1/256, ttl=64 (r
3	1.001284590	10.0.2.15	142.251.33.68	ICMP	98	Echo (ping) request id=0x0003, seq=2/512, ttl=64 (r
5	2.002596693	10.0.2.15	142.251.33.68	ICMP	98	Echo (ping) request id=0x0003, seq=3/768, ttl=64 (r
7	3.006955015	10.0.2.15	142.251.33.68	ICMP	98	Echo (ping) request id=0x0003, seq=4/1024, ttl=64 (r
9	4.008287000	10.0.2.15	142.251.33.68	ICMP	98	Echo (ping) request id=0x0003, seq=5/1280, ttl=64 (r
11	5.009365065	10.0.2.15	142.251.33.68	ICMP	98	Echo (ping) request id=0x0003, seq=6/1536, ttl=64 (r
13	6.014189438	10.0.2.15	142.251.33.68	ICMP	98	Echo (ping) request id=0x0003, seq=7/1792, ttl=64 (r
15	7.014620434	10.0.2.15	142.251.33.68	ICMP	98	Echo (ping) request id=0x0003, seq=8/2048, ttl=64 (r
17	8.015817156	10.0.2.15	142.251.33.68	ICMP	98	Echo (ping) request id=0x0003, seq=9/2304, ttl=64 (r
19	9.017660767	10.0.2.15	142.251.33.68	ICMP	98	Echo (ping) request id=0x0003, seq=10/2560, ttl=64 (r
21	10.020603744	10.0.2.15	142.251.33.68	ICMP	98	Echo (ping) request id=0x0003, seq=11/2816, ttl=64 (r
23	11.026661344	10.0.2.15	142.251.33.68	ICMP	98	Echo (ping) request id=0x0003, seq=12/3072, ttl=64 (r
25	12.030692291	10.0.2.15	142.251.33.68	ICMP	98	Echo (ping) request id=0x0003, seq=13/3328, ttl=64 (r

Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface enp0s3, id 0

Ethernet II, Src: PcsCompu\_43:ca:17 (08:00:27:43:ca:17), Dst: RealtekU\_12:35:02 (52:54:00:12:35:02)

Destination: RealtekU\_12:35:02 (52:54:00:12:35:02)

Address: RealtekU\_12:35:02 (52:54:00:12:35:02)

...1. .... = LG bit: Locally administered address (this is NOT the factory default)

...0. .... = IG bit: Individual address (unicast)

Source: PcsCompu\_43:ca:17 (08:00:27:43:ca:17)

Address: PcsCompu\_43:ca:17 (08:00:27:43:ca:17)

...0. .... = LG bit: Globally unique address (factory default)

...0. .... = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 10.0.2.15, Dst: 142.251.33.68

Internet Control Message Protocol

0000 52 54 00 12 35 02 08 00 27 43 ca 17 08 00 45 00 RT..5... 'C...E.

0010 00 54 41 98 40 00 40 01 3c c3 0a 00 02 0f 8e fb .TA.@.<.....

0020 21 44 08 00 35 3a 00 03 00 01 40 b7 34 63 00 00 !D.5:...@.4C...

0030 00 00 87 d4 07 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

Destination Hardware Address (eth.dst), 6 bytes

Packets: 30 · Displayed: 30 (100.0%) Profile: Default

3. Answer following questions for reply:

- a. Which hardware manufacturer does the destination hardware address of the packet indicate?

In the data-link layer (L2) packet or frame, the MAC address for destination is 08:00:27:43:ca:17 which is the MAC address of Google's servers (142.251.33.68). L2 frame indicates source device is the default gateway and destination is Google's server.

- b. Take a screenshot of the bytes in the packet dump window as shown below

**Capturing from enp0s3 (icmp)**

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
19	9.017660767	10.0.2.15	142.251.33.68	ICMP	98	Echo (ping) request id=0x0003, seq=10/2560, ttl=64
21	10.020603744	10.0.2.15	142.251.33.68	ICMP	98	Echo (ping) request id=0x0003, seq=11/2816, ttl=64
23	11.026661344	10.0.2.15	142.251.33.68	ICMP	98	Echo (ping) request id=0x0003, seq=12/3072, ttl=64
25	12.030692291	10.0.2.15	142.251.33.68	ICMP	98	Echo (ping) request id=0x0003, seq=13/3328, ttl=64
27	13.040387454	10.0.2.15	142.251.33.68	ICMP	98	Echo (ping) request id=0x0003, seq=14/3584, ttl=64
29	14.045185191	10.0.2.15	142.251.33.68	ICMP	98	Echo (ping) request id=0x0003, seq=15/3840, ttl=64
+	2 0.008538163	142.251.33.68	10.0.2.15	ICMP	98	Echo (ping) reply id=0x0003, seq=1/256, ttl=63 (r
4	1.009397534	142.251.33.68	10.0.2.15	ICMP	98	Echo (ping) reply id=0x0003, seq=2/512, ttl=63 (r
6	2.010324363	142.251.33.68	10.0.2.15	ICMP	98	Echo (ping) reply id=0x0003, seq=3/768, ttl=63 (r
8	3.089208840	142.251.33.68	10.0.2.15	ICMP	98	Echo (ping) reply id=0x0003, seq=4/1024, ttl=63 (r
10	4.017229570	142.251.33.68	10.0.2.15	ICMP	98	Echo (ping) reply id=0x0003, seq=5/1280, ttl=63 (r
12	5.017551576	142.251.33.68	10.0.2.15	ICMP	98	Echo (ping) reply id=0x0003, seq=6/1536, ttl=63 (r
14	6.023159894	142.251.33.68	10.0.2.15	ICMP	98	Echo (ping) reply id=0x0003, seq=7/1792, ttl=63 (r

Frame 2: 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\_43:ca:17 (08:00:27:43:ca:17)

Destination: PcsCompu\_43:ca:17 (08:00:27:43:ca:17)

Address: PcsCompu\_43:ca:17 (08:00:27:43:ca:17)

...0... = LG bit: Globally unique address (factory default)

...0... = IG bit: Individual address (unicast)

Source: RealtekU\_12:35:02 (52:54:00:12:35:02)

Address: RealtekU\_12:35:02 (52:54:00:12:35:02)

...1... = LG bit: Locally administered address (this is NOT the factory default)

...0... = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 142.251.33.68, Dst: 10.0.2.15

Internet Control Message Protocol

0000 08 00 27 43 ca 17 52 54 00 12 35 02 08 00 45 00 ...C..RT..5...E..

0010 00 54 00 ef 40 00 3f 01 7e 6c 8e fb 21 44 0a 00 ..T..@.?..~1..!D..

0020 02 0f 00 00 3d 3a 00 03 00 01 40 b7 34 63 00 00 .....:....@.4c...

0030 00 00 87 d4 07 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 8'()\*+,-./012345

0060 36 37 67

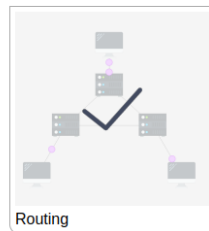
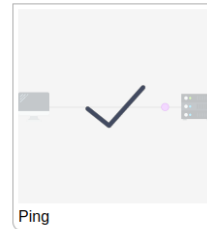
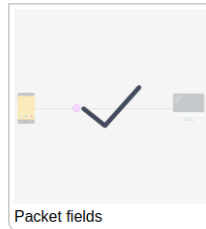
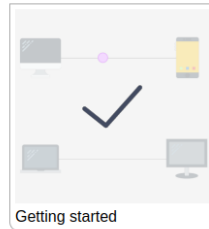
Destination Hardware Address (eth.dst), 6 bytes

Packets: 30 · Displayed: 30 (100.0%) Profile: Default

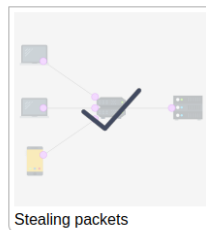
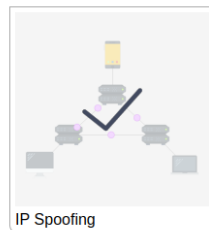
## 2. Netsim #2

☐ Complete all levels

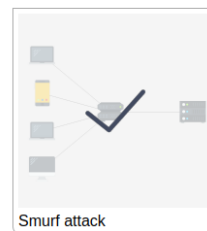
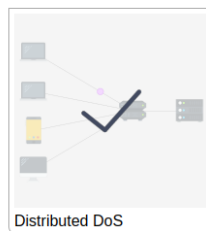
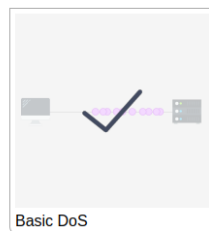
### Basics



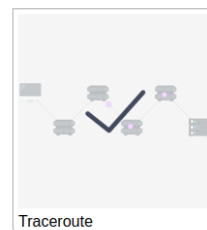
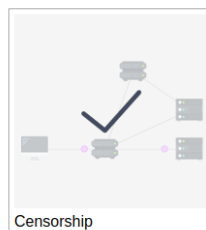
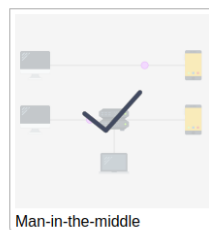
### Spoofs



### Denial of Service



### Attacks



## Cloud Networking

### 1. Network scanning (nmap) #1

- ☐ Create VM
- ☐ Install nmap

### 2. Launch targets

### 3. Scan targets for services

```
atouche@atouche:~$ nmap 10.138.0.2/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-30 03:45 UTC
Nmap scan report for atouche.c.cloud-touche-atouche.internal (10.138.0.2)
Host is up (0.00020s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap scan report for target-1-vm.c.cloud-touche-atouche.internal (10.138.0.3)
Host is up (0.00056s 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 target-2-vm.c.cloud-touche-atouche.internal (10.138.0.4)
Host is up (0.00056s 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 target-3-vm.c.cloud-touche-atouche.internal (10.138.0.5)
Host is up (0.00022s 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 3.08 seconds
```



4. CIDR and subnets #2

5. Navigating default network

☐ Answer following questions:

- i. **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` )**

72 subnetworks are created initially with default.

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

$$2^{(32-20)} - 2 = 4094 \text{ host(s) / subnetwork}$$

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

In 10.150.0.0/instance-1 and 10.182.0.0/instance-2. Yes

```
atouche@instance-1:~$ ping 10.182.0.2
PING 10.182.0.2 (10.182.0.2) 56(84) bytes of data.
```

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

Virtual switch

## 6. Creating custom networks

☐ 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: 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:
```

☐ Ping instance-3&4 from instance-1

- i. Cannot ping outside of region since they are not on the same subnet and do not share the same virtual network switch like instance1&2 does.

☐ Take screenshot of all instances

cloud-Touche-ataouche

Search Products, resources, docs (/)

VM instances

CREATE INSTANCEIMPORT VMREFRESHCREATE SCHEDULEDELETEOPERATIONS

INSTANCES

INSTANCE SCHEDULES

VM instances are highly configurable virtual machines for running workloads on Google infrastructure. [Learn more](#)

Filter

Enter property name or value

	Status	Name	Zone	Recommendations	In use by	Internal IP	External IP	Connect	
	✓	<a href="#">instance-1</a>	us-east4-b			10.150.0.2 ( <a href="#">nic0</a> )	34.85.174.142 ( <a href="#">nic0</a> )	SSH	⌵⋮
	✓	<a href="#">instance-2</a>	us-west4-b			10.182.0.2 ( <a href="#">nic0</a> )	34.125.241.251 ( <a href="#">nic0</a> )	SSH	⌵⋮
	✓	<a href="#">instance-3</a>	us-central1-a			192.168.1.2 ( <a href="#">nic0</a> )	34.172.246.168 ( <a href="#">nic0</a> )	SSH	⌵⋮
	✓	<a href="#">instance-4</a>	eu-west1-d			192.168.5.2 ( <a href="#">nic0</a> )	34.140.21.78 ( <a href="#">nic0</a> )	SSH	⌵⋮

☐ Then visit VPC Network

Name	Region	Subnets	MTU	Mode	Internal IP ranges	External IP ranges	Secondary IPv4 ranges	Gateways	Firewall Rules	Global dynamic routing	Flow
custom-network1		2	1460	Custom	None				0	Off	
	us-central1	subnet-us-central-192			192.168.1.0/24	None	None	192.168.1.1			Off
	eu-west1	subnet-eu-west-192			192.168.5.0/24	None	None	192.168.5.1			Off
default		36	1460	Auto	None				4	Off	
	us-central1	default			10.128.0.0/20	None	None	10.128.0.1			Off
	eu-west1	default			10.132.0.0/20	None	None	10.132.0.1			Off
	us-west1	default			10.138.0.0/20	None	None	10.138.0.1			Off
	asia-east1	default			10.140.0.0/20	None	None	10.140.0.1			Off

7. Clean up