ECE358: Computer Networks

Winter 2018

Project 3: Encapsulation and Network Utilities

Date of submission: Mar 28, 2019

Submitted by:

Student ID: 20558988

Student name Jing, Lun

Waterloo Email address: [l7jing@edu.uwaterloo.ca](mailto:l7jing@edu.uwaterloo.ca)

Marks received:

Marked by:

Table of Contents

[Question 1. Protocol Header Analysis 3](#_Toc4618689)

[Question 2. arp 5](#_Toc4618690)

[Question 3. ifconfig 6](#_Toc4618691)

[Question 4. netstat 7](#_Toc4618692)

[Question 5. nslookup 8](#_Toc4618693)

[Question 6. ping 11](#_Toc4618694)

[Question 7. traceroute 12](#_Toc4618695)

# Question 1. Protocol Header Analysis

f8

485b 397e 6fc6 14da e974 0821 0800 4500

0054 0000 4000 4001 c777 8161 380b 8161

3864 0800 8cb8 de36 0001 1377 8b52 0000

0000 2573 0a00 0000 0000 1011 1213 1415

1617 1819 1a1b 1c1d 1e1f 2021 2223 2425

2627 2829 2a2b 2c2d 2e2f 3031 3233 3435

Ethernet header:

485b 397e 6fc6 14da e974 0821 0800

485b 397e 6fc6 : Ethernet destination address is 48 5b 39 7e 6f c6 (unicast).

14da e974 0821 : Ethernet source address is 14 da e9 74 08 21 (unicast).

0800 : The payload type is IP (0x0800)

IP header:

4500 0054 0000 4000 4001 c777 8161 380b 8161 3864

45: IPv4

45: IP header is 4\*5 = 20 bytes

00: (0 0 0 0 0 0 0 0 in binary)

0 0 0 0 0 0 0 0: the diagram has routine precedence.

0 0 0 0 0 0 0 0: Normal delay.

0 0 0 0 0 0 0 0: Normal throughput.

0 0 0 0 0 0 0 0: Normal Reliability.

0 0 0 0 0 0 0 0: Must be zero, reserved for Future Use.

0054: Total length of IP diagram is 84 (0x0054) bytes.

0000: The identification of this diagram is 0x0000 for fragmentation purpose.

4000: (0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0):

0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0: Don’t fragment.

0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0: More Fragment flag unset.

0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0: Fragment offset is 0.

This diagram cannot be fragmented and there is no fragment after this datagram, and this is the only fragment of the datagram.

40: Time to alive = 64 (0x40) the datagram may exist for at most 64 hops.

01: The Protocol on top is **ICMP**.

C777: The checksum of the datagram.

8161 380b: Source IP address is 129.97.56.11

8161 3864: Destination IP address is 129.97.56.100

ICMP header:

0800 8cb8 de36 0001

08: message type is echo.

00: code is zero.

8cb8: ICMP header checksum.

De36: Identifier.

0001: Sequence number.

Data:

1377 8b52 0000

0000 2573 0a00 0000 0000 1011 1213 1415

1617 1819 1a1b 1c1d 1e1f 2021 2223 2425

2627 2829 2a2b 2c2d 2e2f 3031 3233 3435

f18

0026 f1ff 0800 10bf 4878 4ef4 0800 4500

003c c9c2 4000 4006 c0e6 8161 44a5 3212

b7fa da1f 0050 7ee0 c6bd 0000 0000 a002

16d0 5188 0000 0204 05b4 0402 080a 0008

0f7f 0000 0000 0103 0307

Ethernet header:

0026 f1ff 0800 10bf 4878 4ef4 0800

0026 f1ff 0800: Ethernet destination address is 00 26 f1 ff 08 00 (unicast).

10bf 4878 4ef4: Ethernet source address is 10 bf 48 78 4e f4 (unicast).

0800 : The payload type is IP (0x0800)

IP header:

4500 003c c9c2 4000 4006 c0e6 8161 44a5 3212 b7fa

45: IPv4

45: IP header is 4\*5 = 20 bytes

00: (0 0 0 0 0 0 0 0 in binary)

0 0 0 0 0 0 0 0: the diagram has routine precedence.

0 0 0 0 0 0 0 0: Normal delay.

0 0 0 0 0 0 0 0: Normal throughput.

0 0 0 0 0 0 0 0: Normal Reliability.

0 0 0 0 0 0 0 0: Must be zero, reserved for Future Use.

003c: Total length of IP diagram is 60 (0x003c) bytes.

C9c2: The identification of this diagram is 0xc9c2 for fragmentation purpose.

4000: (0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0):

0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0: Don’t fragment.

0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0: More Fragment flag unset.

0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0: Fragment offset is 0.

This diagram cannot be fragmented and there is no fragment after this datagram, and this is the only fragment of the datagram.

40: Time to alive = 64 (0x40) the datagram may exist for at most 64 hops.

06: The Protocol on top is **TCP**.

c0e6: The checksum of the datagram.

8161 44a5: Source IP address is 129.97.68.165

3212 b7fa: Destination IP address is 50.18.183.250

TCP header:

da1f 0050 7ee0 c6bd 0000 0000 a002

16d0 5188 0000 0204 05b4 0402 080a 0008

0f7f 0000 0000 0103 0307

da1f: The source port is 55839.

0050: The Destination port is 80

7ee0 c6bd: The Seq. no. is 2128660157.

0000 0000: The Ack. No. is 0.

a0: Data offset is 40 (10 \* 4)bytes. This is the length of the TCP header.

02: (0 0 0 0 0 0 1 0):

Flags:

URG: 0 ACK: 0 PSH: 0 RST: 0 SYN: 1 FIN: 0

The number in the synchronize sequence numbers is valid.

16d0: the receiver window size is 5840 (0x16d0) byte.

5188: Checksum of the whole TCP segment.

0000: Urgent pointer (Not used in this segment)

0204 05b4 0402 080a 0008 0f7f 0000 0000 0103 0307: Options data

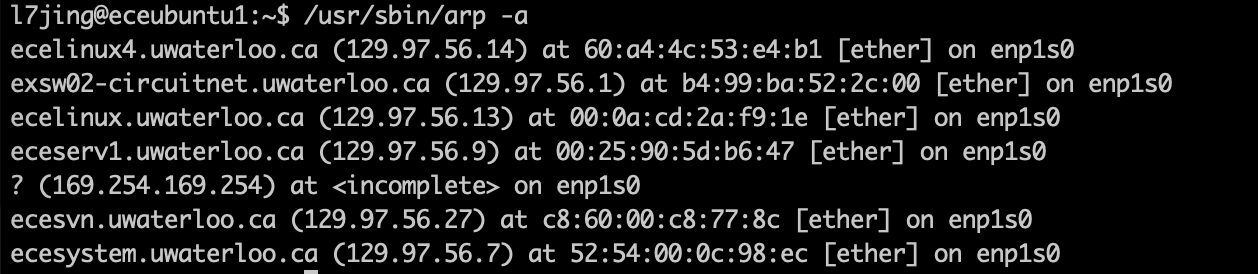
Data:

None data for this datagram.

# Question 2. arp

The arp command is used to check, add, and remove address resolution protocol for the device.

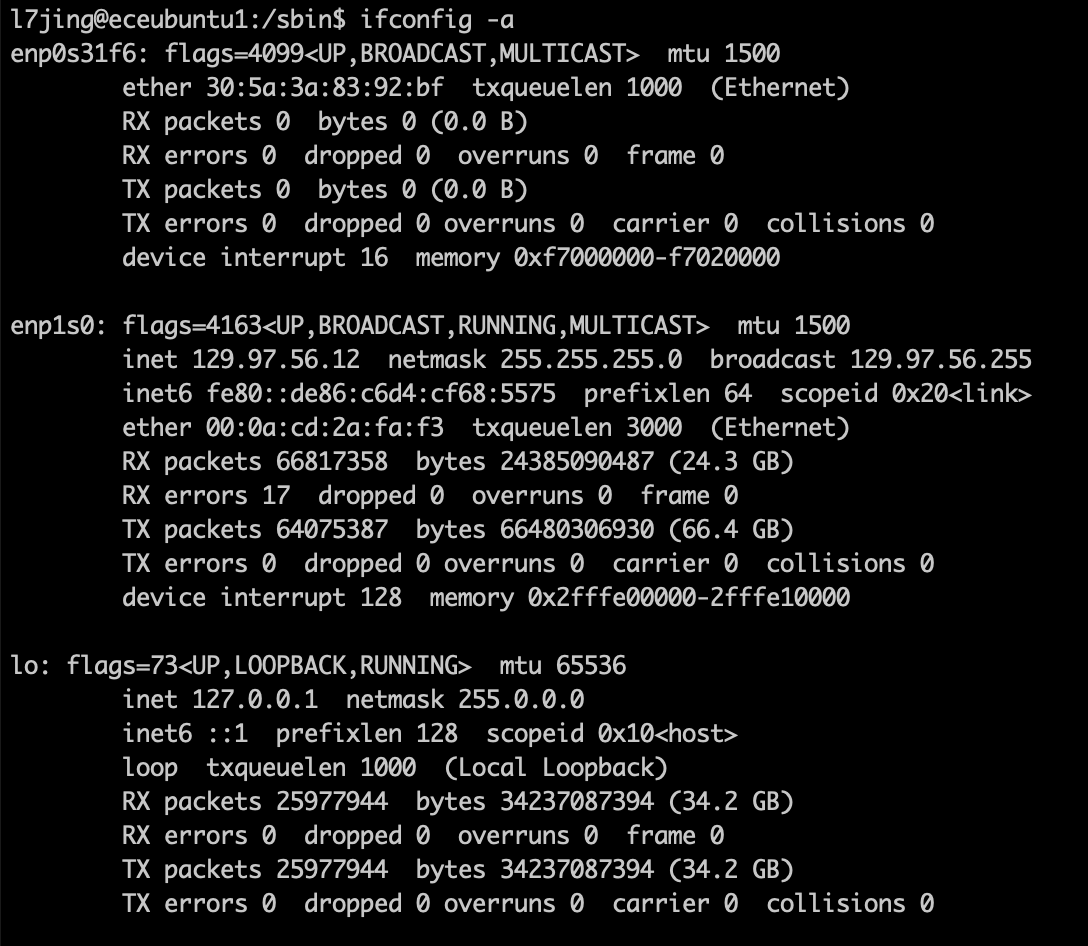
From the following diagram, it shows all the current arp entries. For each entry, it includes the information of its domain name, IP address, MAC address and corresponding network interface. For example, the first entry’s domain name is ecelinux4.uwaterloo.ca, its IP address is 129.97.56.14, with MAC address 60:a4:4c:53:e4:b1, and the interface is enp1s0.



# Question 3. ifconfig

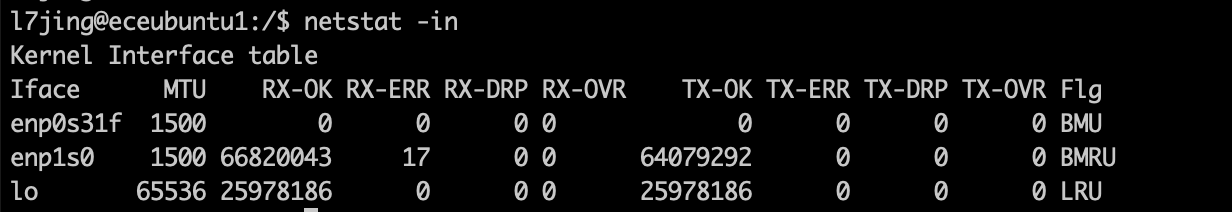
The ifconfig is used for configuring the IP address and netmask of the network interfaces, it may change, enable or disable the interface.

Here, in the following diagram, the enp0s31f6, enp1s0 and lo are the names of active network interfaces. For each interface, it provides some information, for example, MAC address, internet IP address and broadcast address. It also includes the information on packets transmission, RX is for received packets and TX is for transmitted packets.

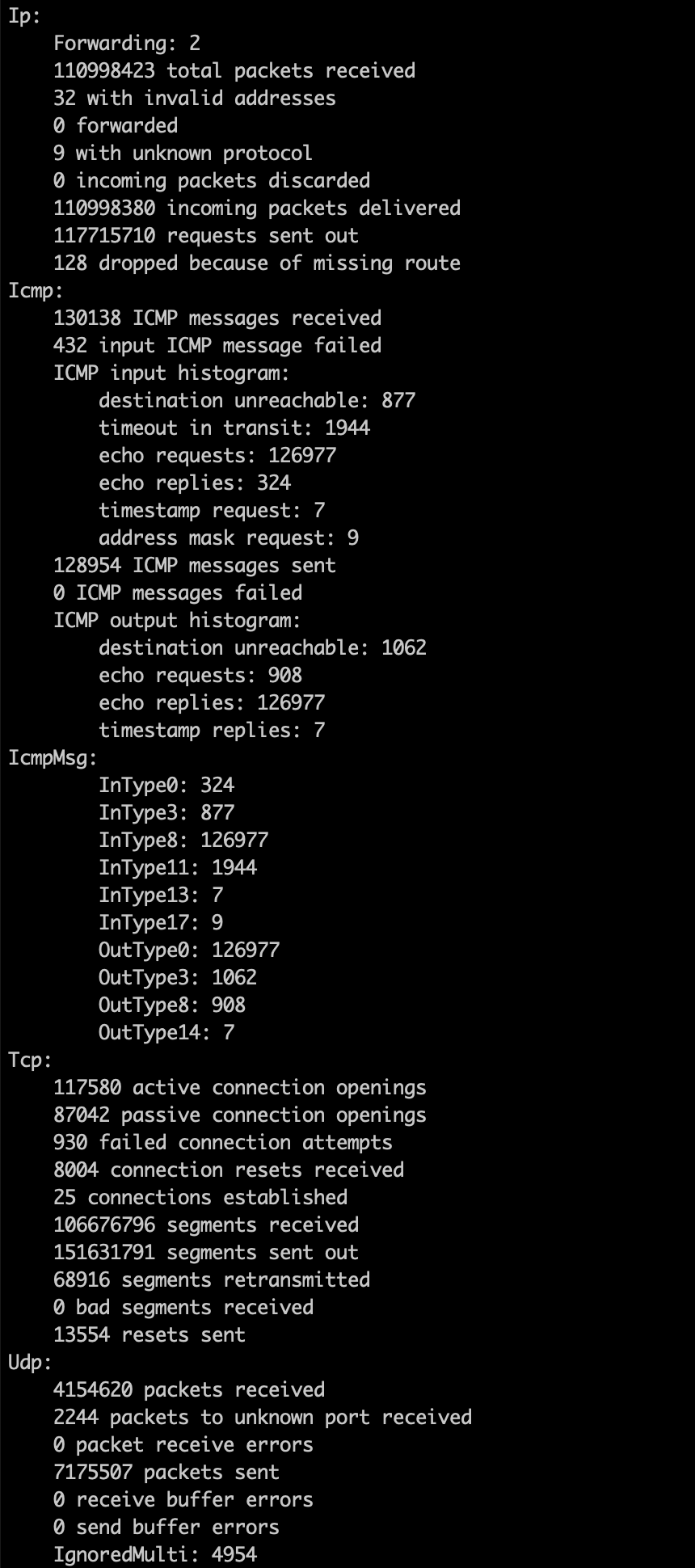
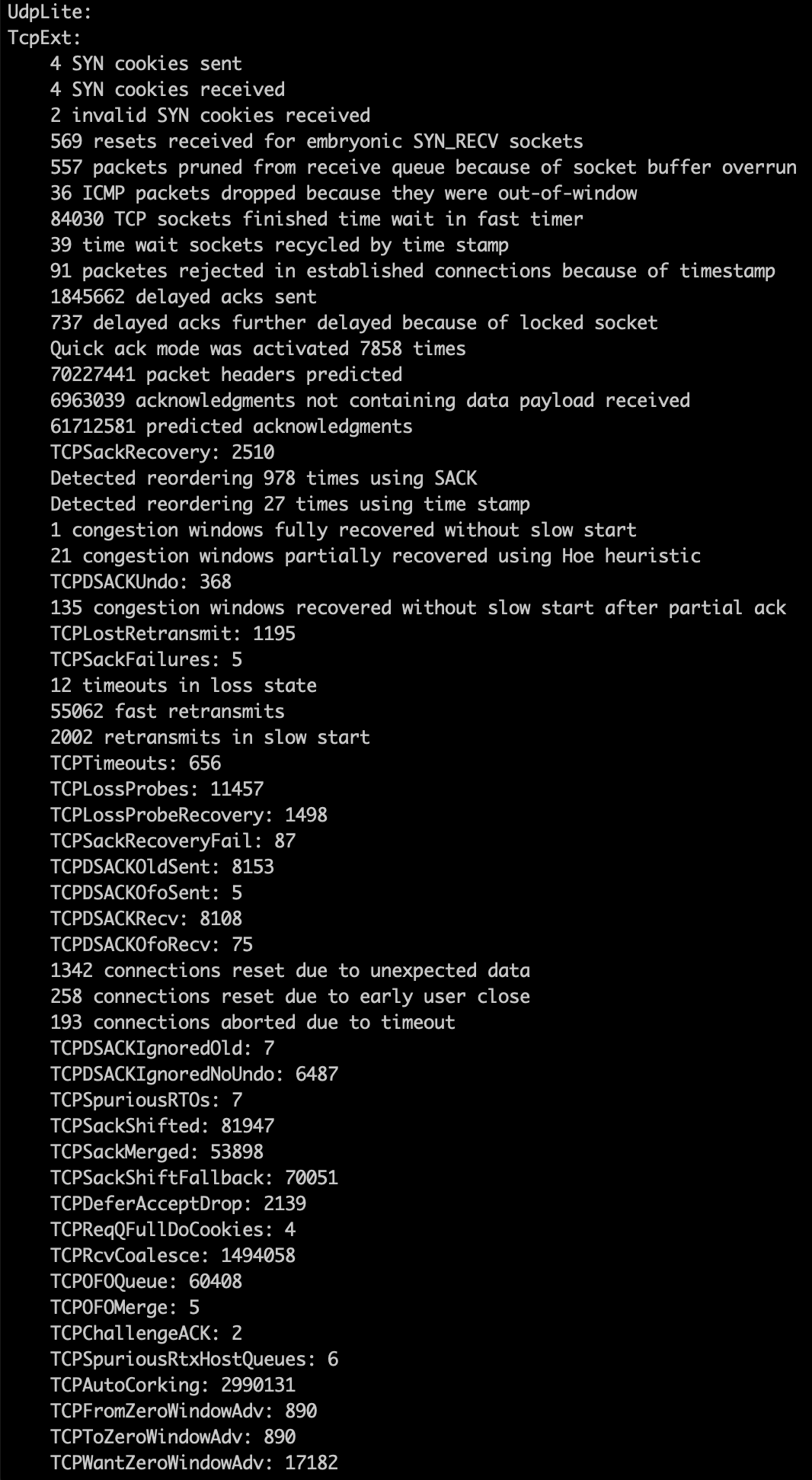


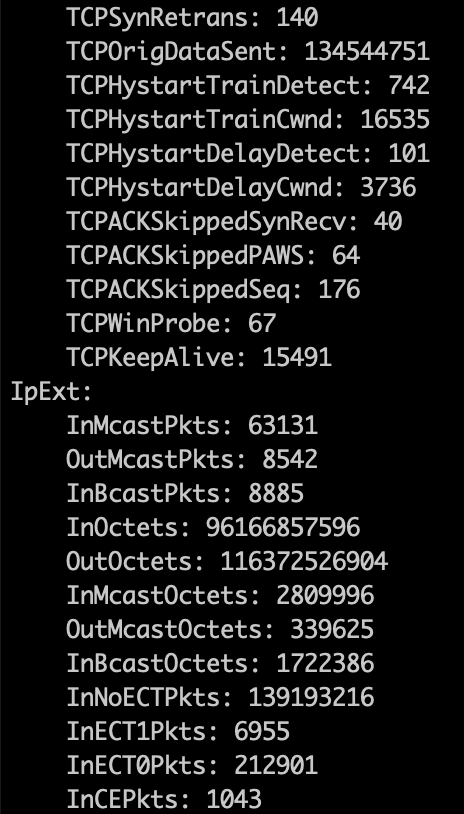
# Question 4. netstat

netstate provides the information and statistics of the network interfaces. For example, for the interface enp1s0, the maximum transmission unit (MTU) is 1500 byte. There are 66820043 packets been received without error, and 17 packets been received with error detected. And it also transmitted 25978186 packets successfully. The Flg denotes the flags of the interface.

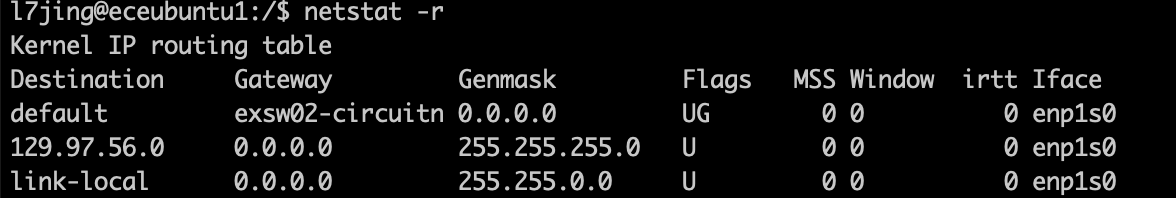


By using netstat -s, it will show the detailed information and statistics for different protocols, including IP, ICMP, TCP etc.



Using netstat -r will display the routing table for different destination IP addresses. Gateway basically describe the next hop to reach the destination. Genmask is the net mask. Flags represents flags, where U stands for “route is up”, G stands for “using gateway”. MSS is the maximum segment size for TCP connections over the route. Window is the default window size of the route. Irtt stands for initial round trip time. Iface is the network interface of the route.



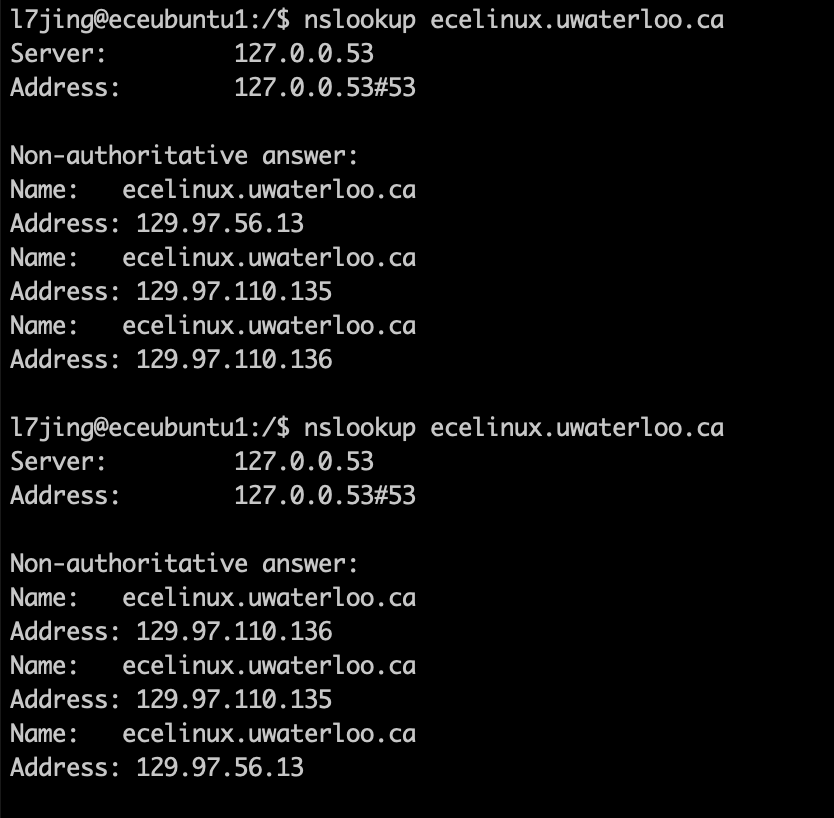
# Question 5. nslookup

Using nslookup can show the internet IP addresses and domain names for the host in parameter.

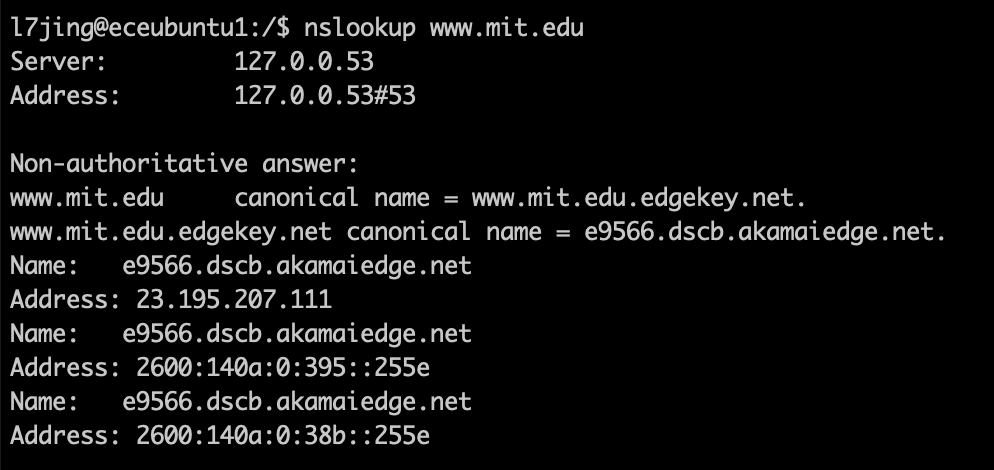
The server is the address of our own system’s DNS. #53 means we are communicating with it in port 53.

There are three answers for ecelinux.uwaterloo.ca, it means that ecelinux.uwaterloo.ca will distribute the loads into these three different addresses. The Non-authoritative answer means the current server do not have the original source files of the domain’s zone.

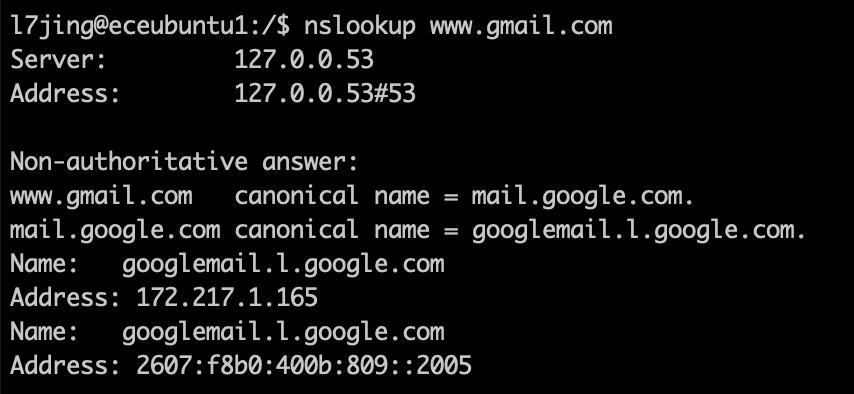
The only difference between the two requests is the order of the addresses are changed, therefore, the order of the answer should not affect the results.



We can see that [www.mit.edu](http://www.mit.edu) also distributes the access queries into three different addresses.



Whereas [www.gmail.com](http://www.gmail.com) has domain names mail.google.com and googlmail.l.google.com, and it has two different addresses.



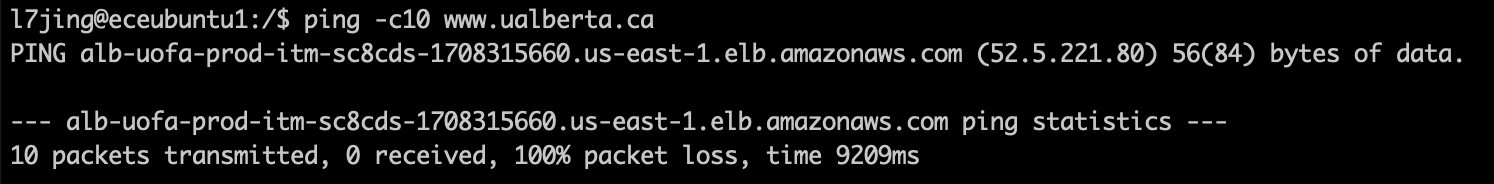
For the [www.facebook.com](http://www.facebook.com), the domain name is star-mini.c10r.facebook.com, and it has two different addresses.



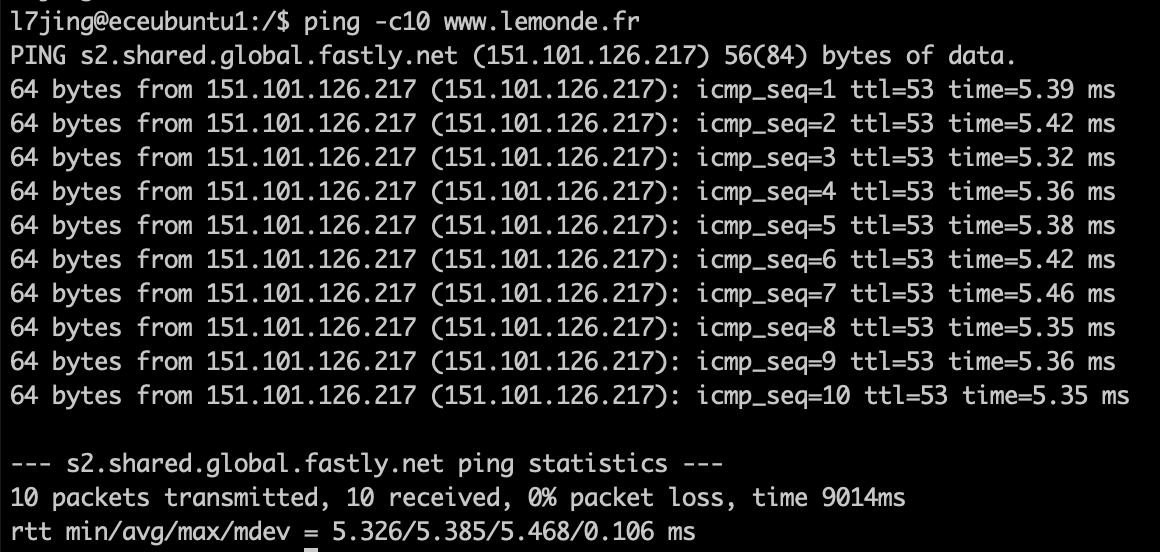
# Question 6. ping

Using ping can help us to check if network data packets could be distributed on the address provided. Basically means if we can send and receive packets from the destination address.

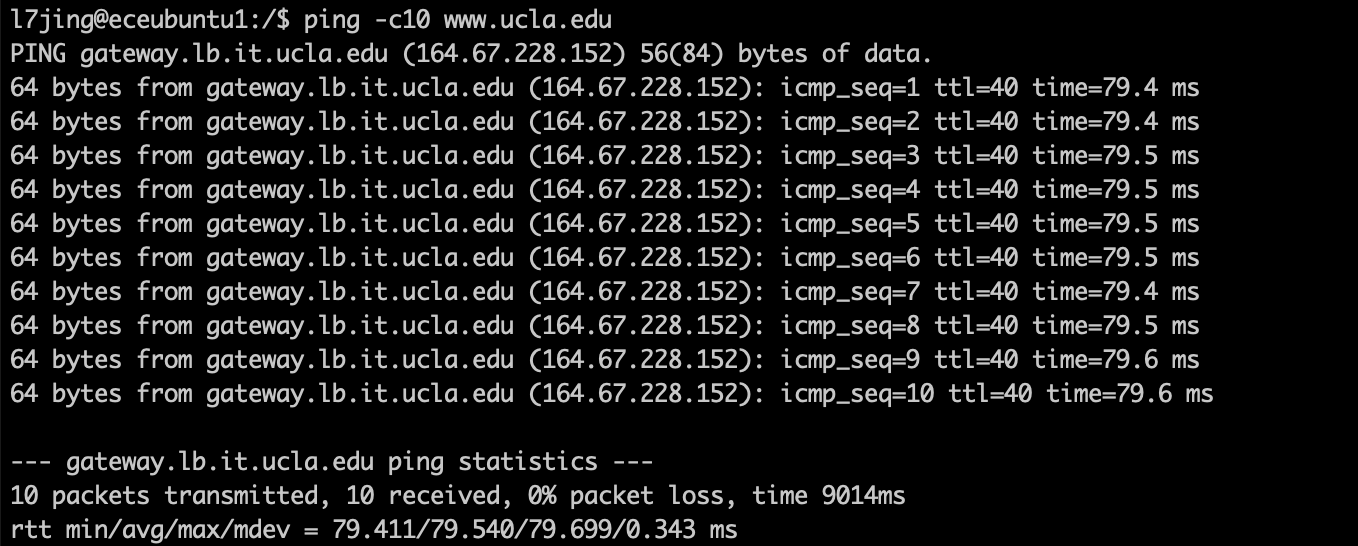
By using ping -c10 *hostname*, we will send 10 packets to the destination host to check if we can access the host and how long will it take to connect the host. In the first example, we did not transmit any data pack successfully. But we can actually access the [www.ualberta.ca](http://www.ualberta.ca) via web browser. The reason is that the [www.ualberta.ca](http://www.ualberta.ca) probable block the ping assessment from outside.



To connect to [www.lemonde.fr](http://www.lemonde.fr), the average time is 5.358 ms. And we can access [www.lemonde.fr](http://www.lemonde.fr) via web browser.



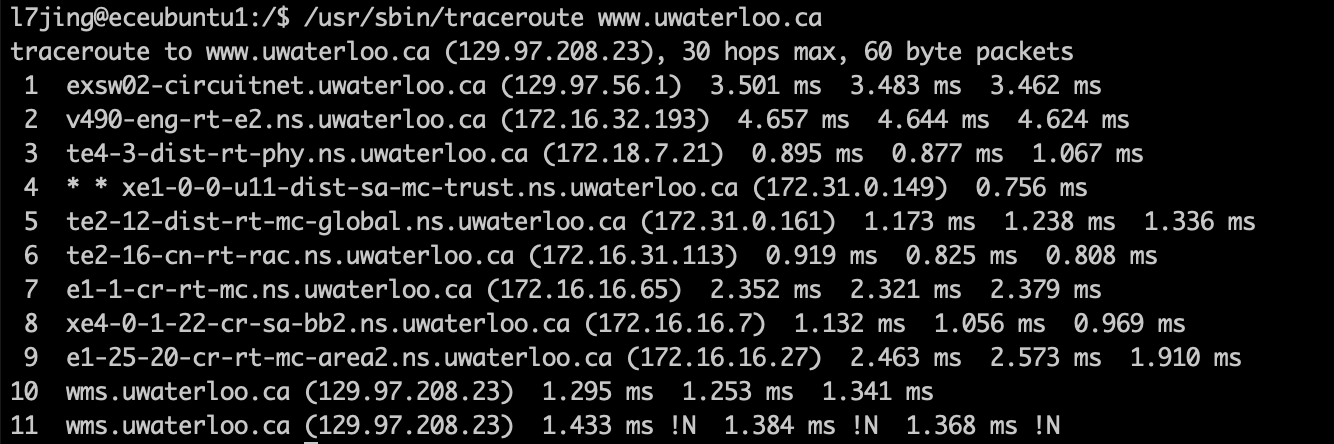
To connect to [www.ucla.edu](http://www.ucla.edu), the average time is 79.540 ms. And we can access [www.ucla.edu](http://www.ucla.edu) via web browser.



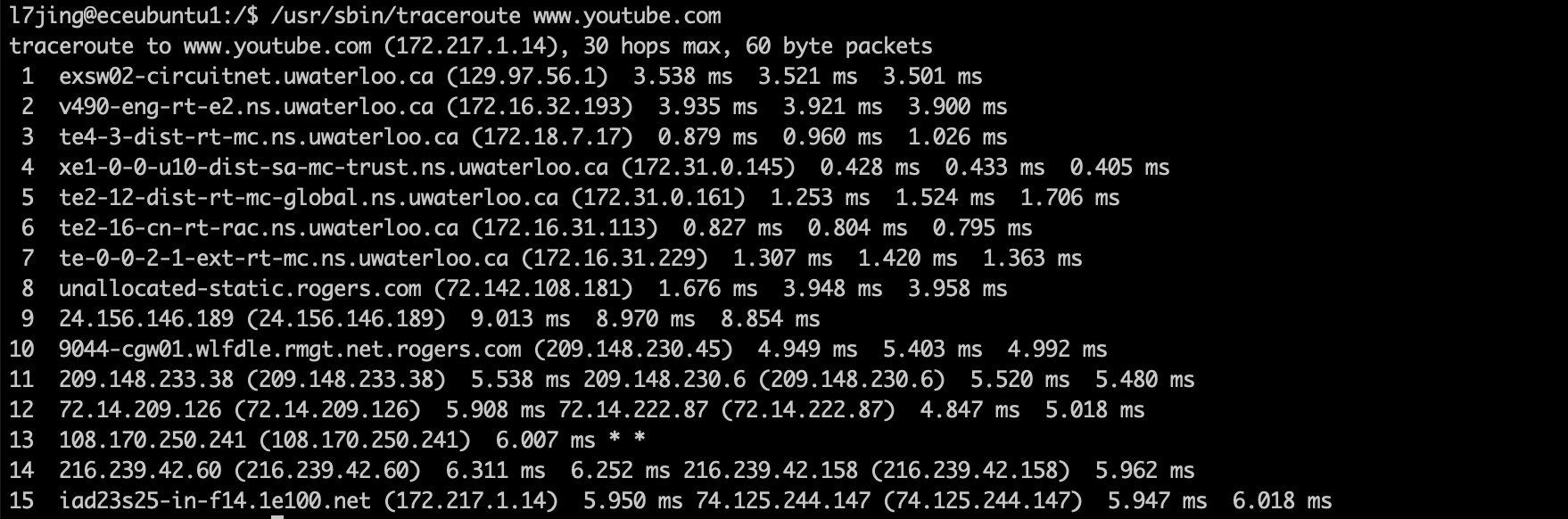
# Question 7. traceroute

Using traceroute can find out the intermediate hops that required to transmit a packet from the starting machine to the ending location.

To access the [www.uwaterloo.ca](http://www.uwaterloo.ca), there are 11 intermediate hops



To access [www.youtube.com](http://www.youtube.com), there are 15 intermediate hops.



To access [www.nytimes.com](http://www.nytimes.com), since we track maximum 30 hops, it seems that we did not reach [www.nytimes.com](http://www.nytimes.com) within 30 hops, and starts to lose information from the 12th hop.

