CSE 232: Programming Assignment 1
Using Command-Line Utilities for Network Debugging

Rohak Kansal
Roll No: 2022412

Due Date: August 30, 2024

Contents

1 IP Address of Network Interface

Command Used:

`ifconfig`

Screenshot:

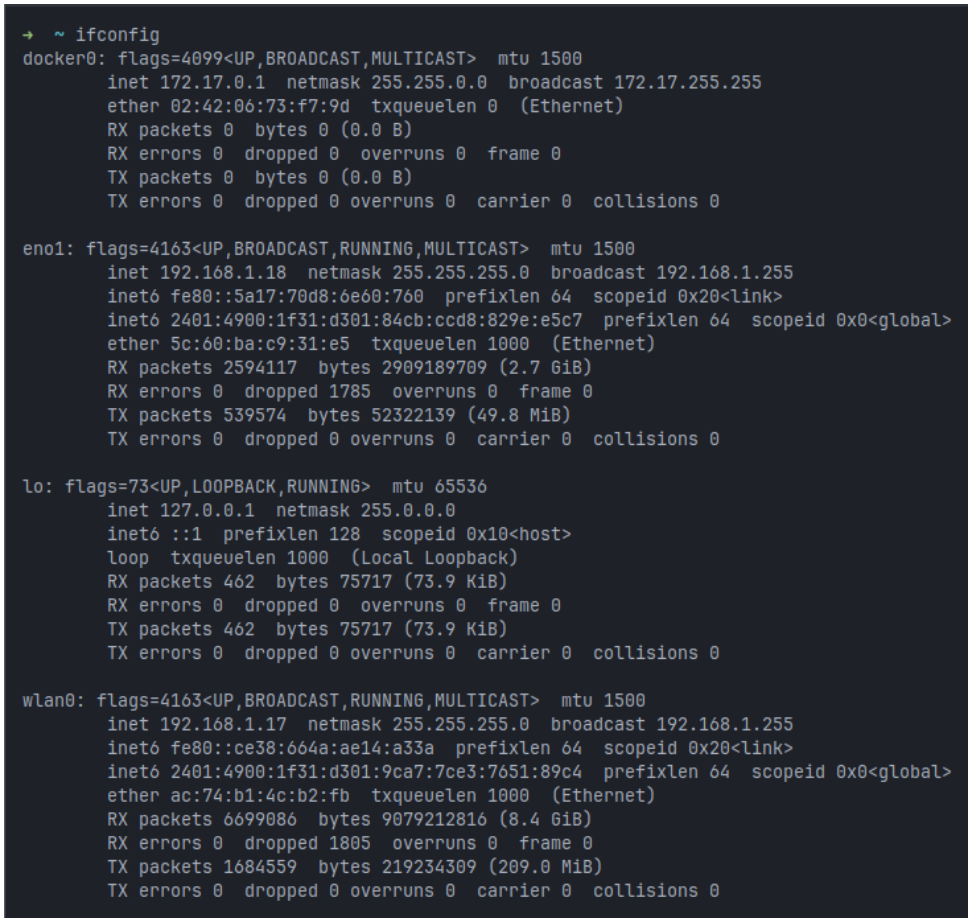

Figure 1: IP address of network interface

2 IP Address from Webpage

Website Used: `https://www.whatismyip.com`

Observation: The IP address on terminal `192.168.1.17` differs from the IP address on the website `122.179.207.70`.

Explanation: The IP address from `ifconfig` is a private IP address assigned to my device within the local network (LAN). The IP address shown on the website is the public IP address assigned to my network by the Internet Service Provider (ISP). This difference occurs due to Network Address Translation (NAT), which allows multiple devices on a local network to share a single public IP address when accessing the internet.

3 Changing the IP Address

Command Used:

```
sudo ip addr show wlan0
sudo ip addr add 192.168.1.100/24 dev wlan0
sudo ip addr del 192.168.1.17/24 dev wlan0
sudo ip addr show wlan0
sudo ip addr del 192.168.1.100/24 dev wlan0
sudo ip addr add 192.168.1.17/24 dev wlan0
sudo ip addr show wlan0
```

Screenshot:

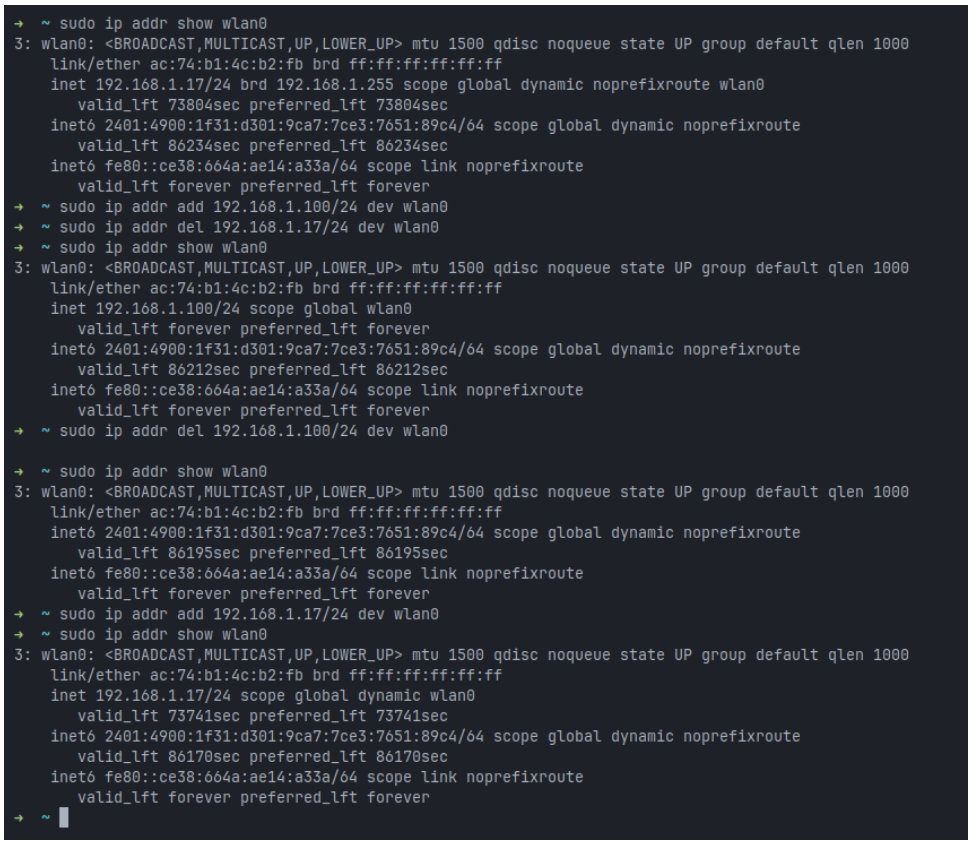

Figure 2: IP address change

4 Setting up a TCP Client/Server Connection

Command Used:

```
nc -v -l -p 1234 (on server)
nc localhost 1234 (on client)
```

Screenshot:

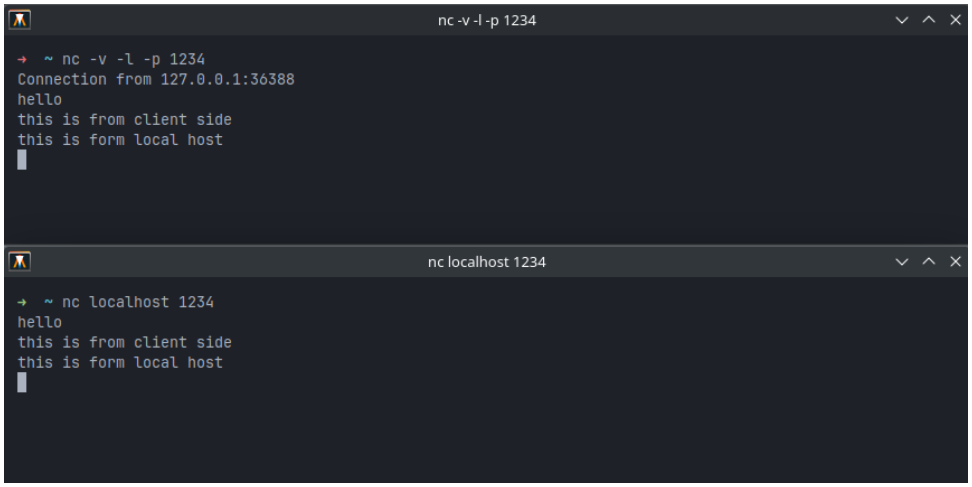

Figure 3: TCP client/server connection

5 TCP Connection State

Command Used:

```
ss -an | grep 1234
```

Screenshot:

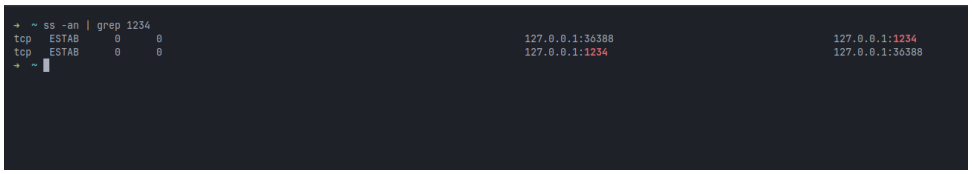

Figure 4: TCP connection state

6 Authoritative nslookup Result

Command Used:

```
nslookup
set type=ns
google.in
server ns3.google.com
google.in
```

Screenshot:

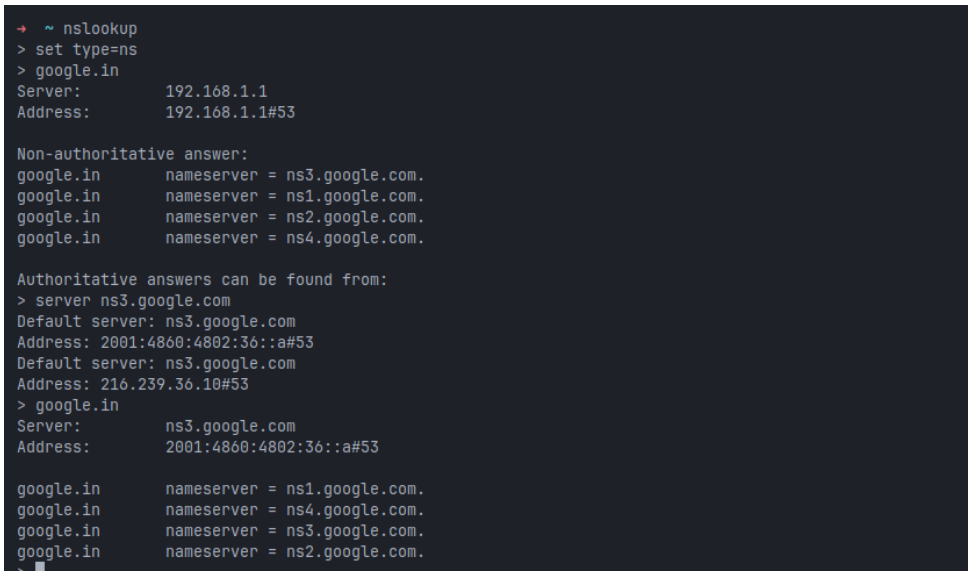

Figure 5: Authoritative nslookup result

Explanation: The authoritative DNS record for `google.in` was obtained using `nslookup`. First, the query type was set to `NS` to find its authoritative name servers. Then, `ns3.google.com` was used as the DNS server to retrieve the authoritative records directly from Google's name server.

7 Time to Live (TTL) for a Website

Command Used:

```
nslookup -debug aliexpress.com
```

TTL Observation: The Time to Live (TTL) for the DNS entry of `aliexpress.com` on the local DNS server is 571 seconds.

Explanation: The TTL value indicates the remaining time (in seconds) before the DNS entry for `aliexpress.com` will expire from the local DNS cache. After 571 seconds, the entry will be considered stale, and the DNS server will need to query an authoritative DNS server to refresh the information. This value controls how long a DNS resolver can cache a response before needing to check for an updated record.

Screenshot:

```
➜  ~ nslookup -debug aliexpress.com
Server:         192.168.1.1
Address:        192.168.1.1#53

------------
    QUESTIONS:
        aliexpress.com, type = A, class = IN
    ANSWERS:
    ->  aliexpress.com
        internet address = 47.246.173.237
        ttl = 571
    ->  aliexpress.com
        internet address = 47.246.173.30
        ttl = 571
    AUTHORITY RECORDS:
    ADDITIONAL RECORDS:
------------
Non-authoritative answer:
Name:   aliexpress.com
Address: 47.246.173.237
Name:   aliexpress.com
Address: 47.246.173.30
------------
    QUESTIONS:
        aliexpress.com, type = AAAA, class = IN
    ANSWERS:
    AUTHORITY RECORDS:
    ->  aliexpress.com
        origin = ns1.alibabadns.com
        mail addr = hostmaster.alibabadns.com
        serial = 2018051019
        refresh = 3600
        retry = 1200
        expire = 86400
        minimum = 360
        ttl = 211
    ADDITIONAL RECORDS:
------------
```

Figure 6: Time to Live (TTL)

8 Traceroute to google.in

Command Used:

```
traceroute google.in
```

8.1 IP Addresses and Average Latency to Each Intermediate Host

- **192.168.1.1**: Average latency = ≈ 0.802 ms
- **125.18.73.17**: Average latency = ≈ 6.474 ms
- **125.21.160.21**: Average latency = 6.665 ms
- **182.79.152.79**: Average latency = ≈ 10.440 ms
- **142.250.161.56**: Average latency = ≈ 11.262 ms
- **172.253.67.100**: Average latency = ≈ 8.998 ms
- **192.178.83.220**: Average latency = ≈ 9.938 ms
- **142.250.234.126**: Average latency = ≈ 27.985 ms
- **192.178.110.245**: Average latency = ≈ 22.715 ms
- **142.250.226.135**: Average latency = ≈ 31.583 ms
- **142.250.214.103**: Average latency = ≈ 29.811 ms
- **142.250.182.228**: Average latency = ≈ 27.476 ms

Screenshot:

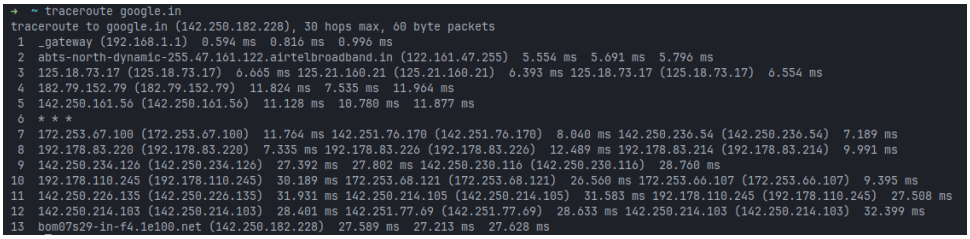

Figure 7: Traceroute to google.in

9 Ping Latency to google.in

Command Used:

```
ping -c 50 google.in
```

Screenshot:

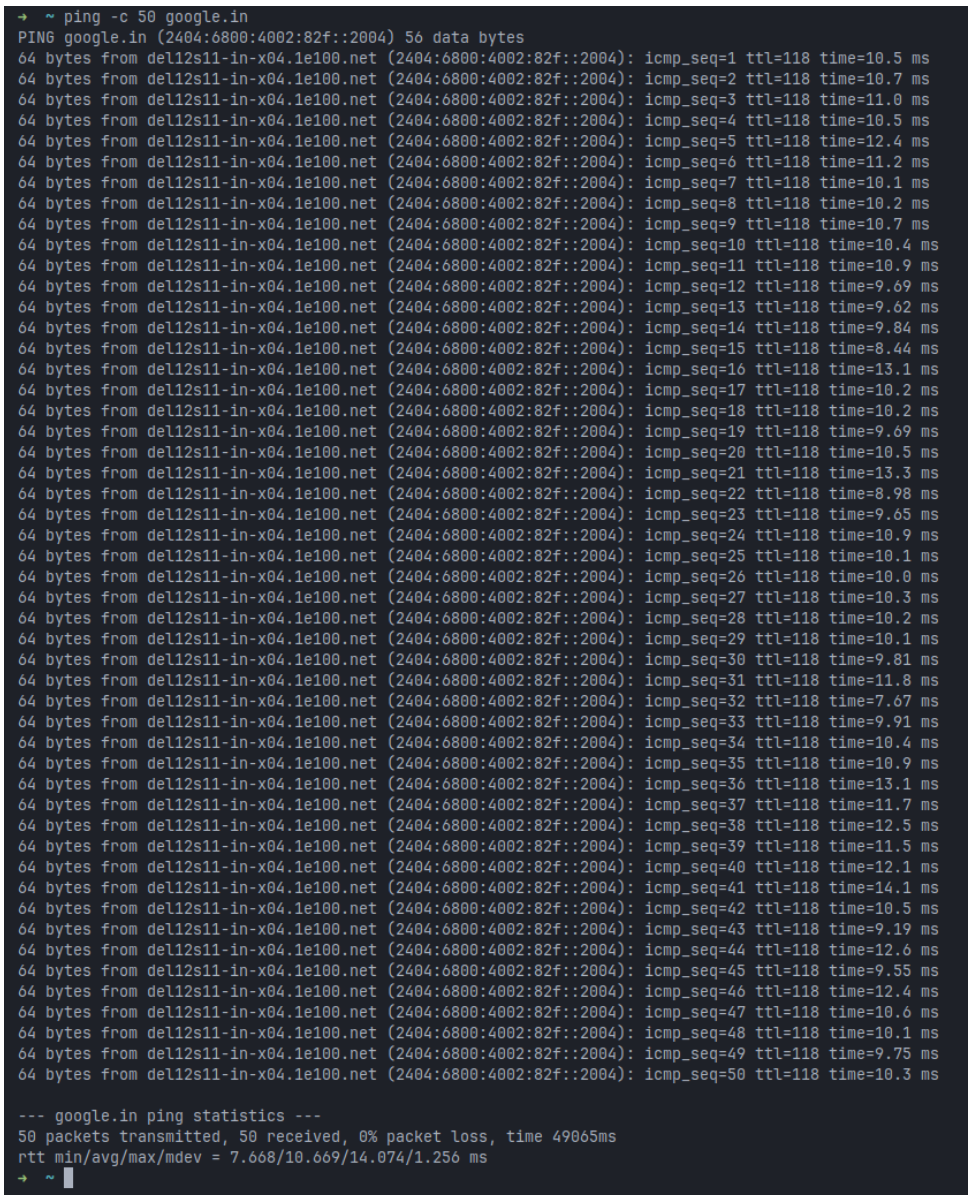

Figure 8: Ping latency to google.in

Average Latency: The average latency to `google.in` is **10.669 ms**.

10 Latency Comparison

10.1 Sum of Latencies from Intermediate Hosts

Total Latency: The sum of the latencies from all intermediate hosts is **193.149 ms**.

10.2 Comparison with Ping Latency

Ping Latency: The average latency to `google.in` from the `ping` command is **10.669 ms**.

10.3 Explanation

The sum of the latencies from the intermediate hosts is much higher than the average latency observed from the `ping` command. This is because the `ping` command measures the round-trip time, which doesn't directly add up the times from each hop. The traceroute provides insight into the latency at each hop, but these latencies don't sum to give the round-trip time directly.

11 Maximum Ping Latency

11.1 Maximum Latency from Intermediate Hosts

Maximum Latency: The maximum latency among the intermediate hosts is **31.583 ms** from IP address `142.250.226.135`.

11.2 Comparison with Ping Latency

Ping Latency: The average latency to `google.in` from the `ping` command is **10.669 ms**.

11.3 Explanation

The maximum latency from the intermediate hosts is higher than the average latency observed from the `ping` command. This is because the maximum latency reflects the delay at a specific hop, while the average `ping` latency measures the overall round-trip time. These two metrics serve different purposes and thus may differ significantly.

12 Multiple Entries for a Single Hop

Explanation: Multiple entries for a single hop in the `traceroute` output indicate the presence of multiple potential paths or routes through the network at that particular hop. This is typically due to load balancing, where traffic is distributed across several paths to optimize network performance, or because of variations in ICMP responses from different interfaces or routes.

13 Ping Latency to stanford.edu

Command Used:

```
ping -c 50 stanford.edu
```

Screenshot:

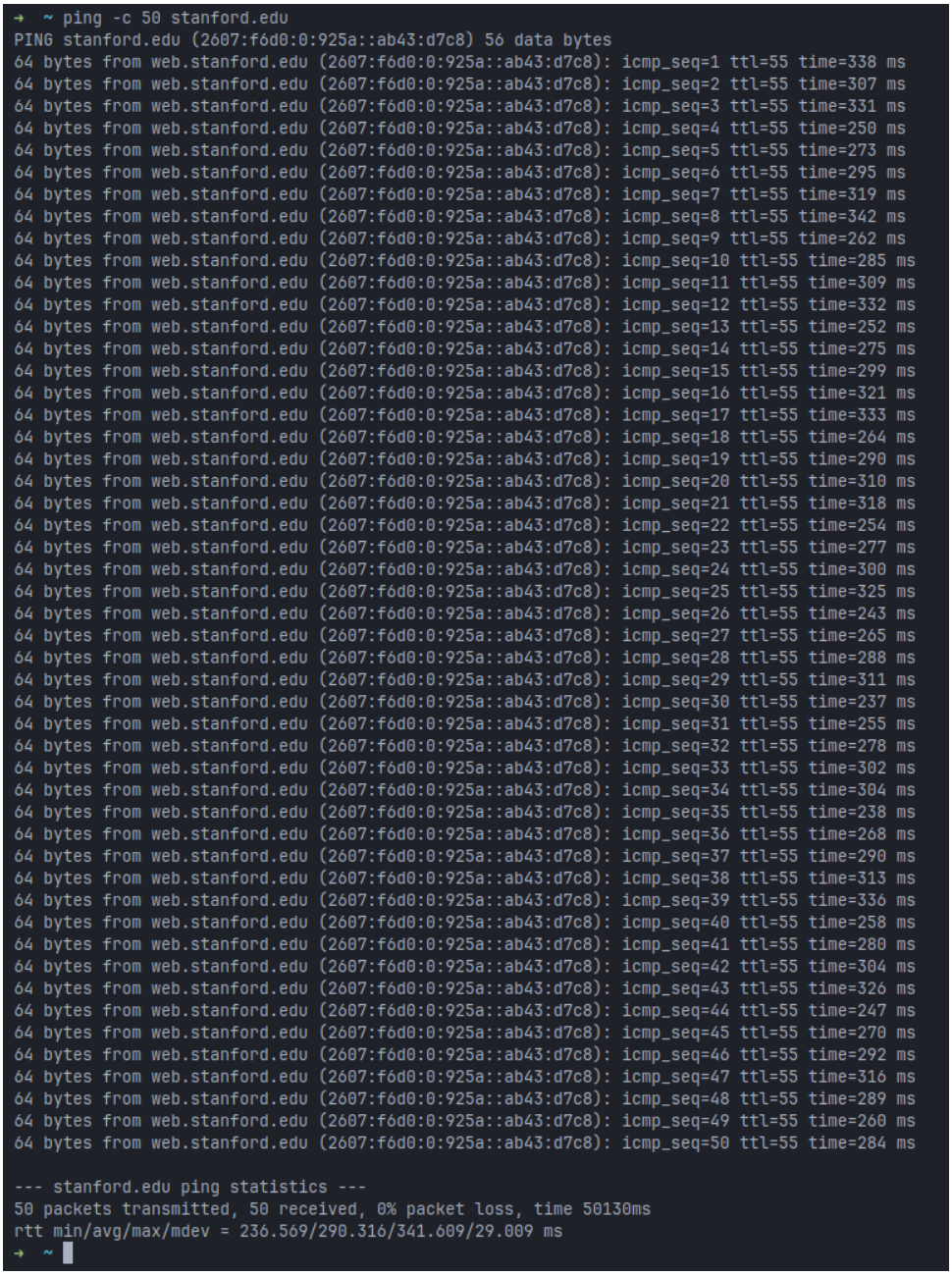

Figure 9: Ping latency to stanford.edu

Average Latency: The average latency to `stanford.edu` is **290.316 ms**.

14 Traceroute to stanford.edu

Command Used:

```
traceroute stanford.edu
```

Screenshot:

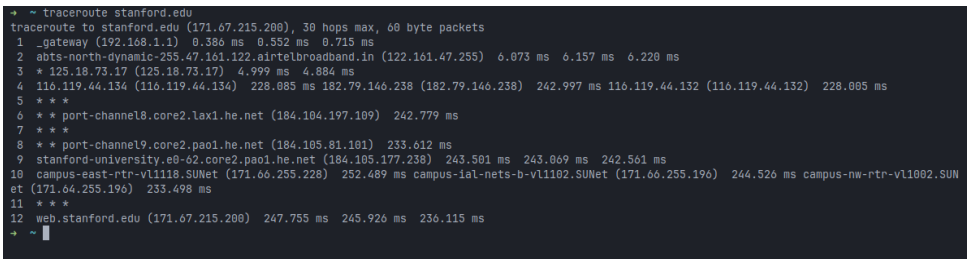

Figure 10: Traceroute to stanford.edu

14.1 Observation

Number of Hops:

- `google.in`: 13 hops
- `stanford.edu`: 12 hops

14.2 Comparison

The traceroute to `stanford.edu` has one fewer hop compared to the traceroute to `google.in`. This indicates a slightly shorter network path to `stanford.edu` in terms of the number of devices traversed.

15 Latency Difference Explanation

Explanation: The latency difference between `google.in` and `stanford.edu` is primarily due to geographical distance and network routing. `stanford.edu` is located in the United States, which is significantly farther from the client compared to `google.in`, likely located in India or a nearby region. The increased distance and the complexity of international network paths result in higher latency for `stanford.edu`. Additionally, factors such as server load and intermediate network congestion may further contribute to the observed latency differences.

16 Making Ping Fail for 127.0.0.1

Command Used:

```
sudo iptables -A OUTPUT -p icmp --icmp-type echo-request -j DROP
```

Screenshot:

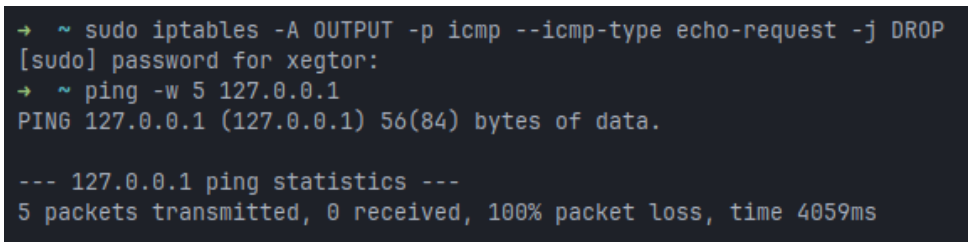

Figure 11: Ping failure for 127.0.0.1

16.1 Explanation

To make the `ping` command fail for `127.0.0.1` with 100% packet loss, I used the `iptables` command to drop all ICMP echo request packets sent from my system. This effectively blocks all `ping` requests to `127.0.0.1`, resulting in 100% packet loss.