# Traceroute

NETMET Lab Exercises 3

## Introduction

In this session we will do a deep analysis of the Traceroute tool.

We will first perform traceroutes between two EdgeNet pods to well understand the output.

Then, we will try to gain information about the Internet macro topology using traceroutes information.

Finally, after being confident about how Traceroute is working precisely, we will code the logic by ourselves and even try to go further to have even more information about the Internet topology.

## Using traceroute to determine routers

Use traceroute to measure the path to *facebook.com* from the EdgeNet node.

At some hops you will see more than one IP address, why ?
At some hops you will see stars (*), why ?

We know that traceroute shows us every router IP address on the way to a target. But do we see the same routers in both ways? When we perform a traceroute from A to B, we should see the same result as from B to A, just in reverse order. Check if this is true, using two EdgeNet nodes. So log into both, and perform a traceroute to the other one.
Do you see the same number of hops? Do you see the same router IP addresses? What is the reason that all the IP addresses on the way are completely different?

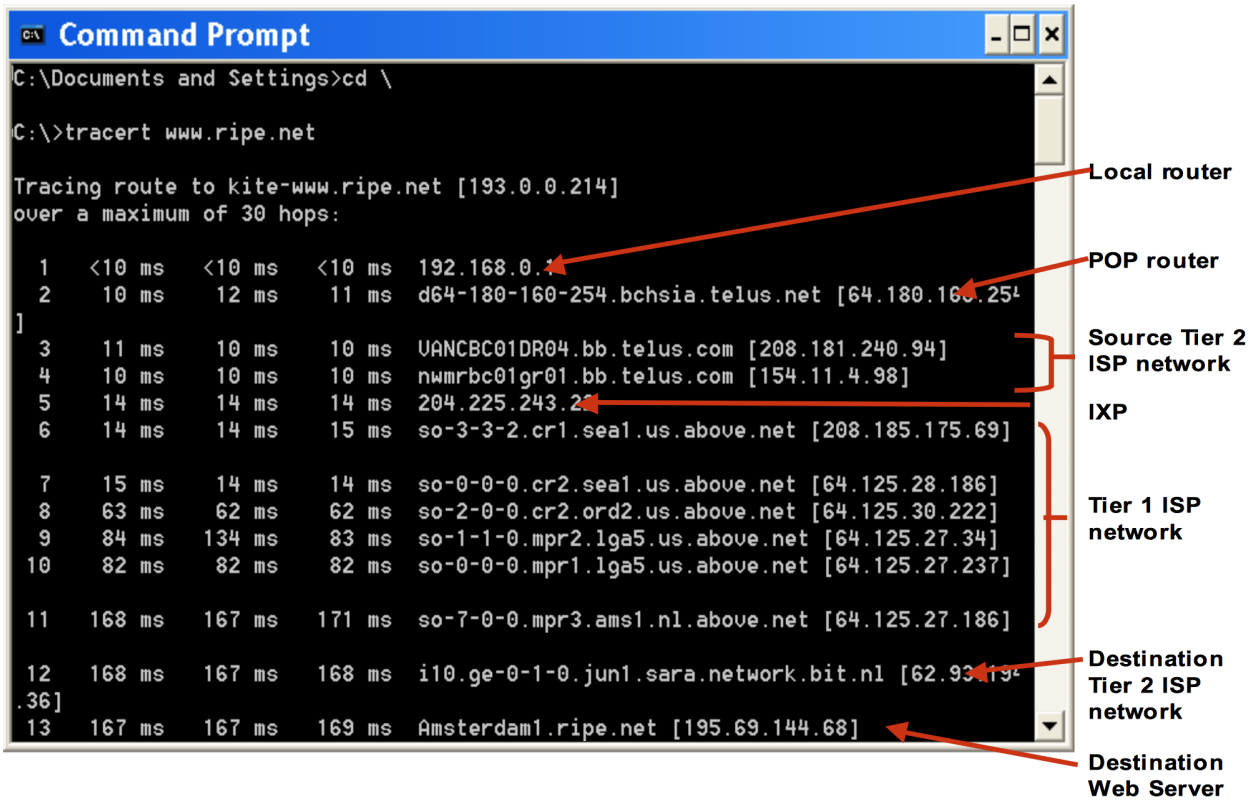
## Visualizing a packet's way through the Internet

Now we want to use traceroute to see exactly which path a packet takes through the Internet. For example, we want to figure out which countries and cities a packet goes through and which POP (points-of-presence) and IXPs (Internet Exchange Points) it passes.

**Definitions (Wikipedia):**

- Point-of-presence: An Internet point of presence typically houses servers, routers, network switches, multiplexers, and other network interface equipment. It is typically located in a data center. ISPs typically have multiple PoPs. PoPs are often located at Internet exchange points and colocation centres.

- Internet Exchange Point: An Internet exchange point (IX or IXP) is a physical infrastructure through which Internet service providers (ISPs) and Content Delivery Networks (CDNs) exchange Internet traffic between their networks (autonomous systems).
- Autonomous System: is a collection of connected Internet Protocol (IP) routing prefixes under the control of one or more network operators on behalf of a single administrative entity or domain that presents a common, clearly defined routing policy to the internet.
- Tier 1 network: A tier 1 network is an Internet Protocol (IP) network that participates in the Internet solely via settlement-free interconnection, also known as settlement-free peering. **List of all Tier 1 networks** here.
- Tier 2 network: A network that peers with some networks, but still purchases IP transit or pays settlements to reach at least some portion of the Internet.
- Tier 3 network: A network that solely purchases transit from other networks to participate in the Internet.




## Analyse traceroute information

- Use a EdgeNet node to perform traceroutes to various targets: afrinic.net (African Internet registry), apnic.net (Asian Internet registry), arin.net (North American Internet registry), lacnic.net (South American Internet registry)
- Figure out which hop belongs to which ISP, and where it is located. Is it an IXP, a POP, does it belong to a tier 1 network?
- Create a table for each traceroute: For each hop note, to which ISP it belongs, where it is located etc. Use `whois <ip address>` to retrieve this information about an IP address. Whois is a program that gets information about an IP address/domain name which is stored in a database. To get the Autonomous system number you can use

`whois -h whois.cymru.com " -v <ip_address>"`. This uses whois and tells it to use a specific database (whois.cymru.com), which contains information about AS-numbers.
**Because whois is blocked by the firewall, use a web based version:** http://ping.eu/ns-whois/

- Use a map (such as https://www.freemaptools.com/measure-distance.htm) to draw the routes. For each hop, create a label on the map, with information such as the AS-number and the name of the ISP.

## Understand the underlying network concepts of Traceroute

Perform some traceroutes along with capturing the network data via a sniffer tool in order to answer these questions.

*Questions :*

- From a network perspective, what does Traceroute do to gather route information ?
- What protocol Traceroute is using ? What protocol Traceroute is receiving ?
- Is the protocol sent the same as the protocol received ? If not, why ?
- Is it possible that Traceroute can be wrong about a route, with your understanding ?

## Code Traceroute logic

With your favorite programming language, let's try to mimic the behavior of *traceroute.*

*Help :* This work can be done quite easily with the Python programming language.
I suggest you look at the documentation of Scapy which is a famous network prototyping Python library.

*To go even further*

Could you include an automatic IP to AS translation in your traceroute ?

*Help* : https://stat.ripe.net/data/prefix-overview/data.json?resource=8.8.8.8

Picture from http://web.nmsu.edu/~jbeasley/Cisco_Discovery_4-1/courses/en0500000000/en0501000000/en0501020000/en0501020300/en0501020303/cm6042232704/lab.pdf