ENSEA
Ecole Nationale
Supérieure
de l'Electronique
et de ses Applications

3RTS – Architecture & Protocols

TP #1 - room D055

C. BARÈS

Goals : To use basic network commands and capture with Wireshark.

Preliminary Notes

The computers in the room D055 are networked using the sepcific network interface (grey cable). Some of the operations described in these labs require you to be an administrator of the machine. For this reason, these sessions can only take place in room D055, with with a special login.

To connect in room D055, you will use the login "tpresau" associated with the password "sethisis". To access the superuser mode, use the sudo command, and to open a root shell the sudo -s <command>.

To access the internet (no matter which tool you use), you will first need to authenticate yourself on the ucopia captive portal.

If a command <command> is missing, install it by typing :

```
  $ sudo apt install <commande>
```

Information about an command can be obtained by typing :

```
   $ <command> -h
   $ man <command>
```

1 – Basic commands

In a terminal window, run the ifconfig or ip addr command to find out the network configuration of your machine on the enpXsY interface.

- How many interfaces does your machine have ?
- Describe the enpXsY interface.
- By consulting the OUI database, determine the manufacturer of your network card. (A copy of the OUI base is available on Moodle.)
- Is the interface IPv6 compatible ?
- What is the network mask of enpXsY ? In which LAN is your machine located ?
- Check if all the machines in the room are accessible from your machine using a ping.
- Then ping external sites (eg : www.ensea.fr, www.google.fr).
- Comment on your results (especially the TTL field).

2 – Capture a ping

Capture a ping to a PC in the room with Wireshark and comment on it.

Repeat with a ping to an external server.

3 – ARP Request Capture

The capture filter to retrieve only ARP requests to or from your machine is simply : `arp and host <myIPaddress>` Start a capture in Wiershark using this filter.

In the terminal window, using the `arp -a` command, look at the machine's address resolution table. Remove an address (RTFM) of one of the machine next to yours, then ping this machine again. Comment on your capture.

4 – DNS Query Capture

The filter to retrieve only DNS queries to or from your machine is a little more complex : `port 53 and host <myIPaddress>` Run a capture using this filter.

Using the `dig <domain> ANY` command, determine the address of the main servers of the school (dns, web, mail, intranet...). What are these servers ? What is the numerical value in an entry ? Comment on your capture.

What do the entries A, AAAA, MX, NS, SOA correspond to ?

Using the same command, determine the IP addresses of the web servers www.google.fr and www.perdu.com Try to access www.google.fr directly via the http protocol using its IP address in a browser. Do the same for www.perdu.com. What can we deduce from this ?

Test the school's dns servers (if necessary add @ option to dig command). What can you conclude from this ?

Test the "+trace" option of the dig command. What can you deduce about the way the DNS protocol works ?

Notes : If you have problems with DIG command in D055 room, do it online at this address :
https://toolbox.googleapps.com/apps/dig/#ANY/

5 – Capture traffic generated by traceroute

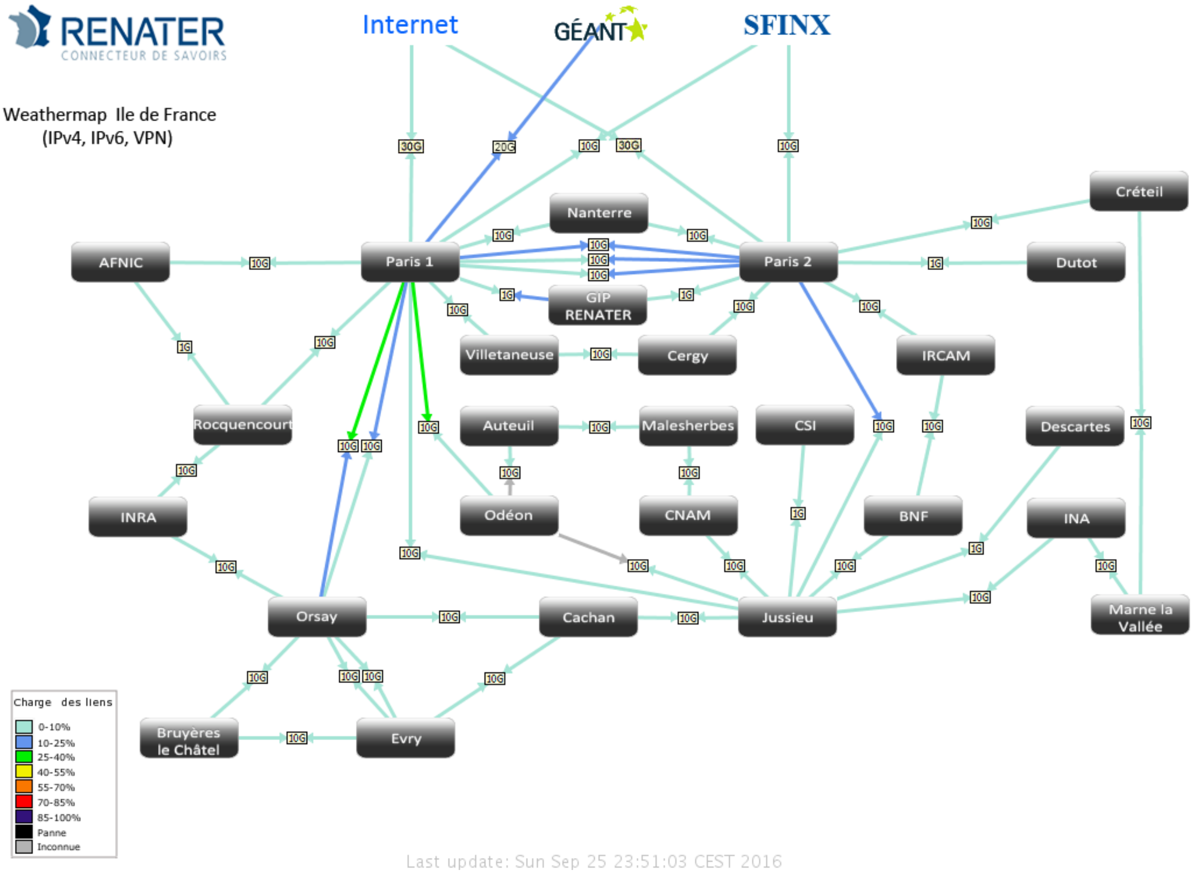
Filtering only the traffic coming from or going to your machine, capture the traffic generated by the "traceroute" utility, which allows you to find the IP nodes crossed to reach a remote machine. You will do your traceroute with the "-I" option to the Stanford University Computer Science website (`cs.stanford.edu`)

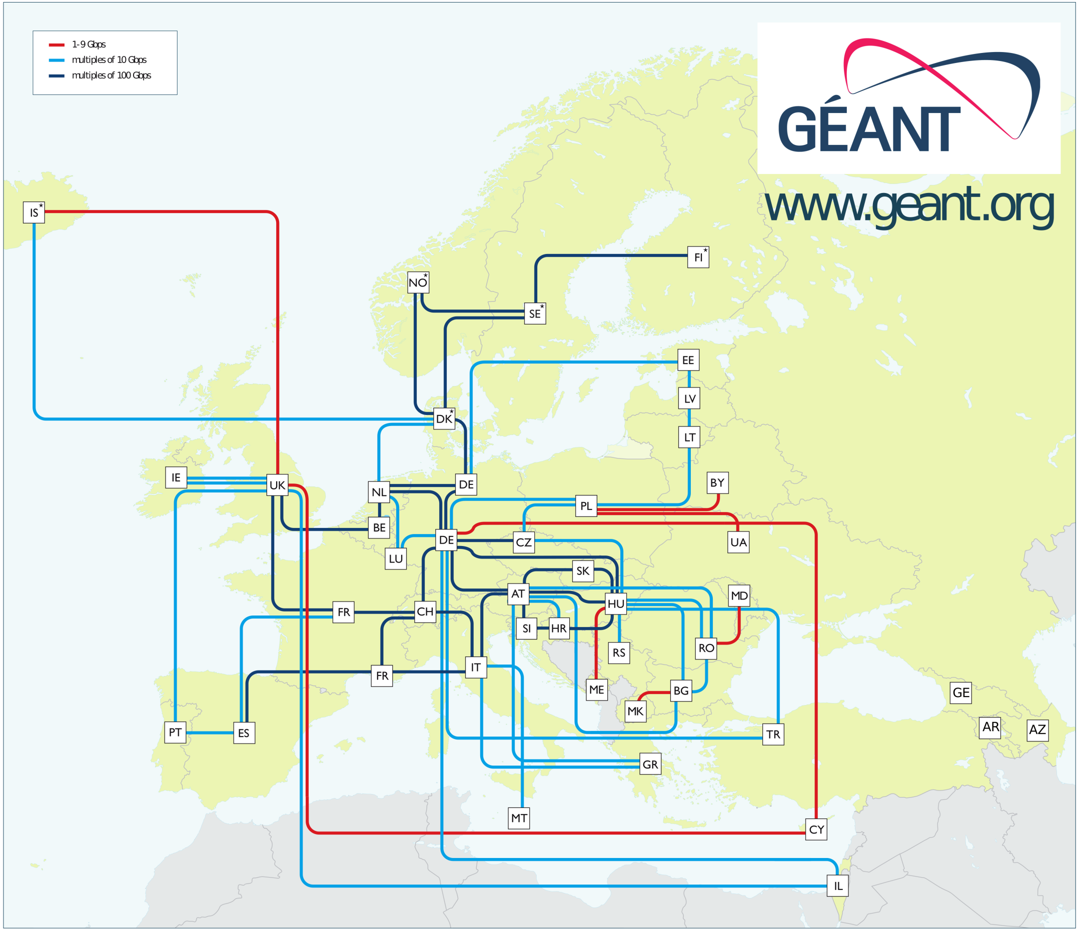
Explain how the utility works. In particular, comment on transatlantic transit using these two graphs, taken from the Renater and Géant websites.

The utility `traceroute` can be used in different ways :

- `traceroute` (without option)
- `traceroute -I`
- `tcptraceroute` (==`traceroute -T`)

What are the differences between these different forms and what is the advantage of having all these options ?


RENATER
CONNECTEUR DE SAVOIRS
Weathermap Ile de France
(IPv4, IPv6, VPN)
Internet
GÉANT
SFINX
30G
20G
10G
30G
10G
Nanterre
Créteil
AFNIC
Paris 1
Paris 2
Dutot
GIP RENATER
Villetaneuse
Cergy
IRCAM
Rocquencourt
Auteuil
Malesherbes
CSI
Descartes
INRA
Odéon
CNAM
BNF
INA
Orsay
Cachan
Jussieu
Marne la Vallée
Bruyères le Châtel
Evry
10G
1G
Charge des liens
🟦 0-10%
🟦 10-25%
🟩 25-40%
🟨 40-55%
🟧 55-70%
🟥 70-85%
🟪 85-100%
⬛ Panne
⬜ Inconnue
Last update: Sun Sep 25 23:51:03 CEST 2016


1-9 Gbps
multiples of 10 Gbps
multiples of 100 Gbps
GÉANT
www.geant.org
IS
FI
NO
SE
EE
LV
LT
DK
BY
IE
UK
NL
DE
PL
BE
LU
DE
CZ
UA
SK
AT
HU
MD
FR
CH
SI
HR
RS
RO
FR
IT
ME
BG
MK
PT
ES
GE
AR
AZ
TR
GR
MT
CY
IL