Alias resolution

NETMET Lab Exercises 5 -- **GRADED**

Introduction

So far in the previous labs, we always had interface level information when we were conducting measurements. That is, in a Traceroute for instance, we were seeing the interface IP addresses of the routers on the path towards a destination, but we didn't actually have information about if two IP addresses were on the same routers.

Given a list of IP addresses gathered via several traceroutes, it could be tempting to know if some of these IP addresses belong to the same routers. This task is known as *alias resolution*.

Several techniques are used to perform alias resolution and it's still an active field of research in network measurements, and therefore we will learn about this field by reading some research papers. In this lab we will see two common techniques and attempt to implement one of the two.

Grading information

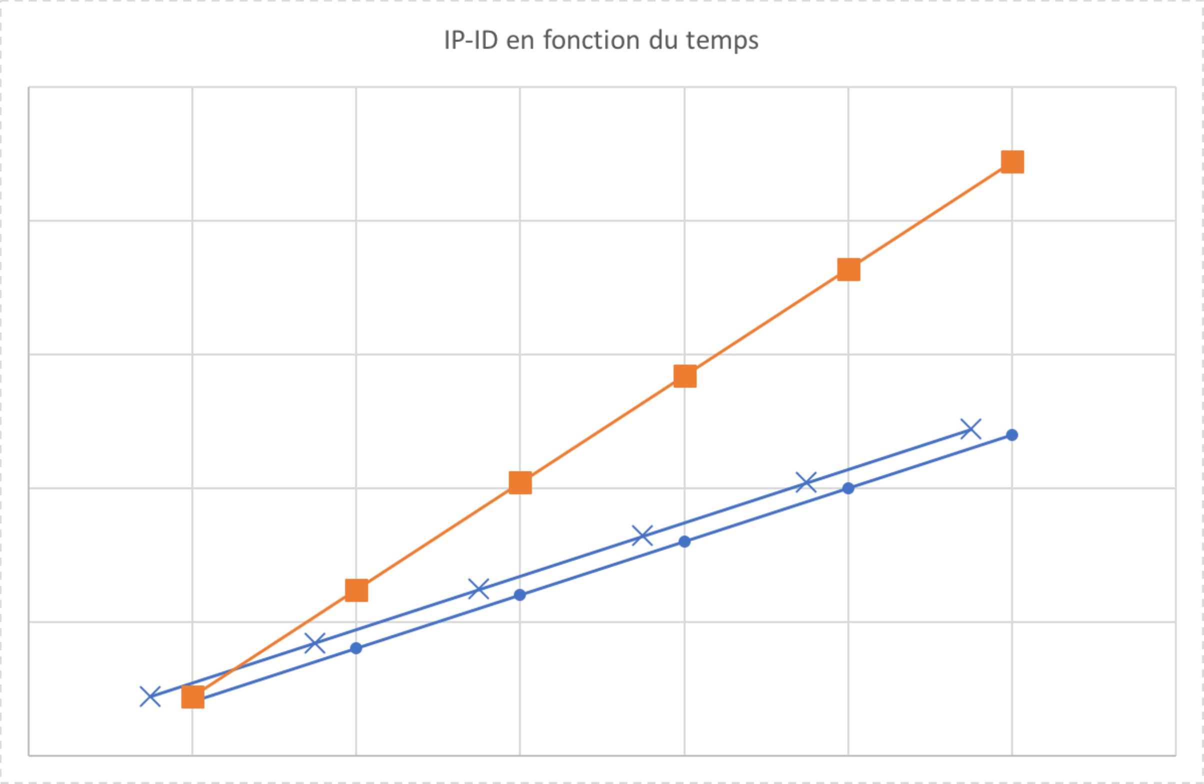
You must give a report following the structure of this lab and answering the questions.
This is individual work.
Any piece of code must be either pasted on the report or transmitted via a Github Gist (https://gist.github.com/) link.

IP identifier method

Have a look on the following paper and try to understand the underlying algorithm:
https://www.caida.org/publications/papers/2013/alias_resolution_midar/alias_resolution_midar.pdf

Questions :

1. Do a summary of how the technique works with your own words.
2. Check the following graph :



Which ones can be inferred as aliases :

A. Squares and Crosses
B. Crosses and Circles
C. Circles and squares
D. None of the above

3. Is this sequence of IP-ID can infer aliases :
A: 52491 B: 62439 A: 6041 B: 12883

We want to know if these two IP addresses are aliases :

186.159.6.105
186.159.7.105

Ping these IPs simultaneously and get the traces into a pcap file (with tcpdump).
Analyze the IP-ID header in Wireshark and manually try to infer if the two IP addresses are aliases.

Fingerprinting method

Have a look on the following paper and try to understand the underlying algorithm:
http://conferences.sigcomm.org/imc/2013/papers/imc055-vanaubelA.pdf

Questions :

1. Do a summary of how the technique works with your own words.
2. Is the TTL signature can be a n-tuple with n > 2 ?
3. Suppose we get the following values for the return TTL of an ICMP Echo Reply and an ICMP TTL Exceeded messages of two IP addresses A and B

   A = <248, 59> , B = <249, 60>

   What can we deduce about A and B?

   A. They belong to the same router
   B. They do not belong to the same router
   C. They may belong to the same router
   D. We can’t tell

Run some traceroutes to multiple destinations, and keep the traces in pcap files.
Gather some IPs of routers along the path and send a ping to each of the IPs.
Can you deduce which IP’s are not aliases? Aliases?

Code one technique logic

Code the technique of your choice in Python (>= 3.6).