Fuentes
Grégory
RT2-TDA1

Rapport cartographie

Janvier 2022

Table des matières

1 RFC qui régissent les réseaux....1
Qu’est ce qu’une RFC ?....1
Qu’elles sont les RFC les plus présentent sur internet ?....2
2 Les protocoles les plus utilisés sur internet....3
Qu’est ce que internet ?....3
Qu’est ce qu’un protocole....3
Quelles sont les protocoles les plus utilisés sur internet ?....4
3 Fonctionnement de traceroute....5
Qu’est ce que traceroute ?....5
Comment fonctionne traceroute ?....5
Qu’elles sont les commandes traceroute que nous pouvons utiliser ?....6
4 Script pour générer une carte automatique....6
5 Génération de la carte avec certaines ip....7
6 Trouver les anomalies. Pourquoi sont elles normales ?....8
Anomalie 1....8
Anomalie 2 :....9
Anomalie 3....10
Solution 1....10
Solution 2....11
7 Conclusion....11

1 RFC qui régissent les réseaux

○ Qu’est ce qu’une RFC ?

Une RFC (Requests For Comments) est un document numéroté qui décrit les spécifications techniques d’internet. Une RFC spécifie les différentes implémentations et normalisations du modèle TCP/IP (internet).

Les RFC sont classées selon 5 classifications :

→ obligatoire

→ recommandé

→ facultatif

→ limitée

→ non recommandé

Les RFC sont également classées selon 3 niveaux de standard :

→ standard proposé

→ standard brouillon

→ standard internet

○ Qu’elles sont les RFC les plus présentent sur internet ?

Nom des RFC	Fonctionnement
RFC 1701	Protocole Generic Routing Encapsulation (GRE): protocole de mise en tunnel qui permet d'encapsuler n'importe quel paquet de la couche réseau dans sa conception d'origine
RFC 1702	Protocole GRE pour IPv4
RFC 2784	Encapsulation de routage générique (GRE) Mis à jour par RFC 2890
RFC 2890	Extensions de clé et de numéro de séquence à GRE
RFC 1661	Protocole Point à Point (PPP) Mis à jour par RFC 2153 Point-to-Point Protocol est un protocole de transmission pour internet
RFC 2153	Extensions de fournisseur PPP Mis à jour par RFC 5342 ET 7042
RFC 1994	PPP Challenge Handshake Authentication Protocol (CHAP)

	méthode d'authentification utilisant PPP Catégorie Standart Track mis a jour par TFC 2484
RFC 2433	Microsoft PPP CHAP Extensions
RFC 2759	Microsoft PPP CHAP Extensions, Version 2
RFC 1700	Numéro attribué instantané du processus en cours d'attribution des paramètres de protocole pour la suite de protocoles Internet. obsolète par rfc 3232
RFC 3232	Numéro attribué par iana

2 Les protocoles les plus utilisés sur internet

○ Qu’est ce que internet ?

Internet est un réseau informatique mondial. C’est un réseau de réseau (Wide Area Network) où *l’information est transmise grâce à un ensemble standardisé de protocoles de transfert de données qui permet des applications variées comme le courrier électronique, le web (World Wibe Web), le partage de fichier, le streaming . (wikipédia)*

○ Qu’est ce qu’un protocole

Un protocole en informatique est un ensemble de règles qui régissent les échanges de données ou le comportement collectif de processus ou d’ordinateurs en réseaux ou d’objets connectés. Un protocole a pour but de réaliser une ou plusieurs tâches concourant à un fonctionnement harmonieux d’une entité générale. (Wikipédia)

○ Quelles sont les protocoles les plus utilisés sur internet ?

Protocole IP (Internet Protocol)	RFC 791 update by RCF 1349, 2474, 6864
Wifi	RFC 5416
Bluetoooth	RFC 7668
Protocol UDP (User Datagram Protocol)	RFC 768
Protocole ICMP	RFC 792
Protocole TCP	RFC 793
Protocole FTP	RFC 959
Protocole Internet Mail	RFC 822
Protocole Telnet	RFC 854
Protocole NNTP	RFC 977
Protocole Netbios	RFC 1001
Protocole SLIP	RFC 1055
Protocole SSH	RFC 4253 Updated By: -RFC 6668 -RFC 8268 -RFC 8308 -RFC 8332 -RFC 8709 -RFC 8758
Protocole MIB-II	RFC 1213
Protocole PPP	RFC 1661
Protocole HTTP	RFC 2616
Protocole LDAPv3	RFC 4511
Protocole SMTP	RFC 5321

Protocole QUIC	RFC 8999
Protocole DNS	RFC 1035
Protocole NTP	**RFC** 958

3 Fonctionnement de traceroute

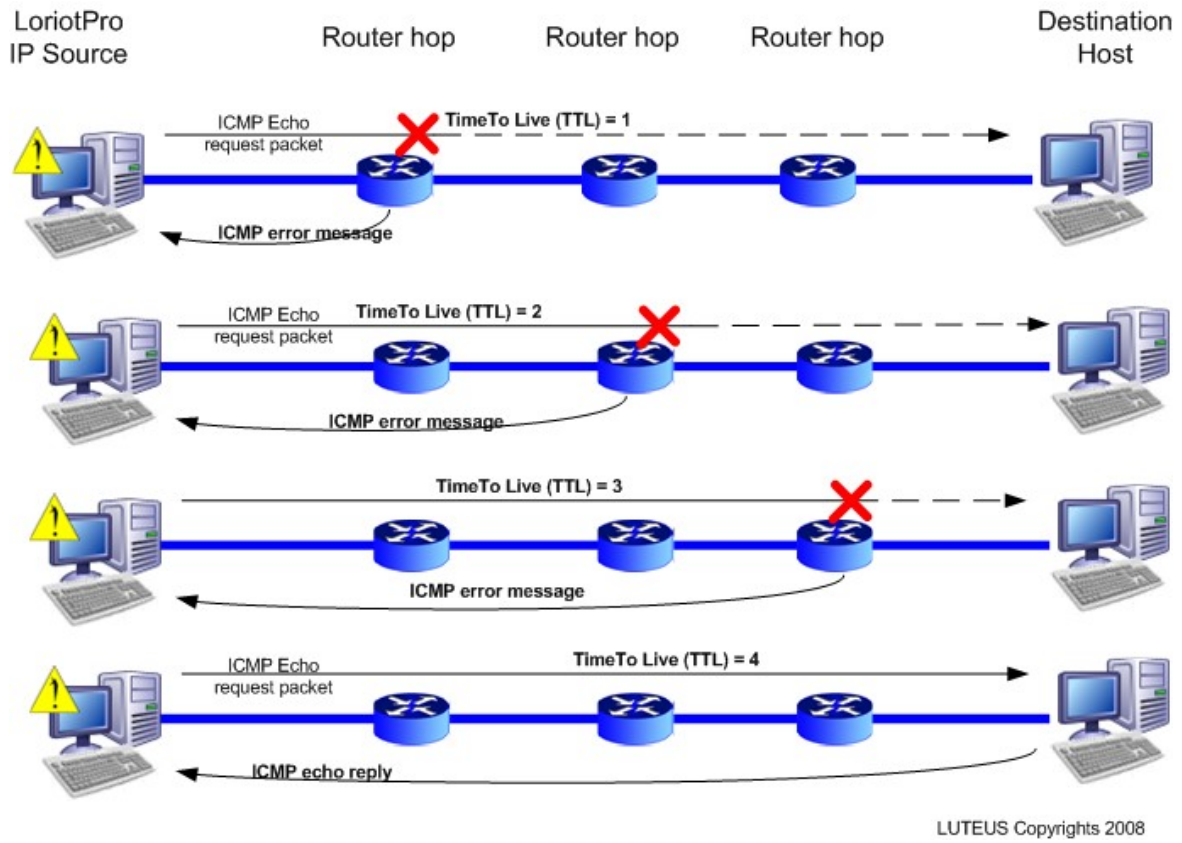
○ Qu’est ce que traceroute ?

Traceroute est un programme utilitaire sous Linux qui permet de suivre les chemins qu’un paquet de données emprunte pour aller d’une machine locale à une machine distante.

Tracert est la commande traceroute sous Windows.

○ Comment fonctionne traceroute ?

Le fonctionnement de traceroute consiste à envoyer des paquets UDP,TCP ou ICMP Echo Request avec un paramètre TTL qui commence par 1 et qui s’incrémente d' une unité pour chaque routeur passé pour découvrir les routeurs de proche en proche. On rappelle que chaque routeur qui reçoit un paquet IP en décrémente le TTL avant de le transmettre et que lorsque le TTL atteint 0 alors le routeur émet un paquet ICMP d’erreur Time to live exceeded vers la source.



○ Qu’elles sont les commandes traceroute que nous pouvons utiliser ?

Traceroute -I <@IP> → Utilise traceroute avec le protocole ICMP

Traceroute -U <@IP> → Utilise traceroute avec le protocole UDP

Traceroute -T <@IP> → Utilise traceroute avec le protocole TCP

Traceroute -p <numéro_port> <@IP> → utilise traceroute sur le port indiqué

4 Script pour générer une carte automatique

Sur le github : https://github.com/gregf34110/tptechnoreseau.git vous pouvez trouver tout les documents du projet de la cartographie du web.

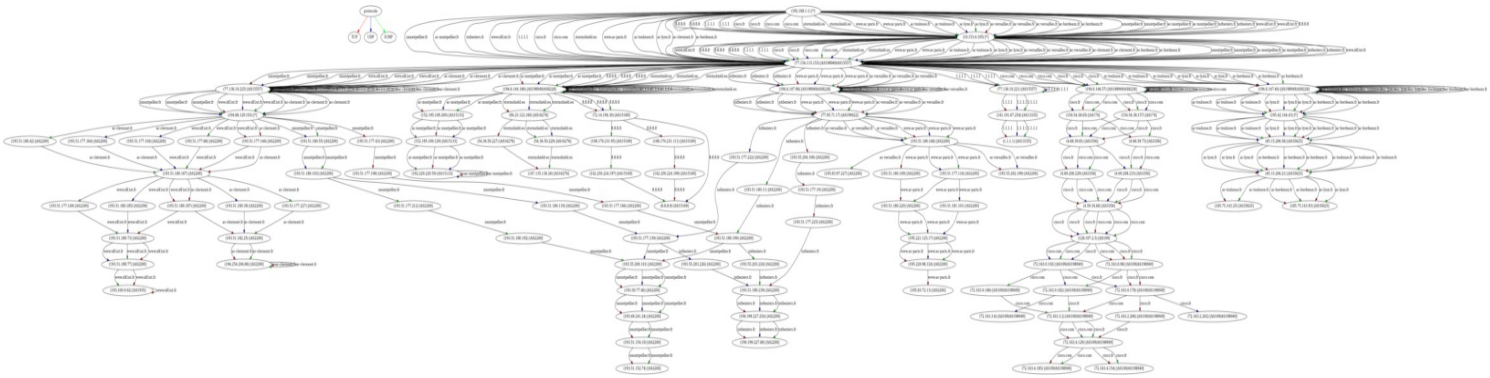
Script pour générer une carte du web de manière automatique :

```
#!/bin/bash
echo -n "Combien d'adresse IP faut il analyser ?"
read a
tab_ip=()
for (( i=1; i<=$a; i++ ))
do
echo "Entrer l'adresse $i : "
read ip
tab_ip[${#tab_ip[*]}]=$ip
done
rm -r ./fichier
mkdir fichier
for ip in ${tab_ip[*]}
do
echo "nmap avec l'adresse ip $ip"
sudo nmap -sU -sT $ip > ./fichier/nmap.txt$ip
tcp=$(grep tcp ./fichier/nmap.txt$ip | cut -d'/' -f1 | grep -w "80" )
udp=$(grep udp ./fichier/nmap.txt$ip |cut -d'/' -f1 | grep -w "33459" )
echo "traceroute avec protocole ICMP de l'adresse $ip:"
sudo traceroute -I -d -A $ip | awk '{ print $3,$4 }' | sed '1d' | sed '/* */d' >
./fichier/traceroute_ICMP$ip
echo "traceroute avec protocole UDP de l'adresse $ip:"
sudo traceroute -U -d -A $ip -p $udp 80 | awk '{ print $3,$4 }' | sed '1d' | sed '/* */d' >
./fichier/traceroute_UDP$ip
echo "traceroute avec protocole TCP de l'adresse $ip:"
sudo traceroute -T -d -A $ip -p $tcp 53 | awk '{ print $3,$4 }' | sed '1d' | sed '/* */d' >
./fichier/traceroute_TCP$ip
done
echo 'digraph G {' > ./fichier/graphe1.dot
liste=("TCP" "UDP" "ICMP")
```

```
couleur=("red" "blue" "green")
echo '"protocole"->"TCP" [color=red];' >> ./fichier/graphe1.dot
echo '"protocole"->"UDP" [color=blue];' >> ./fichier/graphe1.dot
echo '"protocole"->"ICMP" [color=green];' >> ./fichier/graphe1.dot
for ip in ${tab_ip[*]}
do
i=0
while (($i<3))
do
fichier="./fichier/traceroute_"${liste[i]}$ip
l=0
ligne_precedente=0
while read ligne
do
if (($l!=0))
then
echo -e "\"$ligne_precedente""\" -> "\"$ligne""\" [fillcolor=${couleur[i]}, label="\"$ip"\"] ""
>> ./fichier/graphe1.dot
fi
ligne_precedente=$ligne
l=$(($l+1))
done < $fichier
i=$i+1
done
done
echo } >> ./fichier/graphe1.dot
#dot -Tps -o ./fichier/graphe1.png ./fichier/graphe1.dot
#dotty ./fichier/graphe1.dot

sudo cat ./fichier/graphe1.dot | dot -T png > ./fichier/graphe1.png && xdg-open
./fichier/graphe1.png
```

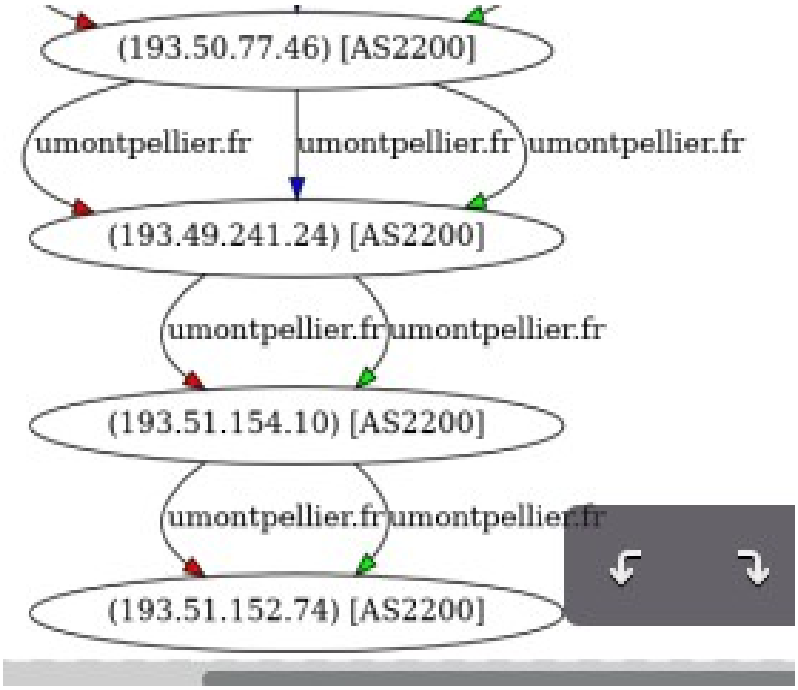
5 Génération de la carte avec certaines ip



(il faut zoomer sur la photo pour bien voir)

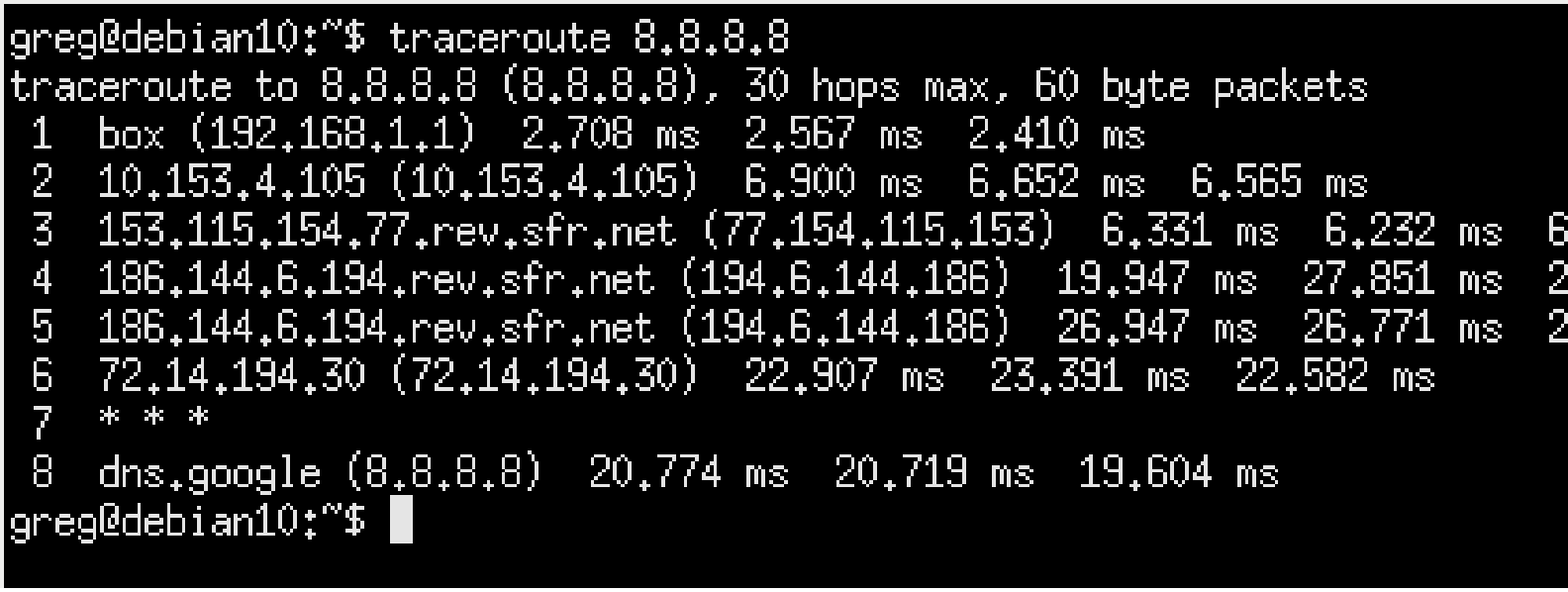
6 Trouver les anomalies. Pourquoi sont elles normales ?

- **Anomalie 1**



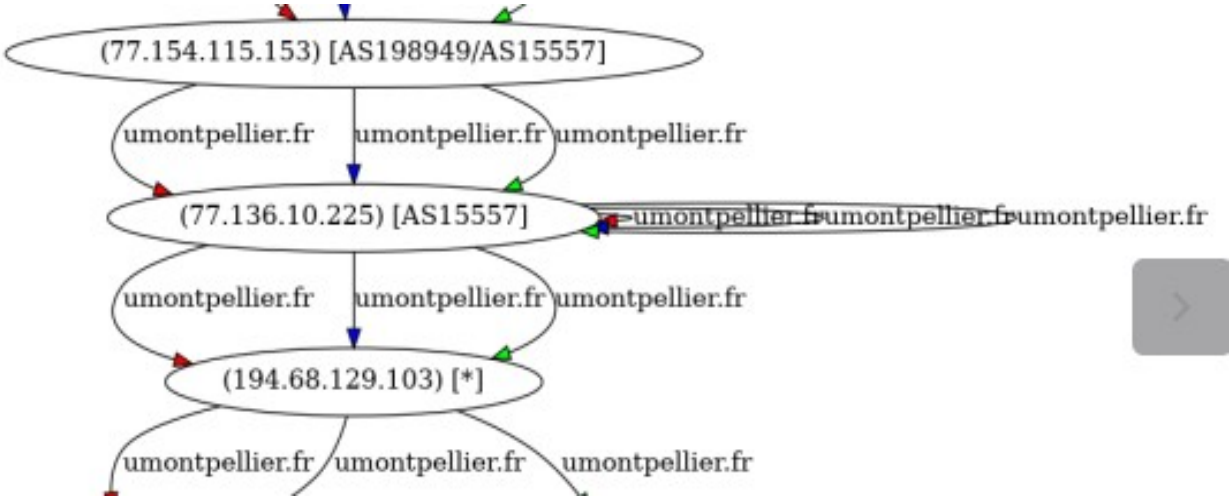
Nous pouvons remarquer que sur le graphe du dessus, nous avons la flèche bleu (UDP) qui n'arrive pas à destination de l'adresse 193.51.152.74 (site de umontpellier.fr).
Cela est peut être du à un firewall présent soit sur l'adresse 193.51.154.10 soit sur l'adresse 192.51.152.74 qui empêche de faire passer des trames udp.
Cette anomalie s'appelle « messing destination » soit « destination manquante ».

- **Anomalie 2 :**



Ci-dessus, voici une capture d'écran d'un traceroute de mon domicile vers le dnsgoogle 8.8.8.8 . Nous pouvons remarquer des astérisques pour le routeur numéro 7. Le routeur retourne donc aucune information. Cette anomalie à très peut d'impact sur la vie réel cependant si le routeur 7 ne fonctionne plus correctement, cela peut être problématique. Cette anomalie se produit généralement lorsqu'un routeurs est protégé par un firewall ou configuré de manière à ne pas générer d'erreurs ICMP TTL exceeded. Cette anomalie est la plus courante de traceroute. Elle s'appelle « messing hops» soit saut manquant.

- ## Anomalie 3



Ci dessus, nous pouvons observer une boucle, le routeur 77.136.10.225 s’envoie des paquets UDP, ICMP et TCP à lui même.
C’est l’anomalie qui se nomme « Loops and Circles », elle est du généralement quand l'équilibrage de charge est utilisé pour des chemins de longueur inégale.

- ## Solution 1

Pour éviter les anomalies à cause des firewall qui ne laissent pas passer les reqêtes ICMP, nous pouvons utiliser traceroute avec les protocole UDP et TCP qui contourne ses restrictions. En générale pour le traceroute en TCP on utilise le port 80. Donc en utilisant UDP ou TCP au lieu des requêtes d'écho ICMP, les sauts manquants ou les destinations manquantes sont éliminés.

○ Solution 2

Pour éviter les anomalies dites « Loops and Circle » nous pouvons utiliser « Paris traceroute »

Paris traceroute contrôle le contenu des en tête des paquets et obtient donc une image plus précise des itinéraires réels suivis par des paquets.

7 Conclusion

Pour conclure, internet contient de nombreux protocoles qui sont normalisé avec de nombreuse RFC. De plus traceroute est un outil très puissant mais qui présente beaucoup d'anomalie. Cependant certaines des anomalies ont très peu d'impact sur l'analyse des réseaux. Pour les anomalies qui posent énormément de problème, il existe des outils qui limite l'impact des anomalies de traceroute dans des contexte d'équilibrage de charge. Il existe également des extension de traceroute qui contribuent également à contrer les plusieurs problème de traceroute.