Tp Etude de traces IP et ICMP

### Messages ICMP générés par le programme ping

#### Question 1 :

Connaitre sa gateaway :

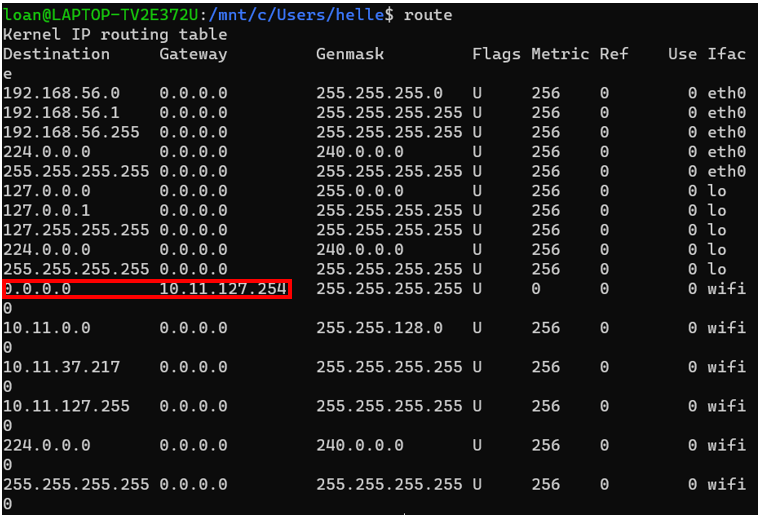
- route (sur linux)

- route get default (sur mac)

Réponse :

192.168.159.254 (si connecté sur réseau Univ-Lorraine)

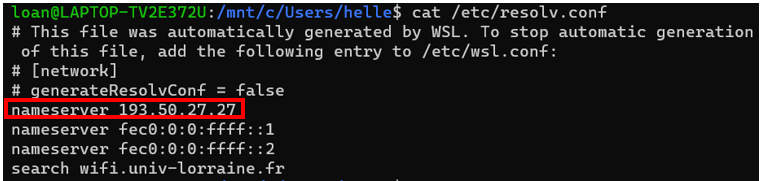
10.11.127.254 (si connecté sur réseau Eduroam)

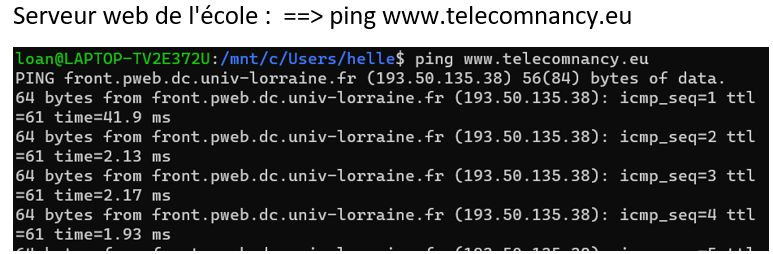


Connaître sa config DNS :

- cat /etc/resolv.conf (sur linux)

- scutil --dns (sur mac)





Réponse :

193.50.27.26 (résolveur local à l'école)

Connaitre IP d'une URL :

nslookup <URL>

(permet aussi de connaître le serveur DNS)

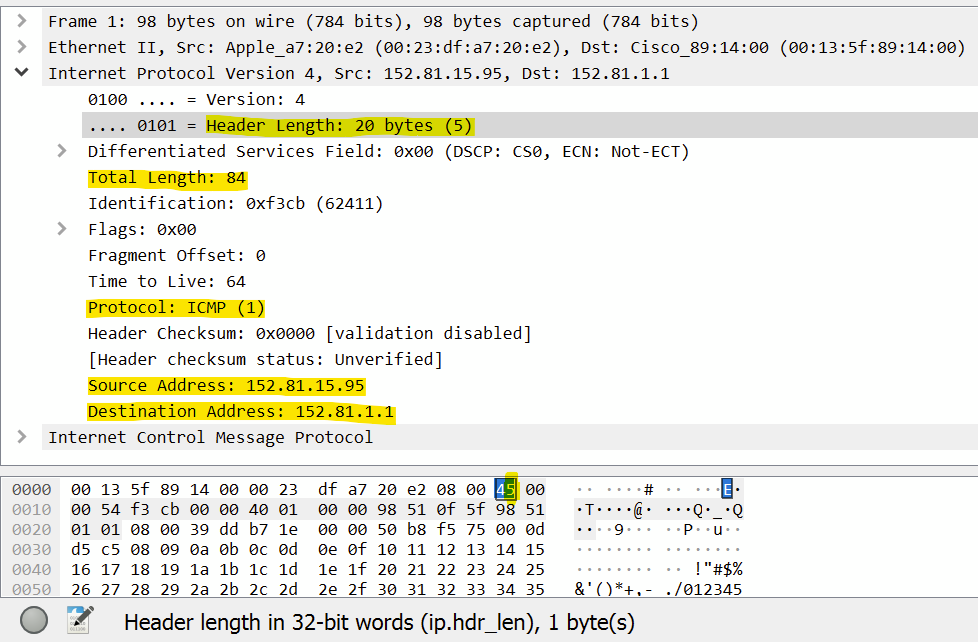
#### Question 2 :

##### Analyse en-tête IP

* Source (du ping) : 152.81.15.95
* Destination : 152.81.1.1
* Valeur = 1, correspond à ICMP
* 20 octets (valeur : 5, header length codé sur 4 bits donc doit être multiplié par 32), codé par paquets de 4 octets (mots de 32 bits)

(explication : avec 4 bits 0 ou 1, on peut seulement faire des valeurs de 0 à 15. Donc pour coder 20 bits, on multiplie chaque bit par 4 octets (donc par 32bits))

* 64 octets dans la partie payload : Total length - Header Length = 84 - 20 = 64



##### Analyse en-tête ICMP

* Un paquet ICMP a-t-il un numéro de port?

Non, ICMP est un protocole de couche réseau pas transport

* Examiner le premier paquet ICMP echo request envoyé par la source:
  + Quels sont les types ICMP et le numéro de code?

Type 8 et code 0 : echo request (ping)

* + Quels sont les autres champs du paquet ICMP?

checksum (2 octets)

identifiant (2 octets)

n° séquence (2 octets)

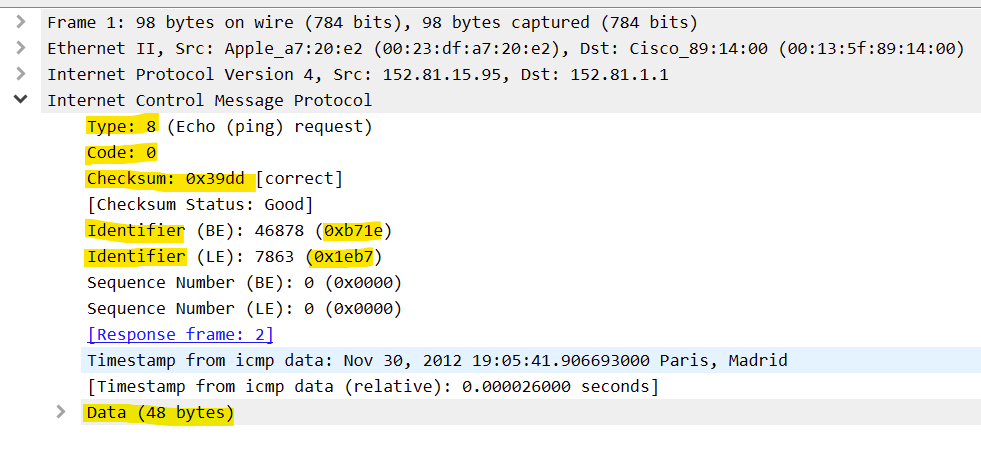
données(48 octets) + 8 octets timestamps

* + Comment évolue le champ **Identifier** entre les différents ICMP echo request? De même le champ **Sequence Number**? identification (2 octets)

id reste inchangé pour les 10 premiers paquets (issus de la même commande)

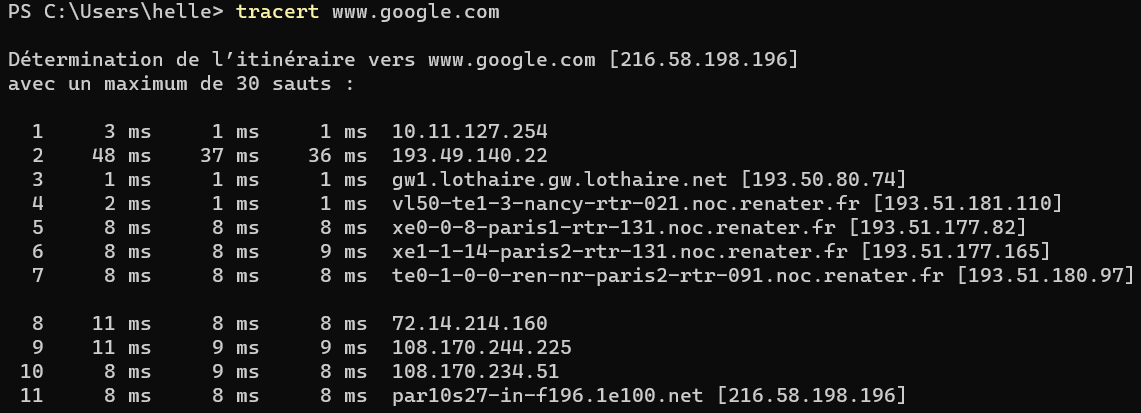
n° de séquence incrémenté de 0 à 9

* Examiner le paquet ICMP reply correspondant à la requête.
  + Quels sont le type ICMP et le numeros de code? type 0 et code 0
  + Quels sont les autres champs du paquet ICMP? Comment est établi le lien avec la requête? identiques à la requête
* 10 requêtes (ping -c 10)
* 2 commandes ping différentes utilisés (2 identifiers différent)



### Messages ICMP générés par le programme Traceroute

#### Question 1 :





inetutils-traceroute -M icmp [www.google.com](http://www.google.com) (pour WSL il faut désactiver les pare feux)

#### Question 2 :

Copier dans votre répertoire le fichier icmp-ethereal-trace-2 et l’ouvrir ensuite avec wireshark.

* Trier les paquets selon le champ information en cliquant sur l’onglet Info. Sélectionner le premier message UDP envoyé.
  + Quelle est la valeur du champ TTL pour les 3 premiers messages, les 3 suivants et ainsi de suite ? (Dans l’entête IP)
    - TTL = 1 pour les trois premières requêtes
    - TTL = 2 pour les trois requêtes suivantes
* Comment évolue le numéro de port ?

Le port source ne change pas mais le port de destination s’incrémente ( 33435, 33436, 33437, ... ) de 1 à chaque fois pour savoir s’il est arrivé à destination et par rapport à quels paquets il en est

* Combien de messages UDP sont envoyés pour la traceroute ?

Traceroute envoie 3 paquets UDP avec la même TTL ⇒ 30 paquets

* En déduire le nombre de routeurs séparant la source de la destination.

9 hops séparent la source et la destination le message UDP avec TTL=10 arrive

* A quel site correspond l’adresse destination(cf question II. 1) ) ?

[www.inria.fr](http://www.inria.fr)

* Trier les paquets selon le champ Numéro en cliquant sur l’onglet No. Sélectionner le premier message ICMP TTL exceeded envoyé à la source par le routeur le plus proche.
  + Quels sont le type ICMP et le numéro de code?

type 11, code 1 : time exceeded in transit

* + Analyser les données contenues danslepaquet ICMP

Contient en plus le 20 octetcs de l’entête IP + les 8 octets de l’entête UDP du paquet en erreur

* Se positionner sur les 3 derniers messages ICMP
  + Quels sont le type ICMP et le numéro de code ?

Type 3 : Destination “unreachable” , code 3 : port “unreachable”

* En déduire comment la source détermine la fin du traceroute :

Différent type d’erreur retourné

* Analyser les données contenues dans le paquet ICMP

Contient en plus IP, UDP et 24 octets de données.

### Pour aller plus loin : fragmentation IP

•Quelle information dans l’en-tête IP indique que le paquet a été fragmenté?

More Fragmented = 1

•En combien de fragments a été découpé le message?

2 (Fragmented) + 1 (ICMP Request) = 3 fragments

•Quelle information indique qu’il s’agit du premier ou du dernier fragment?

Premier fragment ⇒ offset=0, dernier fragment ⇒ More fragment = 0

•Quelle est la taille du message ICMP (sans l’en-tête ICMP) ?

1472 + 1480 + 48 = 3000

•Vérifier votre réponse en regardant les données incluses dans le paquet ICMP Reply.

•Quelle est à votre avis la taille du MTU?

MTU=1480+20=1500 octets(MTU ethernet)

•A quoi correspondent les paquets n° 4 et 5?