Assignment 3
Computer Networks

Vikas Gola : 2016UCS0023

September 2, 2018

Question 1 Enumerate the steps and briefly discuss how the utility traceroute works using an illustrative website as the argument to it. In your explanation of the tool operation discuss the answers to following questions w. r. to traceroute

- What if there was no TTL field in the invocation of the traceroute at all?
- How will the routers in between determine whether the TTL value limit has reached ?
- Should an intermediate router that receives a traceroute packet always respond with an ICMP TTL exceeded message ? If the answer is a yes, reason why and if the answer is a no, then argue how do we know the address of all the routers/hops in between us and the destination ?
- Why does traceroute make use of a destination UDP port number which is invalid - i.e. it sends a packet to a UDP port in the range 33434 to 33534 ?
- How do we know the address of all the routers/hops in between us and the destination when using the traceroute?
- How is traceroute latency calculated?

Answer Traceroute is a network diagnostic tool to examine the path taken by the packets from your computer to destination to determine the problems in network. Traceroute uses TTL which stands for Time To Live which is in IP packet, TTL is used to prevent the Loop in a network, When IP packet forward from one router to another, It decrements the TTL Value by one, When the TTL value will be Zero, The packet will be discarded.

- If there was no TTL field in the invocation of the traceroute at all, the packet will run and go forever or can say flow endlessly from one router to another and goes forever searching for the destination machine.
- TTL limit is set by the sending host in header of packet which is 8 digit binary field which is decreased by the all router and checked if limit has been reached or not.
- No, sometimes routers set "time exceeded" message to that which has been killed and in that case no information return and we don't able to identify.

- Traceroute make use of destination UDP port number which is invalid so that it can know that final destination has been reached by getting the message "ICMP Destination/PORT Unreachable".
- Traceroute sends the packet with starting TTL 1, 2 , 3 and so on till we don't reach the final destination. Each time traceroute send the packet it gets the "ICMP TTL exceeded messages" by that router which contains the IP of that router and hence it get to know the IP's.
- the route is recorded as the round-trip times of the packets received from each successive host (remote node) in the route the sum of the mean times in each hop is a measure of the total time spent to establish the connection.

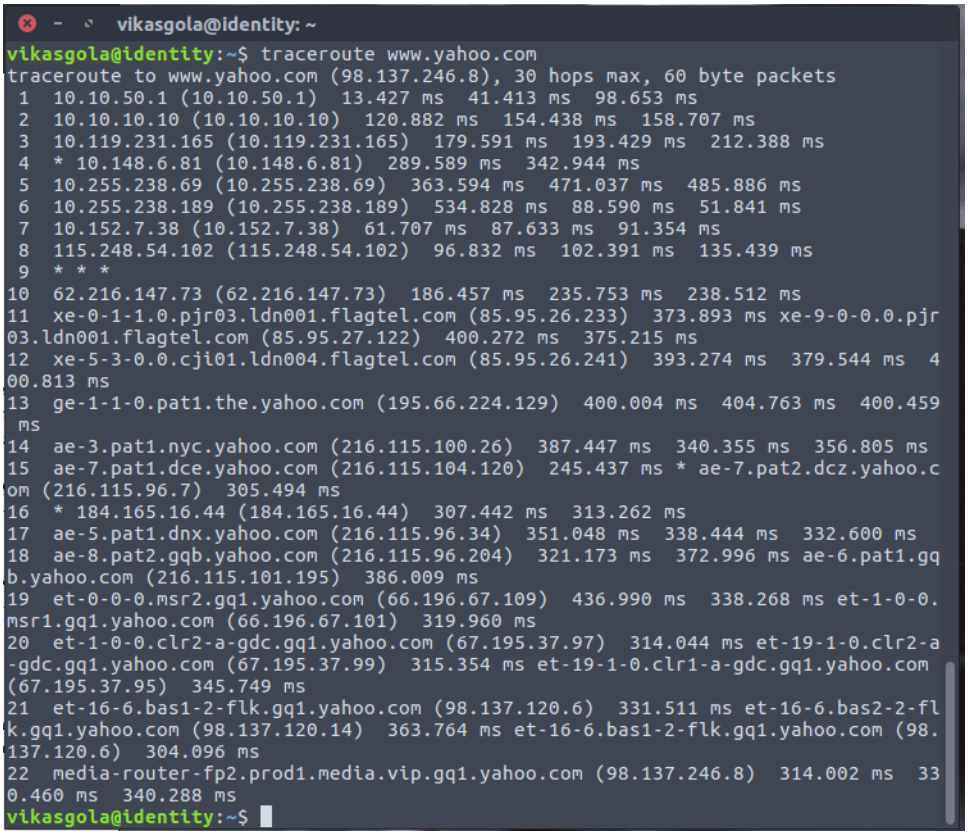
Question 2 Execute the traceroute command with www/yahoo.com as argument. Write down the IP address of yahoo.com that was used for the trace route. Determine the number of iterations required to determine route. Enlist the IP addresses of all the machines between the source and the destination. What is the average round trip time of the packet that reached the destination ?

Answer IP address of the www.yahoo.com is 98.137.246.8. 22 iterations are required to determine the route. IP address of the all machines

The average round trip time of the packet that reached the destination is 328.25.

- 10.10.50.1
- 10.10.10.10
- 10.119.231.165
- 10.148.6.81
- 10.255.238.69
- 10.255.238.189
- 10.152.7.38
- 115.248.54.102

- * * *
- 62.216.147.73
- 85.95.26.233
- 85.95.26.241
- 195.66.224.129
- 216.115.100.26
- 216.115.104.120
- 184.165.16.44
- 216.115.96.34
- 216.115.96.204
- 66.196.67.109
- 67.195.37.97
- 98.137.120.6
- 98.137.246.8



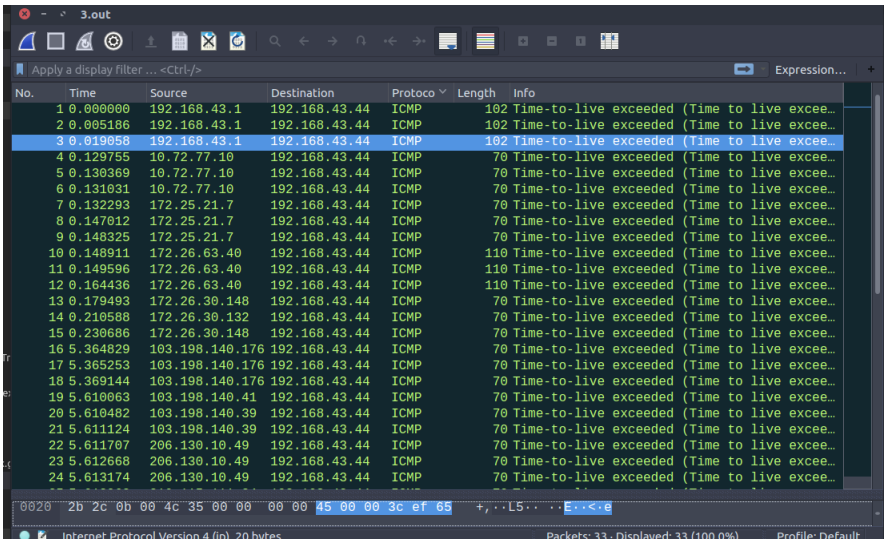
Question 3 With respect to the question no 2, run traceroute on one window of your OS and run tcpdump on the other window. Analyze the output of tcpdump. Answer the following questionsm giving appropriate hihglighted snapshots in support of your answer :

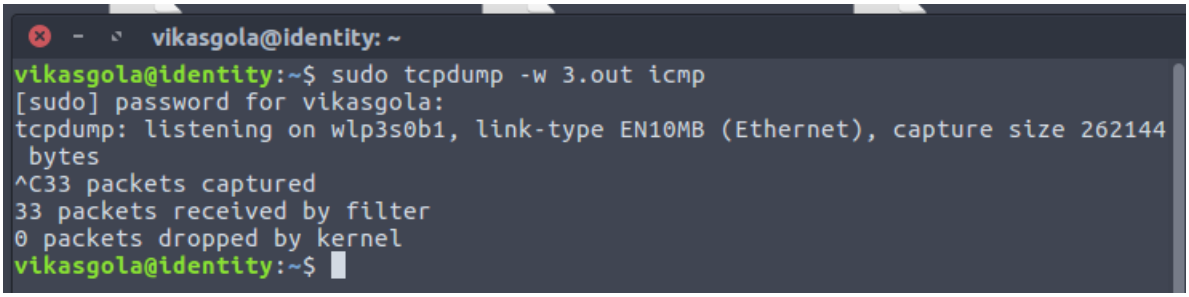
- How many packets are send by traceroute in each iteration ? How can you prove this using the tcpdump output.
- Consider one specific iteration of traceroute invocation/iteration. For this specific iteration, what are the individual round trip times of each of the three probes sent ? What is the average round trip time ? Does it match with the round trip time returned by traceroute ?
- In each iteration of traceroute does it use the same port number for the destination ? IF yes, reason why and if no, then also argue why does it do so.

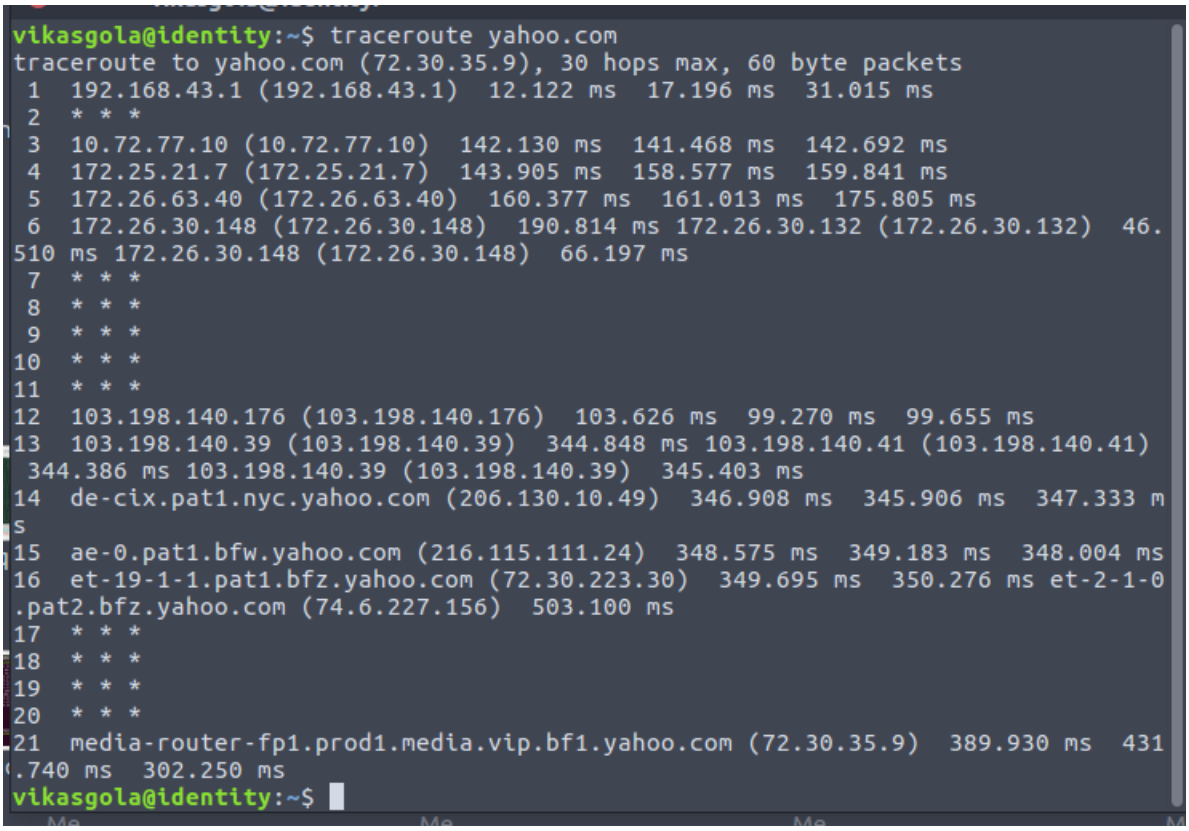
Answer

- 3 packets are send by traceroute in each iteration because tcpdump output shows three packets to same IPA.

- For first iteration 5.18 , 5.16 and 5.22 are the round trip times for each three probes sent.
- NO, it don't use same port number for destination in the each iteration.







Question 4 Use the Visual traceroute command at https://www.monitis.com/traceroute/ What is the source ad- dressand the destination address of these packets ?

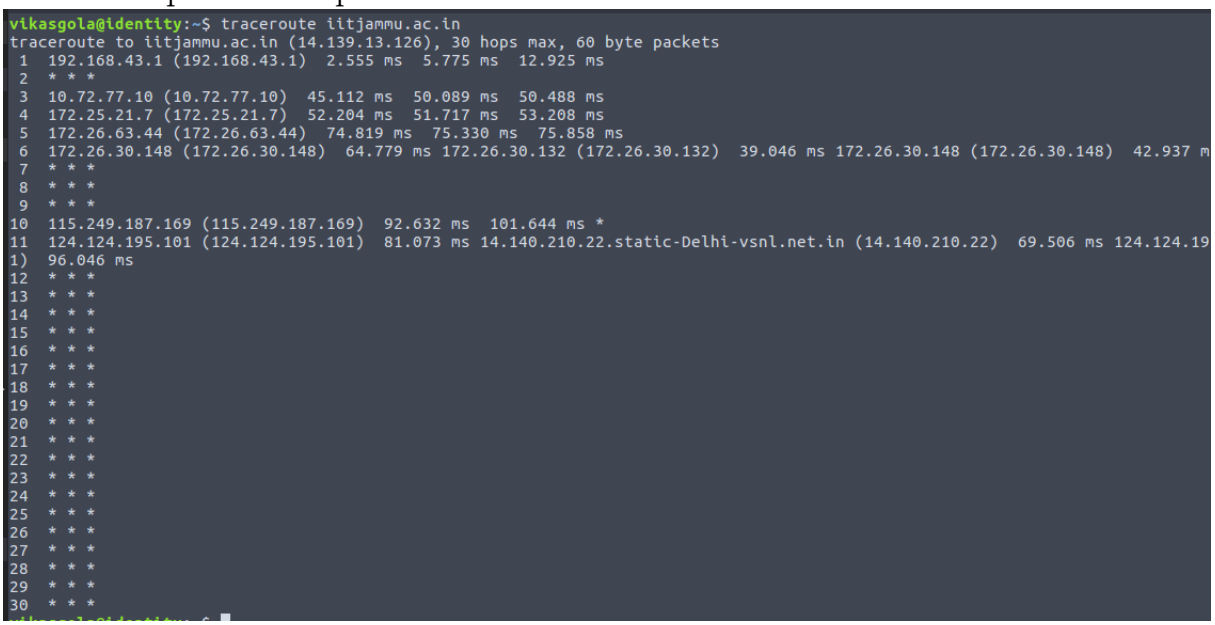
Answer

Source address = 10.0.0.0
Destination address = 98.138.219.231

Question 5 If you think a firewall stopped the packet, how can one know that a firewall has come in the way ? What do you think the IP address of that

firewall is based on where the trace route stopped?

Answer If traceroute is not able to determine the path between the source and destination then it is firewall which is dropping these packets and not able to detect the path. Here is the example where traceroute indicates that there is firewall present in path.



Question 6 If a firewall stopped has not obstructed the packet sent, what does the last IP address appearing in the trace route list indicate ?

Answer The last address in traceroute list is the destination IP address if no firewall has stopped the sent packet.

Question 7 Enlist and briefly explain all the usages of the ping program - explain each use with the help of an example.

Answer

- **Host is Up or Not**
  ping can be used to check if host is live or not.

```
vikasgola@identity:~$ ping localhost
PING localhost (127.0.0.1) 56(84) bytes of data.
64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.058 ms
64 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.045 ms
64 bytes from localhost (127.0.0.1): icmp_seq=3 ttl=64 time=0.049 ms
64 bytes from localhost (127.0.0.1): icmp_seq=4 ttl=64 time=0.076 ms
64 bytes from localhost (127.0.0.1): icmp_seq=5 ttl=64 time=0.076 ms
^C
--- localhost ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4075ms
rtt min/avg/max/mdev = 0.045/0.060/0.076/0.016 ms
vikasgola@identity:~$
```

- **Destination IP**
  ping is also used to find the destination IP address.

```
vikasgola@identity:~$ ping yahoo.com
PING yahoo.com (98.138.219.231) 56(84) bytes of data.
64 bytes from media-router-fp1.prod1.media.vip.ne1.yahoo.com (98.138.219.231): i
cmp_seq=1 ttl=48 time=582 ms
64 bytes from media-router-fp1.prod1.media.vip.ne1.yahoo.com (98.138.219.231): i
cmp_seq=2 ttl=48 time=540 ms
64 bytes from media-router-fp1.prod1.media.vip.ne1.yahoo.com (98.138.219.231): i
cmp_seq=3 ttl=48 time=500 ms
^C
--- yahoo.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 500.376/541.207/582.542/33.546 ms
vikasgola@identity:~$
```

- **As traceroute**
  ping can also be use alternative to traceroute to find the ip address of the middle routers in the path or to find the path between source and destination.
  screenshot is included in next question where we have used ping as traceroute.

- **Check whether the local network interface is up and running**
  ping is also use to check if the local network interface is up and running or not.

```
vikasgola@identity:~$ ping 0
PING 0 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.097 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.075 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.074 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.075 ms
64 bytes from 127.0.0.1: icmp_seq=5 ttl=64 time=0.075 ms
^C
--- 0 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4099ms
rtt min/avg/max/mdev = 0.074/0.079/0.097/0.010 ms
```

- **Flood the network**
  ping is also use to send large number of packets to host.

```
vikasgola@identity:~$ sudo ping -f yahoo.com
[sudo] password for vikasgola:
PING yahoo.com (72.30.35.10) 56(84) bytes of data.
.................................^C
--- yahoo.com ping statistics ---
1068 packets transmitted, 1033 received, 3% packet loss, time 16678ms
rtt min/avg/max/mdev = 256.101/281.617/381.766/15.072 ms, pipe 25, ipg/ewma 15.6
31/284.098 ms
vikasgola@identity:~$
```

- **Record and print route of how ECHO_REQUEST sent and ECHO_REPLY received** It records, and prints the network route through which the packet is sent and received.

Question 8 Write a small shell script that uses ping to simulate the working of traceroute. Briefly explain the operation of the script.

Answer

```
for i in 1..30;do
ping -t $i -c 1 yahoo.com;
done      | grep "Time to live"
```

This script contains a for loop which runs 30 times and pings the destination address with TTLs 1 to 30 one by one. grep command help to capture only the required TTL reply and shows.

```
vikasgola@identity:~/Downloads/assign3_networks$ for i in {1..30};do ping -t $i -c 1 yahoo.com; done
| grep "Time to live"
From 192.168.43.1 icmp_seq=1 Time to live exceeded
From 10.72.77.10 icmp_seq=1 Time to live exceeded
From 172.25.21.7 icmp_seq=1 Time to live exceeded
From 172.26.63.40 icmp_seq=1 Time to live exceeded
From 172.26.30.148 icmp_seq=1 Time to live exceeded
From 49.45.4.251 icmp_seq=1 Time to live exceeded
From 103.198.140.39 icmp_seq=1 Time to live exceeded
From de-cix.pat1.nyc.yahoo.com (206.130.10.49) icmp_seq=1 Time to live exceeded
From ae-7.pat1.dce.yahoo.com (216.115.104.120) icmp_seq=1 Time to live exceeded
From et-2-1-0.pat2.bfz.yahoo.com (74.6.227.156) icmp_seq=1 Time to live exceeded
From et-8-1-1.pat1.sjc.yahoo.com (216.115.107.150) icmp_seq=1 Time to live exceeded
From ae-3.pat2.swp.yahoo.com (216.115.96.57) icmp_seq=1 Time to live exceeded
From et-1-1-0.clr2-a-gdc.ne1.yahoo.com (98.138.97.67) icmp_seq=1 Time to live exceeded
vikasgola@identity:~/Downloads/assign3_networks$
```

Question 9 Explain all the approaches that can be used to do a ping sweep.

Answer There are number of commands to do ping sweep which are gping, fping and nmap. Usually ping sweep contains the ICMP ECHO request but we can also use ICMP timestamp and ARP for the same work.